CORPORATE MANAGEMENT, GOVERNANCE, AND ETHICS BEST PRACTICES

S. Rao Vallabhaneni
Association of Professionals in Business Management

Corporate Management, Governance, and Ethics Best Practices

S. RAO VALLABHANENI, CBM, CABM

Association of Professionals in Business Management

John Wiley & Sons, Inc.

Corporate Management, Governance, and Ethics Best Practices

Corporate Management, Governance, and Ethics Best Practices

S. RAO VALLABHANENI, CBM, CABM

Association of Professionals in Business Management

John Wiley & Sons, Inc.

This book is printed on acid-free paper.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.

Published simultaneously in Canada.

Library of Congress Cataloging-in-Publication Data:

Vallabhaneni, S. Rao.
Corporate management, governance, and ethics: best practices/S. Rao Vallabhaneni.
p. cm.
Includes index.
ISBN 978-0-470-11723-1 (cloth)
1. Management. 2. Corporate governance.
3. Business ethics. I. Title.
HD31.V3162 2008
658—dc22

2007033365

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

CONTENTS

PREFACE

Corporate Management, Governance, and Ethics Best Practices was written to provide a one-stop, comprehensive reference source for corporate business practitioners and government employees worldwide. It takes a "big picture" approach to the subject matter and compiles best practices to show *what* the best practices are but does not address *how* to implement them. We believe that implementation of best practices is organization-specific based on resource availability and management strategies and priorities.

It is our hope that best-in-class employees working for world-class organizations will think differently and radically (i.e., pursue out-of-the-box thinking) and discover best-of-breed solutions and implement best practices to continuously prosper and grow their organization's business. When implemented properly and in a timely fashion, best practices have helped world-class (best-in-class) organizations to (1) increase product sales and service revenues, (2) achieve cost, production, and service efficiencies, (3) increase effective utilization of financial and nonfinancial resources, (4) improve organizational, operational, technical, and financial performance, (5) increase the quality of products and services in the marketplace, (6) increase market share, profits, and returns, (7) adhere to ethical principles and values and comply with all applicable laws, regulations, and standards, (8) enjoy a competitive edge in the industry, (9) enhance their corporate social-responsibility posture, and (10) empower employees so they can enjoy work and contribute to organizational excellence. In short, best-in-class organizations achieve excellent results and effective management through best practices. However, organization senior management's complacency and wrong mindset can become a major hurdle to achieving and maintaining the world-class status.

The best practices included in this book are not specific to an organization or industry or a country. Our goal is to provide general best practices for wider distribution and large-scale application so that all organizations can benefit. Specific industry best practices can be added to or integrated with these general best practices. Best practices in this book are described in terms of strategies; plans; policies; procedures; guidelines; principles and practices; scorecards, metrics, cycle times, and standards; tools and techniques; action steps; controls (i.e., internal controls, management controls, operational controls, and technical controls); and laws, rules, and regulations.

In terms of use and applicability, best practices established for business management professionals are similar to the professional standards established for accountants, auditors, engineers, lawyers, doctors, and other professionals. It is interesting to note that business managers and executives look at the "best practices" as suggestions (advisory and voluntary) in providing flexibility to them during implementation of the practices and they look at the "professional standards" as restrictions (mandatory) in requiring rigid conformance to the standards by technicians.

The audiences for the best practices book are many, as the book is beneficial to all business corporations, business management and accounting consulting firms, business research institutions, governmental agencies, business schools and universities, and manufacturing and service industries around the globe:

- Business practitioners working for profit corporations, regardless of the business, function, industry, or country
- Government agency heads and employees working at the federal (central), state (province), or local level, regardless of the country
- Management consulting firms and accounting firms providing consulting services to business corporations and/or conducting research in best practices and benchmarking
- Procurement, contracting, and manufacturing officers in governmental agencies, such as the U.S. Department of Defense (DoD), working with defense contractors in acquiring manufactured goods and related services
- Procurement and contracting officers in nondefense governmental agencies such as the U.S. Department of Commerce in acquiring goods and services
- Public or private research institutions conducting best practices and benchmarking research in business-related topics
- Business professors teaching in business schools and universities and/or conducting research in best practices and benchmarking

This book provides a single and standard *framework* for organization-wide implementation of best practices and constitutes an authoritative source on best practices covering all functions of a business corporation, including governance and ethics. Each of the 13 self-contained chapters starts with an overview of its topic and a presentation of management's roles and responsibilities, proceeds to a discussion of core topics, and ends with applicable laws, regulations, standards, and principles.

Chapter 1, "Introduction," describes how benchmarking methodology is used to find the best practices; explains the need for performance indicators and measures such as scorecards, metrics, cycle times, and standards; establishes a solid link between cycle times and business velocities (e.g., sales, inventory, production or service, finance, human capital, and systems velocity); and introduces a new model called the best-practices management capability maturity model as a structured way to implement the best practices to improve business processes. Information from Chapter 1 is useful with respect to all chapters because it provides a common framework to apply to them.

Chapter 2, "Corporate-Governance Best Practices," sets the overall stage and tone in discussing the primary driving force to be followed by all business functions and all business managers and executives. It presents corporate governance principles, employee reporting relationships, and roles and responsibilities of the board of directors, the Chief Executive Officer, the Chief Governance Officer, external auditors, internal auditors, audit committee and other committees, the Chief Legal Officer, and gatekeepers. It discusses topics such as corporate control framework, fraud and fraudulent financial reporting, and corporate risk management.

Chapter 3, "Corporate-Ethics Best Practices," provides boundaries within which corporate management and all business functions can operate in a unified, consistent, and ethical manner. Ethical and legal principles such as due process, due care and due diligence, due professional care, and codes of conduct are discussed, along with the roles and responsibilities of the Chief Ethics Officer. How a corporate management should handle various stakeholders from an ethical viewpoint is discussed.

Chapters 4 through 13, all dealing with corporate-management best practices, address specific practices in the areas of general management (Chapter 4); manufacturing and service (Chapter 5); marketing and sales (Chapter 6); quality (Chapter 7); process (Chapter 8); human resources (Chapter 9); accounting, treasury, and finance (Chapter 10); information technology (Chapter 11); international business (Chapter 12); and project management (Chapter 13). Examples of performance indicators such as metrics and cycle time measures are presented in manufacturing and service, marketing and sales, human resources, finance, and information technology. Information regarding quality management and process management should be blended into the other chapters that pertain to corporate management, as it provides a common application featuring tools for quality control, quality management, problem solving, decision making, and process management.

Performance indicators (stretch goals) such as scorecards, metrics, cycle times, and standards are part of an organization's value chain and best practices. The value chain should be enhanced by increasing value-added activities and by eliminating non-value-added activities to provide a permanent value to the internal and external customers as well as to the organization as a whole. This requires first streamlining the business processes; second simplifying; third, standardizing; and then institutionalizing them.

Organization's management can discover best-of-breed solutions only when they listen to various *stakeholder voices*, including internal and external voices, very carefully and closely and only when they think differently and radically (i.e., pursue out-of-the-box thinking). Examples of these "voices" include the voice of the customer, voice of the process, voice of the investor, voice of employees, voice of quality, voice of standards, voice of partners, voice of regulators, and voice of competitors. These nine "voices" can be heard very loud and clear in the manufacturing and service, marketing and sales, human resources, finance, and information technology core chapters. When these nine "voices" are heard together, they bring attention to new perspectives and creative conflicts, forcing new thinking that leads to new solutions (i.e., best-of-breed solutions). Listening to the collective voice of many stakeholders at once will have a greater impact than listening to one voice at a time in isolation, because the collective voice requires a balanced approach after considering all party's concerns. A discovery of best-of-breed solutions combined with analysis of outside-in views (i.e., views of stakeholders about company management) and inside-out views (i.e., views of company management about stakeholders) can help in developing best practices by promoting new and clearer thinking.

Both corporate governance and corporate ethics lay a strong foundation for corporate management. The stronger the foundation in governance and ethics, the better the performance by corporate management. Both corporate governance and corporate ethics support corporate management. That is,

$$\text{Corporate governance} + \text{corporate ethics} = \text{corporate management}$$

Exhibit 1 shows the linkage between corporate governance, ethics, and management through best practices.

This book is based on information from authoritative sources including (1) the Organization for Economic Co-operation and Development's (OECD's) *Principles of*

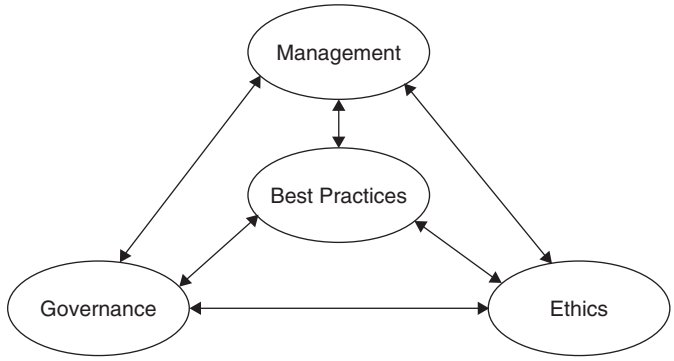

Exhibit 1 Linkages Between Corporate Governance, Ethics, and Management

Corporate Governance (www.oecd.org), (2) Business Roundtable's *Principles of Corporate Governance* (www.businessroundtable.org), (3) the National Association of Corporate Directors (www.nacdonline.org), (4) the Committee of Sponsoring Organizations (COSO) of the Treadway Commission (www.coso.org), (5) the American Institute of Certified Public Accountants (www.aicpa.org), (6) the Institute of Internal Auditors (www.theiia.org), (7) the U.S. Government Accountability Office (GAO, previously known as General Accounting Office), which issues reports to the U.S. Congress (www.gao.gov), (8) the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) Special Publications (www.nist.gov), (9) the U.S. Department of Defense (www.defenselink.mil), (10) *Gatekeepers: The Professions and Corporate Governance* by John C. Coffee, Professor of Law at Columbia University Law School and Director of its Center on Corporate Governance (www.oup.com), (11) the Project Management Institute's (PMI's) *A Guide to the Project Management Body of Knowledge (PMBOK Guide)* (www.pmi.org), (12) the American Marketing Association (AMA), (www.ama.org and www.marketingpower.com), and (13) *The Strategy-Focused Organization: How Balanced Scorecard Companies Thrive in the New Business Environment* by Robert S. Kaplan and David P. Norton (www.hbsp.harvard.edu).

Organizations, both private and public (e.g., the U.S. Department of Defense and its defense contractors, the U.S. Department of Commerce, and other governmental agencies), can use these best practices as a starting point and adjust them to their specific needs by adding or removing best practices to fit specific organizational standards or industry standards. This is because best practices are universal and shareable regardless of an organization's mission and regardless of national borders. The best practices repository should be kept up to date with best practices' constant evolution as organizations research them and learn them from other organizations.

One of the highlights of this book is the way it properly defines the roles, responsibilities, and reporting relationships of the various C-level executives. Improper definition or practice of employee reporting relationships at any management level is often deeply

rooted in corporate governance, control, and ethical problems. Improper reporting relationships, especially between and among the C-level executives (e.g., CEO, CFO, CIO, COO, CAO, CAE, and CMO), create control-related problems and pose ethical dilemmas due to conflict of interest, lack of separation of duties, and lack of independence and objectivity. Incompatible job functions and faulty separation of duties can lead to fraud, collusion, and other irregularities. Corporate goal congruence is at risk when individual goals and interests dominate and conflict with the goals of the corporation. Proper organizational structure and employee reporting relationships can enforce clear lines of responsibility and accountability throughout the organization.

Ethical Behavior versus Unethical Behavior

- Nonconflicting roles and responsibilities can lead to ethical behavior
- Conflicting roles and responsibilities can lead to unethical behavior
- Employees, managers, executives, investors, government regulators, and the general public (the society) all do care about business ethics although in varying degrees and magnitudes due to their different roles and job duties.

We are establishing new knowledge standards for the business management profession with the introduction of a new concept, the chain of knowledge, which is similar to the chain of custody used with regard to legal evidence. The principle of the chain of custody holds that evidence should be collected, protected, and retained intact at all times as it moves from one investigator to another to lawyers to the courts. Similarly, the principle of the chain of knowledge holds that knowledge should be acquired, maintained, and applied continuously and consistently as an employee moves up the management hierarchy of the organization. This requires that (1) lower-level employees possess the basic knowledge, skills, and abilities (KSAs) related to a given business function, and (2) the higher-level employees possess the advanced KSAs relating to the same function, so that a common thread of knowledge runs through the entire function. The chain of knowledge should be as strong as possible, since weak links can be fatal to a chain. As the employee moves up the management hierarchy, more emphasis is placed on soft skills and less emphasis on hard skills.

Examples of Soft Skills and Hard Skills

Soft skills include written/oral communication, interpersonal, qualitative (content and context analysis), implementation, listening, negotiating, leadership, and teamwork skills.

Hard skills include analytical, technical, technological, mathematical, quantitative, problem-solving, decision-making, deductive/inductive reasoning, and functional skills.

The primary goal of the chain of knowledge is to identify knowledge-mismatch employees at all levels of the organization in order to improve their core knowledge competencies. Because best practices are derived from a wealth of knowledge base, understanding and implementing the best practices are part of the chain of knowledge as it can improve both the employees' and the organization's performance levels. The

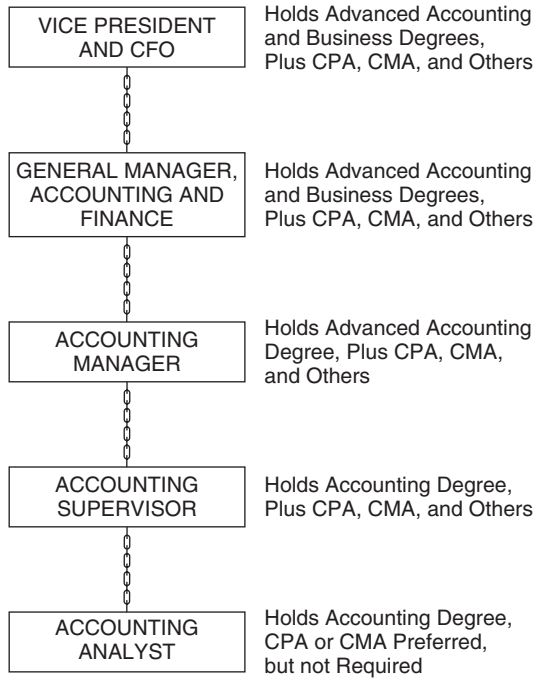

Exhibit 2 Chain of Knowledge Concept Applied to the Finance Management Hierarchy

chain of knowledge helps in creating best-in-class employees by establishing a common base of knowledge among and between employees.

The chain of knowledge concept applies to employee reporting relationships and employee job performance in that lower-level employees who share given KSAs should be reporting to middle-level employees with KSAs, while the middle-level employees, in turn, report to higher-level employees with the KSAs corresponding to their level, thereby keeping the chain of knowledge relevant, strong, and effective. Improper implementation of the chain of knowledge can lead to employee performance deficiencies, communications problems, and expectation gaps. Exhibit 2 presents a sample chain of knowledge for the finance function.

Another highlight of this book is its listing of 26 risk types for the Chief Risk Officer to take account of in managing a total business risk-management program. This comprehensive approach to risk management makes a good deal of business sense, considering the many uncertainties facing organizations today because of changes in economic, political, cultural, regulatory, technical, and global business factors.

Because organizations have a legal and ethical obligation to comply with various laws, rules, and regulations, we have provided a sample collection of applicable laws, rules, regulations, standards, or principles for them to use as a reminder for checklist purposes. Compliance with laws, rules, and regulations will reduce the possibility of

reputation (image) risk, resulting from adverse publicity in the news media. Applicable laws, regulations, standards, or principles are included in each chapter of this book.

The current *research methodology* includes a review of published documents, Web sites, U.S. government agency reports, best-practices research studies, benchmark reports, white papers, symposiums, forums, textbooks, trade books, public domain information, information from professional associations and organizations, informational papers, and personal information. Future editions will draw on greater involvement by many Certified Business Managers (CBMs) and Certified Associate Business Managers (CABMs) to achieve wider participation, distribution, and sharing of global best practices for years to come. The CBM is a masters-level professional credential based on an MBA curriculum and consisting of four-part, 16-hour rigorous exams. The CABM is a bachelors-level professional credential based on a pre-MBA curriculum and consisting of a rigorous one-part, four-hour exam.

The Association of Professionals in Business Management (APBM) has developed a Common Body of Knowledge for Business (CBKB), which is organized into ten learning modules. The CBKB describes the exam content specifications, which serve as a basis for the CBM and CABM exam questions and for the development of exam preparation guides. This best practices book is linked to the ten learning modules for maximum integration. This linkage is beneficial to potential CBMs during their study for the CBM exams, and later for the real CBMs and non-CBMs to use the best practices book as a desk reference source when needed. The CBM credential can transform a business specialist into a business generalist due to its focus on general management KSAs.

APBM wants to make this best practices book a landmark, a legendary research project representing a single and collective voice for the entire business management profession around the world. Today, more than ever, there is a need for a single and collective voice for the entire business management field, but disparate and disconnected professional associations continue to represent the various specialized business functions, such as operations management, supply management, marketing, quality, human resources, accounting, auditing, fraud treasury, finance, IT, and project management. An integrated and umbrella-type professional association, such as the APBM, lends credibility and sends a positive signal to all stakeholders—such as government regulators, investors and creditors, stock/capital markets, legal system, corporate management and employees, labor unions, vendors and suppliers, media/press, consultants and contractors—and to the general public. To this end, APBM symbolizes self-regulation by the profession.

APBM, which was established to represent business managers and executives worldwide, is akin to American Medical Association representing doctors, American Bar Association representing lawyers, and American Institute of Certified Public Accountants representing public accountants in the United States.

APBM is a not-for-profit higher-education professional organization with the mission of making business management a profession, similar to law, medicine, engineering, and accounting. APBM accomplishes its mission through certifications, continuing education, a code of professional ethics, and professional standards through best practices research.

With no bias intended and for the sake of simplicity, the pronoun "he" has been used throughout the book rather than "he/she" or "he or she."

Chicago, Illinois
January 2008

S. Rao Vallabhaneni
Info@apbm.org

Corporate Management, Governance, and Ethics Best Practices

Corporate Management, Governance, and Ethics Best Practices

CHAPTER 1

INTRODUCTION

1.1 BEST PRACTICES

(a) OVERVIEW. "Best practices" refers to processes, practices, and systems that are identified in top-performing public and private organizations and are widely recognized as improving the organizations' performance and efficiency in specific areas. Successfully identifying and applying best practices can reduce business expenses and can improve organizational efficiency.[1]

A best practices review or best management-practices review can be applied to a variety of processes, such as payroll, travel administration, employee training, procurement, accounting and budgeting, transportation and distribution, maintenance and repair services, and information technology (IT). The decision to use a best practices review should be made in a larger context that considers the strategic objectives of the organization and then looks at the processes and operating units that contribute to those objectives. Ask questions like:

- What drives the costs in a particular process?
- Is the process effective in achieving its goals?

An initial step is to determine all the variables that contribute to the expenditures associated with the area. Another early step is to start with the areas that the customers think are of major importance to the organization being reviewed.

Identifying the scope of the process to review is not always easy. It is not always clear where to start and where to stop when one decides to benchmark a process. It is important that the entire process be considered, rather than just part of the process. If an organization fails to capture the entire process, then it is simply pushing costs into other areas of the process or creating an improvement that is inhibited by trying to marry old ways and new ways when the two conflict with each other. However, one cannot look at everything. At least initially, select a process that is about ready to accept change.

(b) BEST PRACTICES METHODOLOGY. Best practices methodology is a relatively new approach to improving business or government operations. Many organizations, in both the public and private sectors, are beginning to recognize that in order to survive in the future, they have to initiate major changes that will make them more productive and reduce costs.

WHAT IS BENCHMARKING?

Benchmarking is more than just a comparison of performance measures and cost ratios. Rather, the total organizational impact must be considered.

The best practices approach to change, one of several approaches, involves identifying organizations that are widely recognized for major improvements in their performance and efficiency in a specific area, such as inventory management. The processes, practices, and systems identified in these organizations are referred to as *best practices* and provide a model for other organizations with similar missions and objectives. Frequently, benchmarking is used to gather information on these practices from a number of different organizations, which is then applied to improving operations. Benchmarking is also an effective approach for promoting organizational change. Best practices are intended to radically change and improve organizational processes.

In identifying best practices among organizations, the "benchmarking" technique is frequently used. When benchmarking, an organization (1) determines how leading organizations perform specific processes, (2) compares their methods to its own, and (3) uses the information to improve upon or completely change its processes. Benchmarking is typically an internal process, performed by personnel within an organization who already have a thorough knowledge of the process under review.

During a best practices review, one is forced to consider new approaches. Specifically, one compares how an organization performs functions with how another organization is doing them differently. The different approach may turn out to be a much better way of performing a function. Implementing this better way to perform a process throughout the organization is what allows an organization to make meaningful changes. In identifying best practices among organizations, the "benchmarking" technique is frequently used.

The best practices evaluation will look not only at quantitative data, such as costs, but also at how other processes and factors, such as organizational culture, might be affected by change. There are six elements that any best practices review should include, as described below:

1. **Understanding the Process to Be Improved.** The first step is to thoroughly understand the process before speaking with people in various organizations. This will help in recognizing opportunities for improvement. Understanding the process will ease analysis by defining a baseline for comparison and providing more focus to questions when making inquiries regarding the best practices identified in other organizations. Further, a good depth of understanding is essential to selecting appropriate companies for comparison. Discussing the process in detail with affected people and flowcharting the process will facilitate data gathering from the comparison organizations and the comparative analysis.
2. **Researching to Plan the Review.** Preliminary planning and research are key elements in preparing a best-practices review; both must be done before selecting the organizations for comparison. Performing a literature search, researching industry trends, and speaking with consultants, academics, and industry/trade group officials will provide valuable background information on the process under review. It will also provide the names of leading-edge companies and public sector organizations. Other sources for leading-edge companies and names of the people involved include telephone books, company annual reports, and commercial databases.
3. **Selecting Appropriate Organizations.** After you have reviewed the literature and conducted your discussions with consultants, academics, and industry/trade

group officials, you will have compiled a list of many organizations cited as "best" in their respective industries for the process you are reviewing. The next decision is determining how many organizations to visit. There is a tradeoff in selecting organizations. Since visiting too many companies can cause "analysis paralysis," the list should be kept at five. It should not be limited to just one company for the sake of time and convenience. Depending on the process under review, you may want to select companies that are geographically dispersed. One needs to determine the criteria that best meet one's needs. The criteria need not require finding the "best of the best" if the difference in the process is not significant among leading-edge organizations. In these cases, what is important is to find companies that are considered by experts to be among the best at the process under review. Such companies may be able to give you more than the very best, which may be followed with requests to study them. Selecting appropriate organizations to visit is the most important and most difficult element of a best practices review.

4. **Collecting Data from Selected Organizations.** After you have researched and begun planning your review, you should develop a list of questions to use as a guide for discussions with consultants, academics, and industry/trade group officials. These questions need to be refined after the first interview with a company to make them more appropriate and focused. A standard list of questions will ensure that you are obtaining comparable information regarding the organizations you visit. Your analysis will involve looking for common practices and characteristics among the organizations you have identified as having the best practices in the selected function under review.
5. **Identifying Barriers to Change.** A major challenge to ensuring that your final recommendations will be implemented and effective lies in identifying the barriers to change, whether real or perceived. Potential sources of barriers include regulatory requirements, organizational culture, and the possible impact of the change on the organization's products and services. Identifying barriers to change is the most difficult step in implementing a best-practices methodology.

   While government regulations do not always prevent the use of best practices, they may make change difficult. Organizational culture can be a major obstacle. Entrenched systems can make changes difficult to implement. Immediate and comprehensive change is unlikely in many organizations; it can take five to ten years or longer to change an organization's culture.
6. **Making Recommendations for Change.** The final step in the best practices review is to compare and contrast the organization's process with the processes of the organizations you benchmarked, and to decide whether the organization would benefit from implementing new processes. If the answer is "yes," then make recommendations, keeping flexibility in mind since it may not be possible to do things exactly as they are done in the other organizations. It is always good to develop a "basket of ideas" from which to choose; this approach not only provides flexibility but also increases the potential for acceptance of the change. Demonstrating possible savings and recommending key steps for change will help to promote the change. Photographs of the consequences of the process comparing "before" and "after" the change are convincing tools for illustrating

the effectiveness of a recommended change. Also, a pilot project gives the ability to work through any concerns or obstacles and allows the organization time to develop cost and benefit estimates for full implementation.

LESSONS LEARNED FROM BEST PRACTICES

- To be effective, organizations should focus on all business processes, not just customer-related processes.
- There is a direct relationship between the quality of the employees an organization has and the quality of service provided to customers.
- Having the right quality and quantity of information is crucial in satisfying the needs of customers, owners, and stakeholders alike.
- Organizations should manage all of their resources, including physical, financial, human, and intangible (intellectual) assets.
- Organizations that are process-oriented, customer-focused, change-oriented, and future-directed will create long-lasting value for customers, owners, and stakeholders alike.

1.2 BENCHMARKING

(a) OVERVIEW. Benchmarking is the comparison of core process performance with other components of an organization (internal benchmarking) or with leading organizations (external benchmarking). Benchmarking is a key tool for performance improvement because it provides "real world" models and reference points for setting ambitious improvement goals. Benchmarking helps to (1) identify the gaps between the organization's process performance and that of leading organizations, and (2) understand how these leaders have changed their structures, work processes, and lines of business to improve performance dramatically. When used in conjunction with performance measurement, benchmarking provides a powerful means of establishing a compelling business case for change.

(b) TYPES OF BENCHMARKING. Two types of benchmarking exist: business process benchmarking and computer-system benchmarking. Business process benchmarking deals with business process improvement (BPI) and business process reengineering (BPR) to reduce costs and to improve quality and customer service. Computer-system benchmarking focuses on computer hardware/software acquisition, computer-system design, computer-capacity planning, and system performance. Each has its own place and time.

LINK BETWEEN BENCHMARKING AND BEST PRACTICES

Benchmarking results are used to develop or modify best practices, and hence there is a link between the two.

(i) Business Process Benchmarking. Business benchmarking is an external focus on internal activities, functions, or operations in order to achieve continuous improvement. The objective is to understand existing processes and activities and then to identify an external point of reference, or standard, by which that activity can be measured or judged.

A benchmark can be established at any level of the organization in any functional area, whether manufacturing or service industries. The ultimate goal is to be better than the best—to attain a competitive edge.

Value creation is the heart of organizational activity, be it a profit or nonprofit entity. Benchmarking provides the metrics by which to understand and judge the value provided by the organization and its resources. Benchmarking focuses on continuous improvements and value creation for stakeholders (i.e., owners, customers, employees, and suppliers), utilizing the best practices to focus improvement efforts.

Benchmarking targets the critical success factors for a specific organization. It considers the mission of an organization, its resources, products, markets, management skills, and others. It requires the identification of customer(s), whether internal or external to the organization. Benchmarking is an early warning system of impending problems and is not a one-time measurement. Benchmarking can focus on improving organization structures, analyzing managerial roles, improving production processes, or developing strategic issues.

What are the sources of information for benchmarking? Benchmarking can be done by using published materials, insights gained at trade association meetings, and conversations with industry experts, customers, suppliers, academics, and others.

An organization benchmarks for three reasons: (1) it wants to attain world-class competitive capability, (2) it wants to prosper in a global economy, or (3) it simply wishes to survive (desperation).

Benchmarking should be undertaken when "triggers" are present. These triggers can arise internally or externally in response to information needs from some other major project or issue or problem in the company. Examples of these "triggers" include (1) quality programs, (2) cost-reduction programs, (3) new management, (4) new ventures, and (5) competitive moves. Benchmarking should be done as needed, without any preconceived notions.

An organization can benchmark in six distinct ways.

1. **Internal Benchmarking** (self-examination) is the analysis of existing practices within various departments or divisions of the organization, looking for best performance as well as identifying baseline activities and drivers. Drivers are the causes of work: the triggers that set in motion series of actions, or activities, that will respond to the requests or demands of the stockholders.

   In doing internal benchmarking, management is looking downward, examining itself first before looking for outside information. Significant improvements are often made during the internal analysis stage of the benchmarking process. Value-added activities are identified and non-value-adding steps are removed from the process. Internal benchmarking is the first step because it provides the framework for comparing existing internal practices with external benchmark data. Internal benchmarking focuses on specific value chains or sequences of driver-activity combinations.
2. **Competitive Benchmarking** (limited to one industry) looks outward to identify how direct competitors are performing. Knowing the strengths and weaknesses of the competitors provides a good input for strategic and corrective actions.
3. **Industry Benchmarking** (looks at industry trends) extends beyond the one-to-one comparison of competitive benchmarking to look for trends. It is still limited in

the number of innovations and new ideas it can uncover because everyone is following the other. At best, it can help establish the performance baseline or can give an incremental gain. It gives a short-run solution and a quick fix to an existing problem. However, it does not support quantum leaps or breakthroughs in performance since the comparison is limited to one industry.

4. **Best-in-class Benchmarking** (looks at multiple industries) goes beyond a single industry to look for new, innovative practices, no matter what their source. This is the ultimate goal of the benchmarking process. It supports quantum leaps in performance and gives a long-run competitive advantage.
5. **Process Benchmarking** (looks at key work processes) centers on specific processes such as distribution, order entry, or employee training. This type of benchmarking identifies the most effective practices in companies that perform similar functions, no matter in what industry.
6. **Strategic Benchmarking** (focuses on market success) examines how companies compete and seeks the winning strategies that have led to competitive advantage and market success.

WHICH BUSINESS PROCESS BENCHMARKING IS WHAT?

- Internal benchmarking is looking downward and inward.
- Competitive benchmarking is looking outward.
- Industry benchmarking is looking for trends. It provides a short-run solution and a quick fix to a problem.
- Best-in-class benchmarking is looking for the best all around. It provides a quantum jump in improvement.
- Process benchmarking is specific to a process.
- Strategic benchmarking is broad, with big impact on the entire organization.

(ii) Computer-System Benchmarking. Although benchmarking is generally thought of as an important and necessary tool during the hardware or software acquisition process, it also has many other useful applications:

- The effects of software and hardware changes on system performance can be evaluated by running a representative benchmark before and after such changes.
- Benchmarking can be used in computer-capacity planning to determine the unused capacity and the saturation point of the present system. This is done by first constructing a benchmark to represent projected workload(s) and then by running the benchmark to stress test the current system (i.e., to determine at what load levels required service levels can no longer be attained). This application of benchmarking would thus enable an organization to plan better for future acquisitions.
- Benchmarking can also be used to evaluate the design of computer systems. The hardware/software vendors themselves largely use this application. Computer-system designers often use benchmarks to evaluate the capabilities and performance of their new computer systems.
- Benchmarking is most commonly used as an evaluation technique in the computer-system acquisition process. It is a common test by which different vendor systems can be evaluated. Benchmarking in this context can serve

several important functions. It can assist the vendors in determining the most cost-effective offering to satisfy the organization's requirements. It can facilitate the verification of the proposed system as to the time required to perform the workload and as to its functional capabilities. And, finally, it can sometimes be used prior to or during acceptance testing, after contract award, to verify that the delivered system is consistent with the system benchmarked during the evaluation phase.

Lessons Learned from Benchmarking

- Benchmarking is more than just a comparison of performance measures and cost ratios. Rather, the total organizational impact must be considered.
- A ''basket of ideas'' gives the organization flexibility in adopting new processes, thus providing more potential for positive acceptance of change.
- Pilot projects give the organization the ability to work through any concerns or obstacles and allow them time to develop cost estimates for full implementation.
- Outsourcing can suggest areas that can benefit from a best practices and benchmarking review.

1.3 PERFORMANCE INDICATORS AND MEASURES

(a) OVERVIEW. In work settings, employees accomplish things and tasks that are measured by their supervisors because these accomplishments become a part of the employee's performance record, which is used during employee appraisal review. It is a fact of business life that an organization's performance is an aggregation of each employee's performance. Strategic, financial, regulatory, legal, and organizational reasons drive the measurement of an organization's performance.

Selection Criteria for Performance Indicators

Selection of the type of performance indicators should be credible, meaningful, and significant to the business and should involve only a few numbers, for better management of the measurement process.

Leading organizations, both in the public and private sectors, are using various performance indicators to measure, track, and report organization performance levels for improvement as part of their best practices. These include scorecards (balanced scorecards, strategy scorecards, stakeholder scorecards, key performance indicator scorecards, functional scorecards, and dashboard scorecards), metrics, cycle times, and standards. These standards include national standards, regional standards, international standards, organization standards, industry standards, and professional standards. For example, some U.S. organizations compare their performance with that of the U.S. Malcolm Baldrige Criteria for Performance Excellence Results, which is an example of a national standard.

Performance indicators such as scorecards, metrics, cycle times, and standards are also a part of an organization's value chain. New performance indicators lead to new initiatives for management. The value chain should be enhanced by increasing value-added activities and by eliminating non-value-added activities to provide a

permanent value to internal and external customers as well as to the organization as a whole.

Selecting the right type of performance indicators (stretch goals) is as important as initiating the performance measurement program, if not more. Incorrect selection leads to unusable results. The selected indicators should be simple in thinking, should be easy to understand, implement, and measure, and should lend themselves to easy interpretation of the results. Performance indicators should be selected from various generic sources, such as the organization's strategic and business plans; functional and operational goals and objectives; internal and external benchmark reports; employee performance targets that are committed; quality, process, and operations improvement plans; teachings from "lessons learned" files; industry white papers; lists of critical success factors; internal/external audit reports; and publicly available databases on best practices and benchmarks.

(b) SCORECARDS. Most businesses on investment, earnings per share) and manufacturing data (e.g., factory productivity, direct labor efficiency, and machine utilization). Unfortunately, many of these indicators are inaccurate and stress quantity over quality. They reward the wrong behavior, lack predictive power, do not capture key business changes until it is too late, reflect functions instead of cross-functional processes, and give inadequate consideration to difficult-to-quantify resources such as intellectual capital. Most measures are focused on cost, not so much on quality.[2]

(i) Balanced Scorecards. Robert S. Kaplan and David P. Norton of Harvard Business School coined the term "balanced scorecard" in response to the limitations of traditional financial and accounting measures. A good balanced scorecard contains both leading and lagging indicators, and both financial and nonfinancial measures. For example, customer surveys (performance drivers) about recent transactions might be a leading indicator for customer retention (a lagging indicator), employee satisfaction might be a leading indicator for employee turnover (a lagging indicator), and so on. These measures and indicators should also establish cause-and-effect relationships across the four perspectives. The cause-and-effect linkages describe the path by which improvements in the capabilities of intangible assets (people) get translated into tangible customer satisfaction and financial outcomes.

(ii) Strategy Scorecards. Kaplan and Norton recommend that key performance measures should be aligned with the strategies and action plans of the organization. They suggest translating the strategy into measures that uniquely communicate the vision of the organization. Setting targets for each measure provides the basis for strategy deployment, feedback, and review.

They divided the strategy-balanced scorecard into four perspectives or categories as follows:

1. **Financial Perspective.** It measures the ultimate results that the business provides to its shareholders, including profitability, revenue growth (net income), return on investment, economic value added, residual income, and shareholder value. Financial measures are lagging measures (lag indicators); they report on outcomes, the consequences of past actions. They tell what has happened. The financial perspective is looking back.

2. **Customer Perspective.** It focuses on customer needs and satisfaction as well as market share, including service levels, satisfaction ratings, loyalty, perception, and repeat business. The customer perspective is looking from the outside in.
3. **Internal Perspective.** It focuses attention on the performance of the key internal processes that drive the business, including such measures as quality levels, efficiency, productivity, cycle time, and production and operating statistics such as order fulfillment or cost per order. Internal process measures are leading measures (lead indicators); they predict what will happen. The internal process theme reflects the organization value chain. The internal process (operations) perspective is looking from the inside out.
4. **Learning and Growth Perspective.** It directs attention to the basis of a future success—the organization's people and infrastructure. Key measures might include intellectual assets, employee satisfaction and retention, market innovation (new product introductions), employee training and skills development, research and development (R&D) investment, R&D pipeline, and time-to-market. The learning and growth perspective is looking ahead.

The strategy scorecards provide graphical representation of strategy maps, and a logical and comprehensive way to describe strategy. They communicate clearly the organization's desired outcomes and describe how these outcomes can be achieved. Both business units and their employees will understand the strategy and identify how they can contribute by becoming aligned with the strategy.

(iii) Stakeholder Scorecards. The stakeholder scorecard identifies the major constituents of the organization—shareholders, customers, and employees—plus, often, others such as partners and the community. This scorecard defines goals for these stakeholders and develops an appropriate scorecard of measures and targets for them. Missing from such scorecards is any indication of how these balanced goals are to be achieved. A vision describes a desired outcome; a strategy, however, must describe how the outcome will be achieved and how stakeholders will be made satisfied. Thus, a stakeholder scorecard is not adequate to describe the strategy and is not an adequate foundation on which to build a management performance system.

Stakeholder scorecards, which miss the element of "how," are a first step on the road to a strategy scorecard. The stakeholder scorecard can also be useful as a corporate scorecard in which internal synergies across the strategic business units (SBUs) are limited. Because each SBU has a different set of internal drivers, the corporate scorecard need only focus on the desired outcomes for the corporation's constituencies. Each SBU then defines how it will achieve those goals and articulates these with its business strategy scorecards.

The stakeholder scorecard can keep the stakeholders satisfied but cannot realize performance breakthroughs. It omits critical internal processes and the linkages for driving breakthroughs for customers and shareholders. The local, low-level stakeholder scorecard must be aligned with the organization-wide, high-level strategy scorecard in terms of deployment, feedback, and review.

(iv) Key Performance Indicator Scorecards. Key performance indicator (KPI) scorecards are found mostly in manufacturing and health care industries, IT functions, and

management consulting organizations. KPI can link with the total quality management (TQM) philosophy. A company database is at the heart of the KPI program, which triggers the scorecard design.

KPI scorecards will be most helpful for departments and teams when a strategic program already exists at a higher level. The lower-level indicators (KPIs) will enable individuals and teams to define what they must do well to contribute to higher-level goals. Without this explicit link between the lower-level and the higher-level goals, the KPI scorecards will be ineffective. The KPI scorecards can drive improved operational performance but cannot realize performance breakthroughs. The scorecards omit critical internal processes and the linkages for driving breakthroughs for customers and shareholders. The local, low-level KPI scorecard must be aligned with the organization-wide, high-level strategy scorecard in terms of deployment, feedback, and review.

(v) Functional Scorecards. Many functional organizations such as IT, human resources, finance, marketing, and R&D have developed functional scorecards. The functional scorecard can be viewed as a business-in-a-business model. To be useful, the functional scorecard must be linked to the SBU scorecard and the corporate scorecard. Some examples of the uses of an IT functional scorecard for the internal process category include (1) providing a flexible global infrastructure, (2) managing technical and operating risk, (3) creating and developing system solutions, (4) understanding, anticipating, and prioritizing customer needs, and (5) servicing the customer. Other IT performance measures include software performance, hardware performance, and project delivery.

IT can make data available to users, provide graphical interfaces, provide drill-down capabilities to reach detailed data and transactions, provide data mining and warehouse capabilities, and provide e-mail links. For example, the enterprise resource planning (ERP) system, customer relationship management (CRM) system, activity-based costing system, and shareholder value system (economic-value-added (EVA) system) can be combined through an organization's data warehouse to facilitate tracking, measuring, and reporting the scorecard indicators. By giving lower-level employees access to the scorecard system, the organization greatly amplifies its problem-identification, problem-solving, opportunity-creating, and knowledge-sharing capabilities. The scorecard system and its results should not be limited to higher-level employees only.

Organizational culture affects technology. Cultural assumptions are frequently overlooked and are often embedded in the technology itself, which can either create or inhibit the climate for change. The following seemingly simple questions, while technically elegant, have complex cultural implications:

- Who can access and use the system?
- How should organizational performance be communicated?
- Is this report an addition to the existing reporting system?

(vi) Dashboard Scorecards. Many organizations have adopted the term "dashboard" scorecard as an alternative to a balanced scorecard. This reference stems from the analogy to an automobile's dashboard—a collection of indicators (e.g., speed, revolutions per minute, oil pressure, and temperature) that summarizes the car's performance. Dashboard scorecards use colors to indicate quality and status, and in so doing they provide a concise, visual summary of overall organizational performance.

(vii) Scorecard Implementation Issues. Kaplan and Norton identified three reasons for disappointment in implementing the scorecard system. They include transitional issues, design issues, and process issues. The transitional issues arise when a company is acquired by or merged with other company. The scorecard project could either be abandoned completely or stopped due to lack of interest on the part of the new company. The design issues come from building a poor scorecard system. A company might have selected too few or too many unimportant measures per perspective. What is needed is few critical measures. The most common causes of scorecard implementation failures are poor organizational processes, not poor scorecard design. Kaplan and Norton identified seven types of process failures:

1. Lack of senior management commitment
2. Too few individuals involved
3. Keeping the scorecard at the top of the organization
4. Prolonging the development process and managing it as a onetime project
5. Treating the balanced-scorecard project as a computer-system project
6. Hiring inexperienced consultants and contractors
7. Introducing the balanced-scorecard project only for compensation purposes

(c) METRICS. Metrics are tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data. Metrics focus on the "amount" dimension, expressed as raw amounts (quantities) or percentages. In general, metrics can be used to:

- Evaluate and understand an organization's current performance levels
- Identify the critical processes that require focused, management attention
- Obtain the knowledge needed to set realistic goals for improvement
- Document results over time

Companies typically measure total savings, cost avoidance, or some other financial measures, which are reported to senior managers and executives. For example, metrics can be useful to increase the likelihood that reengineering efforts will be successful.

During the development of metrics, the following matters must be considered:

- Metrics must yield quantifiable information expressed as percentages, averages, or absolute numbers.
- Data-supporting metrics needs to be readily obtainable.
- Only repeatable processes should be considered for measurement.
- Metrics must be useful for tracking performance and directing resources.

The metrics development process ensures that the metrics are developed with the purpose of identifying causes of poor performance and therefore point to appropriate corrective actions. Organizations can develop and collect metrics of three types:

- Implementation metrics to measure implementation of organization's policies
- Effectiveness or efficiency metrics to measure results of organization's procedures and practices
- Impact metrics to measure business or mission impact of organization's events

(d) CYCLE TIMES. Business processes go through cycles from initiation to completion of defined tasks and activities. Each process has a beginning point and an ending point, and consumes resources (e.g., time, money, people talent, materials, machinery, and energy) to accomplish the defined tasks and activities. The goal is to consume as little of these resources as possible and to complete these tasks and activities as efficiently and effectively as possible. Industrial engineers, known as efficiency experts, can help in establishing and measuring the cycle times. Cycle time measures focus on the "time" dimension, expressed as hours or days.

USES OF CYCLE TIMES IN MARKETING

Cycle times can be used in marketing to develop new products (time to market), improve existing products, and deliver new products to the markets.

Out of all the resources mentioned, time is a limited and critical resource because lost time cannot be regained. Organizations who can beat the time clock are clear winners in the highly competitive global business environment. The goal is to become the best in the best-in-class group using shorter cycle times. The shorter the cycle time, the better—more work can be accomplished in less time. Cycle times measure the elapsed time between two or more successive events, the time taken to reach from Point A to Point B and back, or the time taken to complete a task from beginning to end.

If the cycle times are found to be unacceptable (i.e., too long), management should do the following to make them acceptable (i.e., shorter):

- Streamline the upstream and downstream work processes through work-study analysis, process-flow analysis, flowcharting analysis, and process-mapping analysis.
- Simplify the work processes by eliminating or decreasing non-value-added activities, deleting duplicate tasks, and removing unnecessary handoffs.
- Standardize the work processes by issuing new policies, procedures, equipment, systems, and tools and techniques for organization-wide use.
- Institutionalize the standardized work processes across the entire organization as pilot projects or in phases (i.e., a phased rollout).

The sequence of steps needed to reduce the cycle time in the value chain is:

Streamline ⟶ Simplify ⟶ Standardize ⟶ Institutionalize

(e) STANDARDS. As said earlier, standards include national, regional, international, organizational, industry, and professional standards. For example, a national standard such as the U.S. Malcolm Baldrige criteria for performance excellence results are grouped into five sets of performance measures as follows:

1. **Customer-Focused Performance.** This set includes measures such as customer satisfaction and dissatisfaction, gains and losses of customers and their accounts, and customer complaints and warranty claims. Other measures include perceived

value, loyalty, positive referral, and customer relationship building. Service quality and cycle times are key satisfaction measures for distributors, while product quality is the principal satisfaction indicator for end users.

2. **Financial and Market Performance.** This set includes financial measures such as return on equity, return on investment, operating profit, pretax profit margin, asset utilization, and earnings per share. Market measures include market share size and percentage of new product sales.
3. **Human Resource Performance.** This set includes measures such as employee turnover, absenteeism, satisfaction, training effectiveness, grievances, safety, and suggestion rates.
4. **Supplier and Partner Performance.** This set includes measures such as quality, delivery, price, and cost savings.
5. **Organizational Effectiveness.** This set includes measures such as lead times, machine setup times, time to market, product/process yields, production flexibility, mean time between corrective maintenance, productivity, community services, defects and error rates, regulatory and legal compliance, new-product introductions, safety, and environmental (e.g., pollution).

(f) PRESENTATION TOOLS. All the effort expended on selecting the right type of performance indicators and measuring them will be of no use if their results are not presented to management in a meaningful way that permits making the right decisions. Functional managers and project managers present progress on performance indicators (e.g., scorecards, cycle times, and metrics) to senior managers and executives periodically through reports and memorandums. Leading organizations present these progress results using visual aids so that senior managers and executives can comprehend the data and information clearly and identify the trends quickly.

Presentation tools or visual aids can be classified as soft tools and hard tools. Soft tools include problem-solving tools (Chapter 7, 7.9) and decision-making tools (Chapter 7, 7.9), and listening, negotiating, and communicating tools. Hard tools include quality-control tools (Chapter 7, 7.9), quality-management tools (Chapter 7, 7.9), business-process management tools (Chapter 8, 8.5), and charting tools. The latter are discussed here.

The charting tools include tabular, column, Gantt, pie, line, and layer charts. The tabular chart is used to represent items of interest and requires a fair amount of study in order to grasp the full meaning of the figures. The column chart is most commonly used for demonstrating a comparison between two or more things. The Gantt chart is a bar chart used for milestone scheduling, with each milestone bearing start and completion dates. The pie chart is used to represent a 100 percent total of two or more items. The line chart is exceptionally impressive when comparing several things but could present a visual problem if the comparisons are too many or too close in relation to one another. The layer chart is linear in appearance but has a different representation. It depicts the accumulation of individual facts stacked one over the other to create the overall total. This chart is more complex than the others because it illustrates many more facts.

(g) BUSINESS VELOCITY AND CYCLE TIME. Velocity refers to speed and rate of turnover of something tangible, such as inventory and money currency. As said earlier, cycle time is the time taken to complete a task from the beginning to the end.

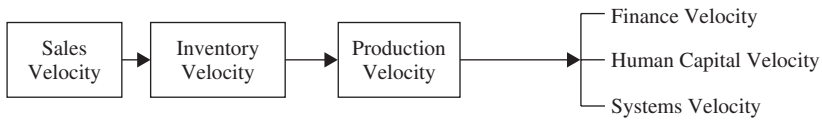

Exhibit 1.1 Business Velocities for Manufacturing Industries

"Time" is the common element between velocity and cycle time and connects them,. Let us look at the velocity concept in two business settings: manufacturing industries and service industries. Exhibit 1.1 and Exhibit 1.2 present business velocities.

For manufacturing industries, as sales are increasing (sales velocity), inventory is depleted quickly (inventory velocity), which should be filled with increased production (production velocity). Money needs to be invested to support the increased production in terms of buying raw materials, parts, and components, and paying for the workforce (finance velocity). More employees may need to be hired to meet the increased production levels (human capital velocity). All these velocities in aggregate may require developing new systems or modifying the existing systems, whether manual or automated (systems velocity). The goal is to synchronize these velocities in a cohesive manner. The same logic applies to pure service industries except that they have no inventories to sell.

When sales velocity is increasing (i.e., more sales), production velocity should also be increasing (i.e., more production), with the two in synchronization with each other. However, longer cycle times for specific internal tasks and operations within the production department can delay producing the required quantities of goods, thus preventing meeting the sales velocity demand. This requires optimizing the cycle times for all of the internal tasks and operations within the production department prior to handling the production velocity. Cycle times should not become a bottleneck to achieving the production velocity or any type of velocity.

In summary, velocities and cycle times are solidly linked in that shorter cycle times increase any type of business velocity, which can then increase revenues, decrease costs, and increase profits. For example, sales velocity, in part, cannot be increased if time-to-market cycle time for introducing new products is taking longer.

Cycle time measures are discussed in marketing and sales, manufacturing and service, finance, human resources, and information technology chapters, with attention to sales velocity, inventory and production or service velocity, finance velocity, human capital velocity, and systems velocity, respectively.

1.4 BEST-PRACTICES MANAGEMENT CAPABILITY MATURITY MODEL

The best-practices management capability maturity model consists of five stages or levels needed to improve the efficiency and effectiveness of business processes through proper implementation of best practices. These five stages are (1) select, (2) implement, (3) measure, (4) evaluate, and (5) institutionalize. When an organization reaches the institutionalization stage, it is a positive reflection of management's capabilities in properly implementing best practices. This model provides a simple and practical framework that can be standardized for organization-wide implementation of best practices.

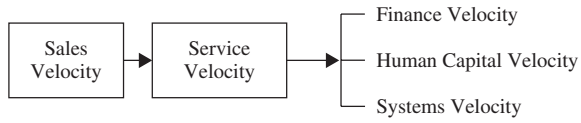

EXHIBIT 1.2 BUSINESS VELOCITIES FOR SERVICE INDUSTRIES

(a) STAGE 1. SELECT. This stage first identifies a business unit, division, or group needing improvement in performance. It can also identify a specific business function (e.g., accounts payable) or a process within the business function (e.g., vendor invoice processing) that needs improvement. Other examples of topics for selection include (1) freight audit and payment, (2) travel and entertainment expense management, (3) payroll processing by an outsourcing vendor, (4) customer-claims processing by an insurance company, and (5) patient bill estimation and processing by a hospital.

Appoint a project manager to manage the best practices project from start to finish. The project manager should prepare an inventory of all business processes that need improvement and should prioritize them with the approval of senior management. The project manager should issue detailed status reports periodically to all affected managers and summarized status reports to senior managers describing the progress, problems, and issues.

As part of a pilot project, the championing or sponsoring functional manager should select a process or function within his responsibility that is easy to address and that is in need of the most improvement. The idea is to demonstrate positive results to senior management and to convince skeptics among the other functional managers. Lessons learned from the pilot project can then be applied to the other parts of the organization.

The project team, consisting of the project manager and the functional manager and his staff, should then search for organizations that were successful in implementing the best practices in the chosen function or process. Benchmark results can be used to develop or modify best practices. Conduct the benchmark research to identify best-in-class public and private organizations (within an industry or across industries) that benefited from best practices. Obtain the benchmark study results, reports, and related information from reputable sources. Due to copyright restrictions, obtaining written permissions from the benchmark organizations to use their best practices methods is a good legal practice. Prior to implementation, it is important to obtain senior management support and commitment by presenting a developed business case to them.

SOURCES FOR BEST PRACTICES AND BENCHMARKING INFORMATION

Internet search engines (for example, www.google.com) can provide a vast amount of information when searched using ''Best Practices'' and ''Benchmarking.'' They provide the names of organizations and institutions sharing information in the form of white papers, case studies, methods, tools, and articles, along with their Web site information.

The project team can also contact industry trade associations, professional organizations, and governmental agencies for additional information. For example, the American Marketing Association

(AMA), a professional organization representing marketers, provides ''Best Practices in Marketing'' in its Web site (www.marketingpower.com). The project team should contact several sources until it finds the right organization that can help its project.

(b) STAGE 2. IMPLEMENT. This stage incorporates into an organization's day-to-day work habits and routines the general best practices available outside the organization. The task is not easy. In fact, many organizations fail in their implementation efforts due to people problems (i.e., people risk). Finalize what benchmark results and best practices are appropriate to the business function or process within a business unit, division, or group. The project team tailors these general best practices into company-specific best practices in terms of developing policies, procedures, tools, and internal systems. Identify resources (e.g., time and people) needed to achieve proper implementation of best practices.

A full implementation of best practices will not be efficient and effective until a business process is streamlined, simplified, standardized, and institutionalized. Otherwise, it is like throwing good money at bad things. To make things better, inefficient and ineffective business processes must be completely fixed prior to implementation of best practices.

The business case should include goals and objectives to be achieved from the implementation of best practices along with expected performance measures (e.g., scorecards, metrics, cycle times, and standards).

(c) STAGE 3. MEASURE. This stage compares actual performance levels resulting from the implementation efforts against the defined performance indicators and measures. The performance measures identified in the business case from the second stage are compared with the generally accepted indicators and measures, such as scorecards, metrics, cycle times, and standards.

This measurement exercise identifies gaps in performance between the actual levels and the expected levels. Management can then develop appropriate remedial plans and take action steps to close the gaps.

(d) STAGE 4. EVALUATE. This stage requires a careful evaluation of progress from stages one through three and takes a snapshot of the progress to date. This stage requires honest feedback from all employees involved in the best-practices project implementation in terms of its strengths and weaknesses. It asks specific questions, such as (1) whether the defined goals and objectives were achieved, (2) whether the defined benefits and gains were achieved, (3) what were the factors that led to success, (4) what went wrong, (5) what lessons were learned, and (6) what worked and what did not, and why. The evaluation should focus on the overall management system for improvement and not on people to blame. It also looks at whether the benefits and gains can be sustainable and repeatable in other business units, divisions, or groups.

If the evaluation turns out to be negative, with many problems surfacing that were not discovered in the previous stages, management should rethink and reassess the situation and replan and proceed further with caution. Or management could direct the project team to start from the first stage by revisiting other best-in-class organizations and obtaining different benchmark study results and reports from other sources.

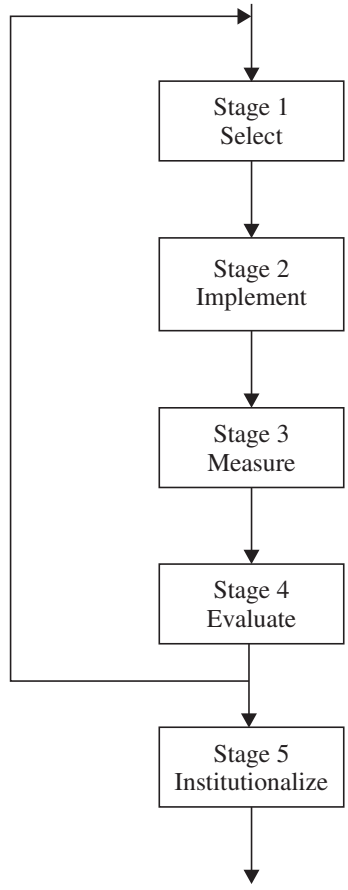

Exhibit 1.3 Five Stages of the Best-Practices Management Capability Maturity Model

(e) STAGE 5. INSTITUTIONALIZE. This stage takes a "big picture" approach to the best practices for continuous improvement throughout the organization. If the evaluation from the previous stage turns out to be positive in a specific business area and the benefits and gains are sustainable and repeatable in other business units, divisions, or groups, management should streamline, simplify, and standardize the business processes related to the selected business area. Management can then institutionalize the standardized best practices by rolling out to the other parts of the business units, divisions, and groups of businesses. Organizations can realize full potential benefits from best practices only after they successfully complete this stage.

Exhibit 1.3 presents a pictorial view of the five stages of the Best-Practices Management Capability Maturity Model along with their connections.

Stages three and four can proceed in parallel while the other stages can follow the prescribed sequence. Notice that stage four loops back to stage one.

Additional Resources

Eckerson, Wayne W. *Performance Dashboards*. Hoboken, NJ: John Wiley & Sons, 2005.

Niven, Paul R. *Balanced Scorecard Step-by-Step*, second edition. Hoboken, NJ: John Wiley & Sons, 2006.

Paladino, Bob. *Five Key Principles of Corporate Performance Management*. Hoboken, NJ: John Wiley & Sons, 2007.

Parmenter, David. *Key Performance Indicators (KPIs): Developing, Implementing, and Using KPIs*. Hoboken, NJ: John Wiley & Sons, 2007.

Smith, Ralph S. *Business Process Management and the Balanced Scorecard*. Hoboken, NJ: John Wiley & Sons, 2006.

Notes

1. Best Practices Methodology: A New Approach for Improving Government Operations (GAO/NSIAD-95-154), U.S. General Accounting Office (GAO), Washington, DC, May 1995.
2. Portions of this section have been reprinted by permission of Harvard Business School Press. Robert S. Kaplan and David P. Norton, *The Strategy-Focused Organization: How Balanced Scorecard Companies Thrive in the New Business Environment* (Boston, MA: Harvard Business School Press, 2001), 23, 102, 103, 204, and 361. Copyright © 2000 by the Harvard Business School Press Corp. All rights reserved.

CHAPTER 2

CORPORATE-GOVERNANCE BEST PRACTICES

2.1 OVERVIEW

Corporate governance sets the right tone and proper stage for the entire corporation. Governance principles are presented here from two different perspectives: that of the Organization for Economic Co-operation and Development (OECD), for an international viewpoint; and that of Business Roundtable, for the U.S. viewpoint.

(a) DEFINITION. While there is no standard definition of corporate governance, it can broadly be understood to refer to the system by which companies are directed and controlled, including the roles of the board of directors, management, shareholders, and other stakeholders. Corporate governance provides the structure through which the objectives of the company are set and the means of attaining those objectives and monitoring performance are determined.

A weak form of corporate governance is one of the root causes of many problems that corporate management faces today. Corporate governance and corporate ethics should support corporate management.

(b) OECD'S CORPORATE GOVERNANCE PRINCIPLES. Since 1999, the OECD's *Principles of Corporate Governance* has become an international benchmark for policy makers, investors, corporations, and other stakeholders worldwide. The OECD, located in Paris, France, has 30 member countries and works to improve economic growth and employment, the world economy, and world trade. The OECD has developed the following six principles of corporate governance:[1]

PRINCIPLE I: ENSURING THE BASIS FOR AN EFFECTIVE CORPORATE GOVERNANCE FRAMEWORK

The corporate governance framework should promote transparent and efficient markets, be consistent with the rule of law, and clearly articulate the division of responsibilities among different supervisory, regulatory, and enforcement authorities.

A. The corporate governance framework should be developed with a view to its impact on overall economic performance, market integrity, and the incentives it creates for market participants and the promotion of transparent and efficient markets.
B. The legal and regulatory requirements that affect corporate governance practices in a jurisdiction should be consistent with the rule of law, transparent, and enforceable.

C. The division of responsibilities among different authorities in a jurisdiction should be clearly articulated, and ensure that the public interest is served.
D. Supervisory, regulatory, and enforcement authorities should have the authority, integrity, and resources to fulfill their duties in a professional and objective manner. Moreover, their rulings should be timely, transparent, and fully explained.

PRINCIPLE II: THE RIGHTS OF SHAREHOLDERS AND KEY OWNERSHIP FUNCTIONS

The corporate governance framework should protect and facilitate the exercise of shareholders' rights.

A. Basic shareholder rights should include the rights to (1) secure methods of ownership registration, (2) convey or transfer shares, (3) obtain relevant and material information on the corporation on a timely and regular basis, (4) participate and vote in general shareholder meetings, (5) elect and remove members of the board; and (6) share in the profits of the corporation.
B. Shareholders should have the right to participate in, and to be sufficiently informed on, decisions concerning fundamental corporate changes such as (1) amendments to the statutes, articles of incorporation, or similar governing documents of the company, (2) the authorization of additional shares, and (3) extraordinary transactions, including the transfer of all or substantially all assets, that in effect result in the sale of the company.
C. Shareholders should have the opportunity to participate effectively and vote in general shareholder meetings and should be informed of the rules, including voting procedures, that govern shareholder meetings.
    1. Shareholders should be furnished with sufficient and timely information concerning the date, location, and agenda of general meetings, as well as full and timely information regarding the issues to be decided at the meeting.
    2. Shareholders should have the opportunity to ask questions to the board, including questions relating to the annual external audit, to place items on the agenda of general meetings, and to propose resolutions, subject to reasonable limitations.
    3. Effective shareholder participation in key corporate governance decisions, such as the nomination and election of board members, should be facilitated. Shareholders should be able to make their views known on the remuneration policy for board members and key executives. The equity component of compensation schemes for board members and employees should be subject to shareholder approval.
    4. Shareholders should be able to vote in person or in absentia, and equal effect should be given to votes whether cast in person or in absentia.
D. Capital structures and arrangements that enable certain shareholders to obtain a degree of control disproportionate to their equity ownership should be disclosed.
E. Markets for corporate control should be allowed to function in an efficient and transparent manner.
    1. The rules and procedures governing the acquisition of corporate control in the capital markets, and extraordinary transactions such as mergers, and sales of substantial portions of corporate assets, should be clearly articulated and disclosed so that investors understand their rights and recourse. Transactions should occur at transparent prices and under fair conditions that protect the rights of all shareholders according to their class.
    2. Antitakeover devices should not be used to shield management and the board from accountability.

F. The exercise of ownership rights by all shareholders, including institutional investors, should be facilitated.
   1. Institutional investors acting in a fiduciary capacity should disclose their overall corporate governance and voting policies with respect to their investments, including the procedures that they have in place for deciding on the use of their voting rights.
   2. Institutional investors acting in a fiduciary capacity should disclose how they manage material conflicts of interest that may affect the exercise of key ownership rights regarding their investments.

G. Shareholders, including institutional shareholders, should be allowed to consult with each other on issues concerning their basic shareholder rights as defined in the Principles, subject to exceptions to prevent abuse.

PRINCIPLE III: THE EQUITABLE TREATMENT OF SHAREHOLDERS

The corporate governance framework should ensure the equitable treatment of all shareholders, including minority and foreign shareholders. All shareholders should have the opportunity to obtain effective redress for violation of their rights.

A. All shareholders of the same series of a class should be treated equally.
   1. Within any series of a class, all shares should carry the same rights. All investors should be able to obtain information about the rights attached to all series and classes of shares before they purchase. Any changes in voting rights should be subject to approval by those classes of shares that are negatively affected.
   2. Minority shareholders should be protected from abusive actions by, or in the interest of, controlling shareholders acting either directly or indirectly, and should have effective means of redress.
   3. Votes should be cast by custodians or nominees in a manner agreed upon with the beneficial owner of the shares.
   4. Impediments to cross-border voting should be eliminated.
   5. Processes and procedures for general shareholder meetings should allow for equitable treatment of all shareholders. Company procedures should not make it unduly difficult or expensive to cast votes.

B. Insider trading and abusive self-dealing should be prohibited.
C. Members of the board and key executives should be required to disclose to the board whether they, directly, indirectly, or on behalf of third parties, have a material interest in any transaction or matter directly affecting the corporation.

PRINCIPLE IV: THE ROLE OF STAKEHOLDERS IN CORPORATE GOVERNANCE

The corporate governance framework should recognize the rights of stakeholders established by law or through mutual agreements and encourage active cooperation between corporations and stakeholders in creating wealth, jobs, and the sustainability of financially sound enterprises.

A. The rights of stakeholders that are established by law or through mutual agreements are to be respected.
B. Where stakeholder interests are protected by law, stakeholders should have the opportunity to obtain effective redress for violation of their rights.

C. Performance-enhancing mechanisms for employee participation should be permitted to develop.
D. Where stakeholders participate in the corporate governance process, they should have access to relevant, sufficient, and reliable information on a timely and regular basis.
E. Stakeholders, including individual employees and their representative bodies, should be able to freely communicate their concerns about illegal or unethical practices to the board and their rights should not be compromised for doing this.
F. The corporate governance framework should be complemented by an effective, efficient insolvency framework and by effective enforcement of creditor rights.

PRINCIPLE V: DISCLOSURE AND TRANSPARENCY

The corporate governance framework should ensure that timely and accurate disclosure is made on all material matters regarding the corporation, including the financial situation, performance, ownership, and governance of the company.

A. Disclosure should include, but not be limited to, material information on:
    1. The financial and operating results of the company
    2. Company objectives
    3. Major share ownership and voting rights
    4. Remuneration policy for members of the board and key executives, and information about board members, including their qualifications, the selection process, other company directorships and whether they are regarded as independent by the board
    5. Related party transactions
    6. Foreseeable risk factors
    7. Issues regarding employees and other stakeholders
    8. Governance structures and policies, in particular, the content of any corporate governance code or policy and the process by which it is implemented
B. Information should be prepared and disclosed in accordance with high-quality standards of accounting and financial and nonfinancial disclosure.
C. An annual audit should be conducted by an independent, competent and qualified, auditor in order to provide an external and objective assurance to the board and shareholders that the financial statements fairly represent the financial position and performance of the company in all material respects.
D. External auditors should be accountable to the shareholders and owe a duty to the company to exercise due professional care in the conduct of the audit.
E. Channels for disseminating information should provide for equal, timely, and cost-efficient access to relevant information by users.
F. The corporate governance framework should be complemented by an effective approach that addresses and promotes the provision of analysis or advice by analysts, brokers, rating agencies, and others, that is relevant to decisions by investors, free from material conflicts of interest that might compromise the integrity of their analysis or advice.

PRINCIPLE VI: THE RESPONSIBILITIES OF THE BOARD

The corporate governance framework should ensure the strategic guidance of the company, the effective monitoring of management by the board, and the board's accountability to the company and the shareholders.

A. Board members should act on a fully informed basis, in good faith, with due diligence and care, and in the best interest of the company and the shareholders.
B. Where board decisions may affect different shareholder groups differently, the board should treat all shareholders fairly.
C. The board should apply high ethical standards. It should take into account the interests of all stakeholders.
D. The board should fulfill certain key functions, including
    1. Reviewing and guiding corporate strategy, major plans of action, risk policy, annual budget, and business plans; setting performance objectives; monitoring implementation and corporate performance; and overseeing major capital expenditures, acquisitions, and divestitures
    2. Monitoring the effectiveness of the company's governance practices and making changes as needed
    3. Selecting, compensating, monitoring, and—when necessary—replacing key executives and overseeing succession planning
    4. Aligning key executive and board remuneration with the longer-term interests of the company and its shareholders
    5. Ensuring a formal and transparent board nomination and election process
    6. Monitoring and managing potential conflicts of interest of management, board members, and shareholders, including misuse of corporate assets and abuse in related party transactions
    7. Ensuring the integrity of the corporation's accounting and financial reporting systems, including the independent audit, and that appropriate systems of control are in place, in particular, systems for risk management, financial and operational control, and compliance with the law and relevant standards
    8. Overseeing the process of disclosure and communication
E. The board should be able to exercise objective independent judgment on corporate affairs.
    1. Boards should consider assigning a sufficient number of non–executive board members capable of exercising independent judgment to tasks where there is a potential for conflict of interest. Examples of such key responsibilities are ensuring the integrity of financial and nonfinancial reporting, the review of related party transactions, nomination of board members and key executives, and board remuneration.
    2. When committees of the board are established, their mandate, composition, and working procedures should be well defined and disclosed by the board.
    3. Board members should be able to commit themselves effectively to their responsibilities.
F. In order to fulfill their responsibilities, board members should have access to accurate, relevant, and timely information.

(c) BUSINESS ROUNDTABLE'S CORPORATE GOVERNANCE PRINCIPLES Business Roundtable supports the following eight guiding principles as part of good corporate governance practices:[2]

1. The paramount duty of the board of directors of a public corporation is to select a chief executive officer (CEO) and to oversee the CEO and senior management in the competent and ethical operation of the corporation on a day-to-day basis.
2. It is the responsibility of management to operate the corporation in an effective and ethical manner to produce value for shareholders. Senior management is expected

to know how the corporation earns its income and what risks the corporation is undertaking in the course of carrying out its business. The CEO and board of directors should set a "tone at the top" that establishes a culture of legal compliance and integrity. Management and directors should never put personal interests ahead of or in conflict with the interests of the corporation.

3. It is the responsibility of management, under the oversight of the audit committee and the board, to produce financial statements that fairly present the financial condition and results of operations of the corporation and to make the timely disclosures investors need to assess the financial and business soundness and risks of the corporation.
4. It is the responsibility of the board, through its audit committee, to engage an independent accounting firm to audit the financial statements prepared by management, issue an opinion that those statements are fairly stated in accordance with Generally Accepted Accounting Principles (GAAP), and oversee the corporation's relationship with the outside auditor.
5. It is the responsibility of the board, through its corporate governance committee, to play a leadership role in shaping the corporate governance of the corporation. The corporate governance committee also should select and recommend to the board qualified director candidate for election by the corporation's shareholders.
6. It is the responsibility of the board, through its compensation committee, to adopt and oversee the implementation of compensation policies, establish goals for performance-based compensation, and determine the compensation of the CEO and senior management.
7. It is the responsibility of the board to respond appropriately to shareholder's concerns.
8. It is the responsibility of the corporation to deal with its employees, customers, suppliers, and other constituencies in a fair and equitable manner.

These eight responsibilities and others are critical to the functioning of the modern public corporation and the integrity of the public markets. No law or regulation alone can be a substitute for the voluntary adherence to these principles by corporate directors and management.

Business Roundtable continues to believe that corporate governance should be enhanced through conscientious and forward-looking action by a business community that focuses on generating long-term shareholder value with the highest degree of integrity.

The principles discussed here are intended to assist corporate management and boards of directors in their individual efforts to implement best practices of corporate governance, as well as to serve as guideposts for the public dialogue on evolving governance standards.

(d) EMPLOYEE REPORTING RELATIONSHIPS. Improperly defining and practicing employee reporting relationships is often at the root of problems involving corporate governance, control, or ethics. Improper reporting relationships between and among a company's C-level executives create control-related problems and pose ethical dilemmas due to conflict of interest, lack of separation of duties, and lack of independence and objectivity. Incompatible job functions and improper separation of duties can lead to fraud, collusion, and other irregularities. Corporate goal congruence is at risk when individual goals and interests dominate and conflict with the goals of the corporation.

Proper organizational structure and reporting relationships can enforce clear lines of responsibility and accountability throughout the organization.

Below is a list of common and generic C-level executive titles, which could vary from organization to organization with more or fewer titles or even different titles in place. Most C-level executives are Vice Presidents or Directors of a business division or group. The following describes the proper and improper reporting relationships between and among the C-level executives.

- The Chief Executive Officer (CEO) should report to the board of directors, can assume the role of the President, but cannot assume the role of the chairperson of the board or the role of the CFO. A non–executive board member should assume the role of the chairperson of the board.
- The Chief Financial Officer (CFO) should report to the CEO or to the Executive Vice President of Finance. The CFO cannot assume the role of the CEO.
- The Chief Accounting Officer, or Corporate Controller, or Treasurer should report to the CFO. A business unit/division controller should not directly report to the business unit/division general manager. Such a controller should functionally report to the Corporate Controller and administratively report to the business unit/division general manager.
- The Chief Marketing Officer (CMO) should report to the CEO only.
- The Chief Audit Executive (CAE) should report functionally to the audit committee of the board and administratively to the CEO, not to the CFO or Executive Vice President of Finance
- The Chief Administrative Officer (CAO) should report to the Executive Vice President or Chief People (Human Resource) Officer, not to the CFO.
- The Chief Legal Officer (CLO) should report to the CEO or the President of the firm, not to the Executive Vice President of Finance or the CAO. A business unit/division legal counsel should not directly report to the business unit/division head. Such a legal counsel should functionally report to the Corporate Legal Officer and administratively report to the business unit/division head.
- The Chief Governance Officer (CGO) should report to the CEO or CLO or the Corporate General Counsel, not to the CAE or CFO.
- The Chief Operating Officer (COO) or Chief Operations Officer should report to the CEO, not to the CAO. A business unit/division's manufacturing manager should report to the Chief Manufacturing Officer, not to the business unit/division's general manager.
- The Chief Manufacturing Officer or Chief Service Officer should report directly to the COO, not to the business unit/division general manager.
- The Chief Information Officer (CIO) should report to the CEO, not to the CFO or Executive Vice President of Finance, or COO, CAO, or Controller. A business unit/division information technology (IT) Manager should not directly report to the business unit/division head. Such an IT Manager should functionally report to the CIO or its equivalent and administratively report to the business unit/division head.
- The Chief Research and Development (R&D) Officer should report to the CEO or COO if the organization's focus is on research and development, not report to the Chief Manufacturing Officer.

- The Chief Risk Officer (CRO) should report to the CEO or CGO, not to the CFO or Treasurer because risk is not limited to finance or treasury function as it is enterprise-wide
- The Chief Ethics Officer should report to the CGO or to the CLO or to the Corporate General Counsel, not to the CAE or the CFO.
- The Chief Globalization Officer should report to the CEO, not to the CMO or COO.
- The Chief People Officer should report to the CEO, not to the CAO or the CFO.
- The Chief Learning Officer should report to the Chief People Officer, not report to the Chief Communications Officer, CIO, or CFO.
- The Chief Communications Officer should report to the CGO.
- The Chief Quality Officer should report to the CEO or COO if the organization's focus is on quality, not report to the Chief Manufacturing Officer.
- The Chief Procurement Officer should report to the COO, not report to the Chief Manufacturing Officer or Chief Service Officer.
- The Chief Design Officer should report to the COO, not report to the Chief Manufacturing Officer or Chief Service Officer.
- The Chief Technology Officer should report to the COO, not report to the Chief Manufacturing Officer or Chief Service Officer.
- The Chief Compliance Officer should report to the CGO, not report to the CFO or CAE.

Having so many C-level executives directly reporting to the CEO is a challenging administrative task for the CEO to handle on a daily basis, especially when the CEO's time is a limited and critical resource. Some organizations have established Executive Vice President (EVP) or Senior Vice President (SVP) positions where some C-level executives directly report to the EVP or SVP in order to reduce the workload of the CEO. For example, the CFO, the Chief Accounting Officer (the Controller), the Chief Treasurer, and the Chief Administrative Officer directly reports to the EVP of Finance.

In a similar context, the U.S. President, who is the CEO of the country, also has many S-level executives (e.g., Secretary of Defense) directly reporting to the President. Goal congruence, consistency, harmony, and a single and collective voice are the primary benefits accruing to private or public sector organizations resulting from this type of wide span of control.

Both the CEO and the Senior Executive Management must ensure that employee reporting relationships in the management hierarchy below that of the C-level executives (e.g., group/division heads, general managers, middle-level managers, and lower-level managers) is structured in such a way to prevent conflict of interest, goal congruence, control, and ethical problems.

2.2 ROLES AND RESPONSIBILITIES OF THE BOARD OF DIRECTORS

(a) OVERVIEW. In this section the roles of the board of directors are presented from two different perspectives: that of the OECD, for an international viewpoint; and that of Business Roundtable, for the U.S. viewpoint.

(b) OECD'S ROLES OF THE BOARD OF DIRECTORS. The roles and responsibilities of the board of directors are described in terms of six topics: monitoring of management, duty of care and loyalty, ethical standards, key functions, corporate affairs, and access to information.

(i) Monitoring of Management. Together with guiding corporate strategy, the board is primarily responsible for monitoring managerial performance and achieving an adequate return for shareholders, while preventing conflicts of interest and balancing competing demands on the corporation. In order for boards to effectively fulfill their responsibilities, they must be able to exercise objective and independent judgment. Another important board responsibility is to oversee systems designed to ensure that the corporation obeys applicable laws, including tax, competition, labor, environmental, equal opportunity, and health and safety laws. In some countries, companies have found it useful to explicitly articulate the responsibilities that the board assumes and those for which management is accountable.[3]

The board is not only accountable to the company and its shareholders but also has a duty to act in their best interests. In addition, boards are expected to take due regard of, and deal fairly with, other stakeholder interests, including those of employees, creditors, customers, suppliers, and local communities (i.e., social responsibility).

(ii) Duty of Care and Loyalty. The two key elements of the fiduciary duty of board members include duty of care and the duty of loyalty. The *duty of care* requires board members to act on a fully informed basis, in good faith, with due diligence and care. In some jurisdictions there is a standard of reference, which is the behavior that a reasonably prudent person would exercise in similar circumstances. In nearly all jurisdictions, the duty of care does not extend to errors of business judgment so long as board members are not grossly negligent and a decision is made with due diligence. Good practice takes this to mean that they should be satisfied that key corporate information and compliance systems are fundamentally sound and underpin the key monitoring role of the board. In many jurisdictions this meaning is already considered an element of the duty of care, while in others securities regulations or accounting standards require it.

The *duty of loyalty* is of central importance, since it underpins effective implementation of other principles such as the equitable treatment of shareholders, monitoring of related-party transactions, and the establishment of remuneration policy for key executives and board members. It is also a key principle for board members who are working within the structure of a group of companies: Even though a company might be controlled by another enterprise, the duty of loyalty for a board member relates to the company and all its shareholders and not to the controlling company of the group. Where board decisions may affect different shareholder groups differently, the board should treat all shareholders fairly.

(iii) Ethical Standards. The board has a key role in setting the ethical tone of a company, not only by its own actions, but also in appointing and overseeing key executives and consequently the management in general. High ethical standards are in the long-term interests of the company as a means to make it credible and trustworthy, not only in day-to-day operations but also with respect to longer-term commitments. To make the objectives of the board clear and operational, many companies have found it useful

to develop company codes of conduct based on, inter alia, professional standards and sometimes broader codes of behavior.

Company-wide codes serve as a standard for conduct by both the board and key executives, setting the framework for the exercise of judgment in dealing with varying and often conflicting constituencies. At a minimum, the ethical code should set clear limits on the pursuit of private interests, including dealings in the shares of the company. An overall framework for ethical conduct goes beyond compliance with the law, which should always be a fundamental requirement.

(iv) Key Functions. An area of increasing importance for boards, and one closely related to corporate strategy, is risk policy. The policy involves specifying the types and degree of risk that a company is willing to accept in pursuit of its goals. It is thus a crucial guideline for management in addressing risks to meet the company's desired risk profile.

Monitoring of governance by the board also includes continuous review of the internal structure of the company to ensure that there are clear lines of accountability for management throughout the organization. In addition to requiring the monitoring and disclosure of corporate governance practices on a regular basis, a number of countries have moved to recommend or indeed mandate self-assessment by boards of their performance as well as performance reviews of individual board members and the CEO/Chairman.

In an increasing number of countries it is regarded as good practice for boards to develop and disclose a remuneration policy statement covering board members and key executives. Such policy statements specify the relationship between remuneration and performance, and include measurable standards that emphasize the longer-run interest of the company over short-term considerations. Policy statements generally tend to set conditions for payments to board members for extra-board activities, such as consulting. They also often specify terms to be observed by board members and key executives about holding and trading the stock of the company, and the procedures to be followed in granting and repricing options. In some countries, a policy statement will also cover the payments to be made when terminating the contract of an executive.

It is an important function of the board to oversee the internal control systems covering financial reporting and the use of corporate assets, and to guard against abusive related-party transactions. These functions are sometimes assigned to the internal auditor, which should maintain direct access to the board. Where other corporate officers are responsible, such as the general counsel, it is important that they maintain reporting responsibilities similar to those of the internal auditor.

In fulfilling its control oversight responsibilities, it is important for the board to encourage the reporting of unethical or unlawful behavior without fear of retribution. The existence of a company code of ethics should aid this process, which should be underpinned by legal protection for the individuals concerned. In a number of companies, either the audit committee or an ethics committee is specified as the contact point for employees who wish to report concerns about unethical or illegal behavior that might also compromise the integrity of financial statements.

Ensuring the integrity of the essential reporting and monitoring systems will require the board to set and enforce clear lines of responsibility and accountability throughout the organization. The board will also need to ensure that there is appropriate

oversight by senior management. One way of doing this is through an internal-audit function directly reporting to the board. In some jurisdictions it is considered good practice for the internal auditors to report to an independent audit committee of the board or an equivalent body that is also responsible for managing the relationship with the external auditor, thereby allowing a coordinated response by the board. It should also be regarded as good practice for this committee, or the equivalent body, to review and report to the board the most critical accounting policies, which are the basis for financial reports. However, the board should retain final responsibility for ensuring the integrity of the reporting systems. Some countries have provided for the chair of the board to report on the internal control process.

Companies are also well advised to set up internal programs and procedures to promote compliance with applicable laws, regulations, and standards, including statutes that make bribing foreign officials a criminal offense. Such compliance programs will also underpin the company's ethical code. To be effective, the incentive structure of the business needs to be aligned with its ethical and professional standards so that adherence to these values is rewarded and breaches of law are met with dissuasive consequences or penalties. Compliance programs should also extend where possible to subsidiaries.

(v) Corporate Affairs. In order to exercise its duties of monitoring managerial performance, preventing conflicts of interest, and balancing competing demands on the corporation, it is essential that the board is able to exercise objective judgment. In the first instance this will mean independence and objectivity with respect to management, a fact that has important implications for the composition and structure of the board. Board independence in these circumstances usually requires that a sufficient number of board members will need to be independent of management. In a number of countries with single-tier board systems, the objectivity of the board and its independence from management may be strengthened by the separation of the role of the CEO and that of the chairperson of the board, or, if these roles are combined, by designating a lead non–executive director to convene or chair sessions of the outside directors. Separation of these two positions may be regarded as good practice, as it can help to achieve an appropriate balance of power, increase accountability, and improve the board's capacity for decision making independent of management. The designation of a lead director is also regarded as a good practice alternative in some jurisdictions. Such mechanisms can also help to ensure high-quality governance of the enterprise and the effective functioning of the board. A company secretary may, in some countries, support the Chairperson or lead director. In the case of two-tier board systems, consideration should be given to whether corporate governance concerns might arise if the head of the lower board traditionally becomes the Chairman of the supervisory board upon retirement.

Independent board members can contribute significantly to the decision making of the board. They can bring an objective view to the evaluation of the performance of the board and management. In addition, they can play an important role in areas where the interests of management, the company, and its shareholders may diverge, such as executive remuneration, succession planning, changes of corporate control, takeover defenses, large acquisitions, and the internal-audit function. In order for them to play this key role, it is desirable that boards declare who they consider to be independent and the criterion for this judgment.

Service on too many boards can interfere with the performance of board members. Companies may wish to consider whether multiple board memberships by the same person are compatible with effective board performance and disclose the information to shareholders. Some countries have limited the number of board positions that can be held.

In order to improve board practices and the performance of its members, an increasing number of jurisdictions are now encouraging companies to engage in board training and voluntary self-evaluation that meets the needs of the individual company. This might include requiring that board members acquire appropriate skills upon appointment and thereafter remain abreast of relevant new laws, regulations, and changing commercial (business) risks through in-house training and external courses.

CERTIFICATE OF DIRECTOR EDUCATION

Obtain and maintain the Certificate of Director Education from the National Association of Corporate Directors (NACD) in the United States

(vi) Access to Information. Board members require relevant information on a timely basis in order to support their decision making. Non–executive board members do not typically have the same access to information as key managers within the company do. The contributions of non–executive board members can be enhanced by providing access to certain key managers within the company, such as the company secretary and the internal auditor, and providing recourse to independent external advice at the expense of the company. In order to fulfill their responsibilities, board members should ensure that they obtain accurate, relevant, and timely information.

(c) BUSINESS ROUNDTABLE'S ROLES OF THE BOARD OF DIRECTORS. An effective system of corporate governance provides the framework within which the board and management address their respective responsibilities.[4]

- The business of a corporation is managed under the direction of the corporation's board. The board delegates to the CEO—and, through the CEO, to other senior management—the authority and responsibility for managing the everyday affairs of the corporation. Directors monitor management on behalf of the corporation's shareholders.
- Making decisions regarding the selection, compensation, and evaluation of a well-qualified and ethical CEO is the single most important function of the board. The board also appoints or approves other members of the senior management team.
- Directors bring to the corporation a range of experience, knowledge, and judgment. Directors should not represent the interests of particular constituencies.
- Effective directors maintain an attitude of constructive skepticism; they ask incisive, probing questions and require accurate, honest answers; they act with integrity and diligence; and they demonstrate a commitment to the corporation, its business plans, and long-term shareholder value.
- In performing its oversight function, the board is entitled to rely on the advice, reports, and opinions of management, corporate counsel, auditors, and expert

advisers. The board should assess the qualifications of those it relies on and hold managers and advisers accountable. The board should ask questions and obtain answers about the processes used by managers and the corporation's advisers to reach their decisions and recommendations, as well as about the substance of the advice and reports received by the board. When appropriate, the board and its committees should seek independent advice.

- Given the board's oversight role, shareholders and other constituencies can reasonably expect that directors will exercise vigorous and diligent oversight of a corporation's affairs. However, they should not expect the board to micromanage the corporation's business by performing or duplicating the tasks of the CEO and senior management team.
- The board's oversight function carries with it a number of specific responsibilities in addition to that of selecting and overseeing the CEO. These responsibilities include:
  - *Planning for management development and succession.* The board should oversee the corporation's plans for developing senior management personnel and plan for CEO and senior management succession. When appropriate, the board should replace the CEO or other members of senior management.
  - *Understanding, reviewing, and monitoring the implementation of the corporation's strategic plans.* The board has responsibility for overseeing and understanding the corporation's strategic plans from their inception through their development and execution by management. Once the board reviews a strategic plan, it should regularly monitor implementation of the plan to determine whether it is being implemented effectively and whether changes are needed. The board also should ensure that the corporation's incentive compensation program is aligned with the corporation's strategic plan.
  - *Understanding and approving annual operating plans and budgets.* The board is responsible for understanding, approving, and overseeing the corporation's annual operating plans and for reviewing the annual budgets presented by management. The board should monitor implementation of the annual plans to assess whether they are being implemented effectively and within the limits of approved budgets.
  - *Focusing on the integrity and clarity of the corporation's financial statements and financial reporting.* The board, assisted by its audit committee, should be satisfied that the financial statements and other disclosures prepared by management accurately present the corporation's financial condition and results of operations to shareholders and that they do so in an understandable manner. To achieve accuracy and clarity, the board, through its audit committee, should have an understanding of the corporation's financial statements, including why the accounting principles critical to the corporation's business were chosen, what key judgments and estimates were made by management, and how the choice of principles and the making of these judgments and estimates affect the reported financial results of the corporation.
  - *Advising management on significant issues facing the corporation.* Directors can offer management a wealth of experience and a wide range of perspectives. They provide advice and counsel to management in formal board and

committee meetings, and they are available for informal consultation with the CEO and senior management.

- *Reviewing and approving significant corporate actions.* As required by state corporate law, the board reviews and approves specific corporate actions, such as the election of executive officers, the declaration of dividends, and (as appropriate) the implementation of major transactions. The board and senior management should have a clear understanding of what level or types of decisions require specific board approval.
- *Reviewing management's plans for business resiliency.* As part of its oversight function, the board should designate senior management who will be responsible for business resiliency. The board should periodically review management's plans to address this issue. Business resiliency can include such items as business-risk assessment and management, business continuity, physical and cyber security, and emergency communications.
- *Nominating directors and committee members and overseeing effective corporate governance.* It is the responsibility of the board, through its corporate governance committee, to nominate directors and committee members and oversee the composition, independence, structure, practices, and evaluation of the board and its committees.
- *Overseeing legal and ethical compliance.* The board should set a "tone at the top" that establishes the corporation's commitment to integrity and legal compliance. The board should oversee the corporation's compliance program relating to legal and ethical conduct. In this regard, the board should be knowledgeable about the corporation's compliance program and should be satisfied that the program is effective in preventing and deterring violations. The board should pay particular attention to conflicts of interest, including related party transactions.

2.3 ROLES AND RESPONSIBILITIES OF THE CHIEF EXECUTIVE OFFICER AND OTHER SENIOR EXECUTIVES

The CEO's management style, tone, and leadership skills set the stage for the entire corporation and determine the ultimate success or failure of the organization. The CEO is the linchpin to the strategic-management process in setting the overall direction for the organization and mobilizing resources to accomplish the organization's mission, vision, goals, and objectives.

The CEO is the contact person for the stock markets, investment analysts, and the media, with the CFO also taking part to communicate financial and operational-performance results. The CEO possesses more soft skills than hard skills. The other senior executives' management style and leadership skills should be compatible with that of the CEO to ensure goal congruence.

Business Roundtable defines the following specific roles and responsibilities for the CEO and other senior executives:

- It is the responsibility of the CEO and senior management (senior executives), under the CEO's direction, to operate the corporation in an effective and ethical

manner. As part of its operational responsibility, senior management is charged with the following tasks:

- *Operating the Corporation.* The CEO and senior management run the corporation's day-to-day business operations. With a thorough understanding of how the corporation operates and earns its income, they carry out the corporation's strategic objectives within the annual operating plan and budget, which are reviewed and approved by the board. In making decisions about the corporations' business operations, the CEO considers the long-term interests of the corporation and its shareholders and necessarily relies on the input and advice of others, including senior management and outside advisors. The CEO keeps the board apprised of significant developments regarding the corporation's business operations.
- *Strategic Planning.* The CEO and senior management generally take the lead in strategic planning. They identify and develop strategic plans for the corporation, present those plans to the board, implement the plans once board review is completed, and recommend and carry out changes to the plans as necessary.
- *Annual Operating Plans and Budgets.* With the corporation's overall strategic plans in mind, senior management develops annual operating plans and budgets for the corporation and presents the plans and budgets to the board. Once the board has reviewed and approved the plans and budgets, the management team implements the annual operating plans and budgets.
- *Selecting Qualified Management and Establishing an Effective Organizational Structure.* Senior management is responsible for selecting qualified management and implementing an organizational structure that is efficient and appropriate to the corporation's particular circumstances.
- *Identifying and Managing Risk.* Senior management identifies and manages the risks that the corporation undertakes in the course of carrying out its business. It also manages the corporation's overall risk profile.
- *Accurate and Transparent Financial Reporting and Disclosures.* Senior management is responsible for the integrity of the corporation's financial reporting system and the accurate and timely preparation of the corporation's financial statements and related disclosures in accordance with Generally Accepted Accounting Principles (GAAP) and in compliance with applicable laws and regulations. It is senior management's responsibility—under the direction of the CEO and the CFO—to establish, maintain, and periodically evaluate the corporation's internal controls and procedures. In accordance with applicable laws and regulations, the CEO and the CFO also are responsible for certifying the accuracy and completeness of the corporation's financial statements and the effectiveness of the corporation's internal and disclosure controls.

- The CEO and senior management are responsible for operating the corporation in an ethical manner. They should never put individual, personal interests before those of the corporation or its shareholders. Business Roundtable believes that when carrying out this function, corporations should have the following three elements in place:

  - *A CEO of Integrity.* The CEO should be a person of integrity who takes responsibility for the corporation adhering to the highest ethical standards.
  - *A Strong, Ethical "Tone at the Top."* The CEO and senior management should set a "tone at the top" that establishes a culture of legal

compliance and integrity communicated to personnel at all levels of the corporation.

- *An Effective Compliance Program.* Senior management should take responsibility for implementing and managing an effective compliance program relating to legal and ethical conduct. As part of its compliance program, a corporation should have a code of conduct with effective reporting and enforcement mechanisms. Employees should have a means of seeking guidance and alerting management and the board about potential or actual misconduct without fear of retribution, and violations of the code should be addressed promptly and effectively.[5]

2.4 ROLES AND RESPONSIBILITIES OF THE CHIEF GOVERNANCE OFFICER

The overall role of the chief governance officer (CGO) is to promote good corporate governance practices. The CGO position must be a permanent one, not a one-time job created to handle a corporate crisis situation. Stakeholders will invite the permanent establishment of a CGO position since it sends a positive signal to the capital markets. This good news, in turn, increases the market price of a company's stock and lowers the cost of capital for the company. Like any other sensitive position, the corporation's internal environment consisting of directors and management must be supportive of good governance principles and in the hiring and proper functioning of a good CGO. In order to fulfill the roles and responsibilities, the CGO should have a free and full access to all board members and the chairperson of the board.

Specifically, the following are the roles and responsibilities of a CGO:

- Establish the goals of good corporate governance, addressing board oversight, exacting ethical behavior, creating trust, and hiring competent management.
- Make corporate board members and management accountable for their actions.
- Develop governance principles, policies, and practices, covering the composition of the board; qualities of nonmanagement (nonexecutive) directors; the composition and responsibilities of various committees; and the allocation and balance of power among the owners, management, and the board.
- Communicate freely and fully about governance principles and policies both inside and outside of the organization.
- Notify government regulators and authorities through periodic filings to them about governance accomplishments. Do the same thing with the general public through news media.
- Provide training to management and nonmanagement employees of the organization about good governance principles, policies, and practices.
- Seek out "best practices" in corporate governance that other organizations implemented through benchmarking.
- Reexamine and reevaluate governance principles, policies, and practices, and update them as needed on an ongoing basis.
- Conduct governance audits, compliance audits, management reviews, and self-assessment reviews periodically and proactively to ensure continuous improvement in corporate governance practices.
- Analyze outside-in views (i.e., views of stakeholders about company management) and inside-out views (i.e., views of company management about

stakeholders) to identify disconnections between these views and to integrate them in a coherent manner.

2.5 ROLES AND RESPONSIBILITIES OF EXTERNAL AND INTERNAL AUDITORS

(a) OVERVIEW. *External auditors* play an important role in capital markets. Financial statements audited by external auditors permit the flow of capital to companies both in the form of equity and credit. External auditors owe a duty of due professional care when performing their work since they are accountable primarily to the stakeholders and secondarily to the company. Full disclosure of accurate and clear financial information should be the goal of external auditors to protect shareholders, investors, and creditors (i.e., stakeholders). External auditors need to establish credibility, honesty, ethical values, and integrity in delivering high-quality financial reporting useful for the proper functioning of the capital market system. External auditors should use professional skepticism when dealing with corporate management's assertions and representations. External auditors should act as gatekeepers in preventing and/or detecting their client organization's management wrongdoings.

Internal auditors play an important role for the organization they work for by adding value to the organization. Internal auditors help the organization in achieving its goals and objectives by reviewing business functions and operations for efficiency and effectiveness. Internal auditors owe a duty of due professional care when performing their work since they are accountable primarily to the company and secondarily to its shareholders. Internal auditors should use professional skepticism when dealing with corporate management's assertions and representations. Internal auditors should act as gatekeepers in preventing and/or detecting their organization's management wrongdoings.

(b) ROLE OF EXTERNAL AUDITORS. Financial statements of an organization (i.e., balance sheet, income statement, cash-flow statement, and notes to the financial statements) are prepared by company management and audited by external auditors.[6] Audited financial statements are the most widely used sources of information on companies. In their current form, the two major goals of financial statements are to enable monitoring to take place by outside parties (e.g., investors) and to provide the basis for valuing company securities. Management's discussion and analysis (MD&A) of operations is typically included in annual reports. This discussion is most useful when read in conjunction with the accompanying financial statements. Investors are particularly interested in information that may shed light on the future performance of the organization.

Arguably, failures of corporate governance can often be linked to the failure to disclose the "whole picture," particularly where off–balance sheet items are used to provide guarantees or similar commitments between related companies. It is therefore important that transactions relating to an entire group of companies be disclosed in line with high-quality domestic and international accounting standards, including information about contingent liabilities and off–balance sheet transactions, as well as special-purpose entities.

The application of high-quality standards is expected to significantly improve the ability of investors to monitor the company by providing increased reliability and comparability of financial reporting and also improved insight into company performance.

The quality of information substantially depends on the standards under which it is compiled and disclosed.

In addition to certifying that the financial statements represent fairly the financial position of a company, the audit statement should also include an opinion on the way in which the financial statements have been prepared and presented. This should contribute to an improved control environment in the company.

(c) ROLE OF INTERNAL AUDITORS. Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.[7]

The Institute of Internal Auditors (IIA) has developed *The Professional Practices Framework*, which consists of three categories for guidance: standards and code of ethics, practice advisories, and development and practice aids.

The first category (Mandatory Guidance) centers on *the Standards and the Code of Ethics* for the Professional Practice of Internal Auditing (Standards). Three sets of standards exist: attribute, performance, and implementation standards. The attribute standards address the attributes of organizations and individuals performing internal audit services. The performance standards describe the nature of internal audit services and provide quality criteria against which the performance of these services can be measured. The attribute and performance standards apply to all internal audit services. The implementation standards expand upon the attribute and performance standards, providing guidance applicable in specific types of engagements. Compliance with the concepts enunciated in the Mandatory Guidance is essential before the responsibilities of internal auditors can be met.

The purpose of the IIA's code of ethics is to promote an ethical culture in the profession of internal auditing. A code of ethics is necessary and appropriate for the profession of internal auditing, founded as it is on the trust placed in its objective assurance about risk management, control, and governance.

The second category, *Practices Advisories*, although not mandatory, represents best practices as a way to implement the standards. The practice advisories, in part, may help to interpret the standards or to apply them in specific internal audit environments. Many practice advisories are applicable to all internal auditors in a specific industry, audit specialty, or geographic area.

The third category, *Development and Practice Aids*, includes research studies, books, seminars, conferences, and other products and services related to the professional practice of internal auditing that do not meet the criteria for inclusion in Mandatory Guidance or Practice Advisories. The development and practice aids provide internal audit practitioners with the views of various experts on techniques and processes related to the professional practice of internal auditing.

For example, performance standards describe risk management and control as follows: the Internal audit activity should evaluate risk exposures or controls relating to the organization's governance, operations, and information systems regarding the reliability and integrity of financial and operational information, effectiveness and efficiency of operations, safeguarding of assets, and compliance with laws, regulations, and contracts.

The chief audit executive (CAE) conducts internal audits, special management reviews, and control self-assessment reviews periodically and proactively based on risk assessment and resource availability.

2.6 ROLES AND RESPONSIBILITIES OF THE AUDIT COMMITTEE AND OTHER COMMITTEES

(a) ROLES AND RESPONSIBILITIES OF THE AUDIT COMMITTEE

(i) Overview. Vibrant and stable capital markets depend on, among other things, reliable, transparent, and objective financial information to support an efficient and effective capital allocation process.[8] The vital oversight role audit committees play in the process of producing financial information has never been more important. As the capital markets continue to digest various corporate governance reforms, audit committees have been forced to refine—some would say redefine—their mission. And with these changes, the natural tension between the board's dual roles as an adviser to management and a fiduciary to shareholders is heightened—with the audit committee often at the center of the tension. Quite fundamentally, the capital market system today expects more from an audit committee than it ever has. How audit committees react to these changing expectations is a key factor in restoring credibility in financial information.

The audit committee's key responsibility—overseeing the process that produces reliable and credible financial statements while ensuring the company has effective internal controls—requires it to conduct activities that previously had been executed mostly by management. Today audit committees are also expected to retain and compensate the external auditors, grasp all of the key information included in a company's financial reporting, and oversee risk management and compliance with the laws and regulations affecting the company. This change is occurring in an environment that demands transparency.

(ii) Charter and Evaluation. Charters—the clearest articulation of the audit committee's purpose, composition, roles and responsibilities, and authority—are public documents. That makes it even more important for committees to evaluate regularly whether their charters are appropriate and whether they are discharging all their responsibilities. Committee evaluations, useful in identifying areas for improvement and training needs, raise new concerns over putting results in writing.

(iii) Financial Statements. In today's world, financial statements are extremely dense and, too often, difficult to understand. Indeed, they are so complicated that many audit committees struggle to grasp them or to feel completely confident they portray business results in the most effective way, particularly in areas where the accounting is highly technical and complex. Although many individual investors do not read the full financial statements, that does not diminish the importance of the audit committee's role in ensuring they are understandable and transparent for those companies and individuals who do. Audit committees can bring the discipline to ensure companies provide information to the investor world that is digestible and reliable.

(iv) Risk Management and Internal Control. When people talk about risk, they often mean different things—like insurance or hedging, or regulatory, product, or technology

risk. While audit committees long have overseen how companies respond to financial reporting risks, some now are overseeing the effectiveness of management's responses to additional types of risk, the kinds outlined above and other risks that might prevent a company from achieving its strategic objectives. It is vital up front that the board agrees on the scope of the audit committee's oversight, so the board can ensure all key risks are monitored somewhere at the board level. Then the audit committees needs to understand those risks within its purview and be confident that management's responses—the internal controls it has established and operate—are satisfactory and that management's process for identifying and assessing risk is sound. And in the same way that the audit committee should ensure proper transparency of the financial statements, it also should ensure that management's reporting on the effectiveness of internal controls over financial reporting is complete and understandable.

(v) Oversight of Management and Internal Audit. Audit committees always have needed to balance their fiduciary role with their role as advisers to management. However, as audit committee responsibilities have increased and the external pressure to emphasize committees' fiduciary role mounts—questioning and pressing management more, trusting less—tensions naturally increase.

Audit Committees and Corporate Management

Audit committees should press more and trust less with corporate management

Of course, audit committees must evaluate whether what management is telling them is supportable. Many audit committees look to the internal audit function for that insight, and rely on internal audit's objective assessment of risk and control in operational, compliance, and reporting areas. Audit committees should consider whether the internal audit function has the proper stature in the company. The audit committee will benefit, and it is in the committee's self-interest to be internal audit function's champion.

(vi) Relationship with External Auditors. External auditors play one of the key gatekeeper roles in the capital markets. Audit committees should own the relationship with the external auditors—and if they do not, and it is evident management still does, they need to take immediate steps to own it. Audit committees "owning" the relationship have direct reporting by external auditors, ongoing communication, frequent meetings, and robust discussions about audit scope and audit results. They pay more attention to greater levels of detail, evaluating potential services to determine whether the committee will grant its preapproval, taking steps to ensure the auditors' independence, and considering how well the auditors perform.

(vii) Compliance and Ethics. Witnessing how quickly corporate and personal reputations can be destroyed has provided a wake-up call for many directors. They recognize that, often, the greatest harm is caused by an individual's unethical actions. Therefore, ethics, codes of conduct, and tone at the top are vital in protecting a company against reputation risk. While failing to comply with legal and regulatory requirements may stem from carelessness regarding process problems—more neglect than outright malfeasance—to the outside world, such lack of compliance simply looks as though the company does not care enough about compliance to focus on it, which links again to

reputation. Many audit committees are playing a central role in addressing the evolving regulatory expectations for board-level involvement in compliance and ethics.

(viii) Committee Composition. Requirements for independence and financial literacy, limitations on the number of audit committees on which a director can serve, and concerns about liability have made it more challenging to recruit qualified members to an audit committee. The significant workload and time commitment required of audit committee members may be responsible for shifting committee composition, with active board chairs, CEOs, and presidents constituting a smaller portion of committees' membership than they did in the past.

(ix) Meetings. Audit committees have to steer their agenda instead of abdicating responsibility to management. Audit committee chairs often provide the foundation for effective audit committee meetings—driving the agenda, facilitating the discussion, holding premeetings to explore issues, and ensuring the right people are present. Audit committee members also are on the hook to prepare thoroughly for meetings. And the meetings need to have active meaningful participation, not presentation, sometimes requiring that presenters be coached in advance of meetings.

(x) Training. With the intricate nature of companies' business activities, the complexity of accounting transactions and policies, and frequent changes to financial accounting standards, even the most experienced audit committee members can benefit from training. New audit committee members also need robust orientation, allowing them to understand their role and the company's financial reporting process, so they can add value sooner.

(xi) Resources and Special Investigations. Audit committees' right and willingness to access needed resources further support their shift to being self-sufficient and autonomous. This requires that the audit committee is ready to direct special investigations. Crises may develop suddenly and arise in unexpected places. Committees directing a special investigation have to remember the importance of acting quickly, ensuring the investigating firm is independent, being comfortable with the level of communication, cooperating with regulators, and ensuring appropriate remedial actions.

(b) ROLES AND RESPONSIBILITIES OF OTHER COMMITTEES. Other committees may include the governance committee, compensation (remuneration) committee, special committee, nominating committee, finance committee, and employee benefits committee, and specific committees such as ethics, policy, or technology committees as needed.

The *governance committee* maximizes the effectiveness of the board through an annual review and evaluation of the structure, size, composition, development, and selection of the board members and its committees.

The *compensation committee* focuses on compensation arrangements for the board of directors and key executives that help achieve the organization's objectives and that do not emphasize short-term results at the expense of long-term performance.

It is considered good practice in an increasing number of countries that compensation (remuneration) policy and employment contracts for board members and key executives be handled by *a special committee* of the board, with independent directors making up either a majority of the committee or all of it. There are also calls for barring executives from sitting on each others' remuneration committees, since letting them do so can lead to conflicts of interest.

The *nominating committee* provides control over the selection of candidates for the board of directors and the key executives such as the CEO.

The *finance committee* controls major commitment of funds and ensures that capital expenditure budgets are consistent with strategic and operational plans.

The *employee benefits committee* oversees employee benefit programs and ensures they are consistent with the organization's objectives and that fiduciary responsibilities are properly discharged.

2.7 ROLES AND RESPONSIBILITIES OF THE CHIEF LEGAL OFFICER

The corporate Chief Legal Officer (CLO) or Corporate Legal Counsel or Corporate General Counsel establishes policies and procedures relating to prosecution of identified instances of fraud, waste, and abuse cases, and employee criminal acts; oversees the implementation of an ethics program throughout the organization; handles patent, trademark, and copyright violations by individuals or organizations; reviews discrimination suits filed by employees, contractors, and consultants against the corporation; and takes part in labor union negotiations.

Specifically, the following are the roles and responsibilities of a CLO:

- Participate in the due diligence process during a proposed merger or acquisition as one of the subject matter experts from operations, finance, information technology, and marketing.
- Develop business contracts and provide technical support to management to enforce contractual terms and conditions.
- Work with investment bankers and brokers in developing prospectus document and filing securities regulation application during stock and bond offerings to potential investors.
- Participate in labor union negotiations for a win-win outcome.
- Conduct in-house training classes for functional managers and executives regarding interpretation of laws, regulations, the Uniform Commercial Code (UCC), and court cases.
- Establish a solid and sustainable Chain of Knowledge linked through the entire legal management hierarchy to ensure core knowledge competencies.
- Conduct legal audits, management reviews, compliance audits, and self-assessment reviews periodically and proactively to ensure continuous improvement in legal matters.
- Comply with the professional standards and code of ethics established by the American Bar Association for the legal profession (www.abanet.org).
- Analyze outside-in views (i.e., views of stakeholders about company management) and inside-out views (i.e., views of company management about stakeholders) to identify disconnections between these views and to integrate them in a coherent manner.

2.8 ROLES AND RESPONSIBILITIES OF GATEKEEPERS

(a) OVERVIEW. Gatekeepers—including external auditors, attorneys, securities analysts, credit-rating agencies, and investment bankers—are not fulfilling their gatekeeper

or agent role to its fullest extent if they inform and advise the board of directors and the shareholders.[9] These gatekeepers should be serving investors, creditors, and stockholders by assuming an independent monitor or watchdog role and by avoiding conflict-of-interest situations that can compromise their independence and objectivity.

Gatekeepers are, in a way, policemen who prevent corporate wrongdoing. Some examples of corporate wrongdoing include manipulating earnings (earnings management), abusing financial restatements, capitalizing expenses, deferring or misclassifying expenses, hiding liabilities, engaging in off–balance sheet transactions, or getting involved in other types of financial fraud in order to increase stock price and receive big bonuses from corporate management.

Gatekeepers provide certification and verification services to investors, and they are hired and paid by the corporate managers that they are assigned to watch. The impact of these services is to lower the cost of capital for a corporation and thereby increase its stock price. Both shareholders and the board of directors depend on gatekeepers for an unbiased flow of information that is not edited, filtered, or modified in favor of corporate management. Effective corporate governance requires a chain of actors, including directors, managers, and gatekeepers. The latter cannot become the weakest link. Taking the broadest view, the board of directors and the Securities and Exchange Commission (SEC) can also be viewed as gatekeepers.

Gatekeepers are not fulfilling their watchdog role in preventing and/or detecting fraud or other irregularities if they do any of the following. Gatekeepers cannot wear blinders, cannot ignore "red flags," cannot be indifferent to sins of omission, and cannot do perfunctory audits or investigations.

Gatekeepers should increase their positive reputational capital and decrease their negative reputational capital by exhibiting unbiased and professional behavior.

Organizations should do the following:

- The board of directors must be active and independent of corporate management in order to discharge the directors' fiduciary responsibilities. The board should not approve loans to the CEO or other executives.
- A principal-agent relationship between the gatekeepers and the corporation must be reconsidered and restructured.

Organizations should not do "opinion-shopping" for accounting, auditing, and legal services.

(b) ROLE OF EXTERNAL AUDITORS. The highlights of the external auditor's (EAs) function and role include:

- EAs certify that a corporation's financial statements comply with generally accepted accounting principles (GAAP).
- Some organizations take advantage of soft and permissible GAAP and EAs allow them to happen.
- EAs are paid by the corporation that hires them. This raises a conflict-of-interest situation because the party paying the gatekeeper will be the party that the gatekeeper is expected to monitor.

- EAs who discover a serious problem with a corporate client's financial statements or disclosures can prevent a merger from closing by declining to deliver an opinion, a necessary precondition for that transaction.
- EAs should be faithful to investors and should not provide a false or reckless certification. They should not ignore "red flags" (i.e., turn their head the other way)
- EAs should use professional skepticism when dealing with corporate management assertions.
- EAs should act like a gatekeeper, not like a salesperson.

(c) ROLE OF ATTORNEYS. The highlights of the attorney's function and role include:

- Attorneys should conduct due diligence reviews in connection with an organization's securities offerings.
- Attorneys are paid by the corporation that hires them. This raises a conflict-of-interest situation because the party paying the gatekeeper will be the party that the gatekeeper is expected to monitor.
- Attorneys who discovers a serious problem with a corporate client's financial statements or disclosures can prevent a merger from closing by declining to deliver an opinion, a necessary precondition for that transaction
- Attorneys should use professional skepticism when dealing with corporate management representations
- Attorneys should comply with Section 307 of the Sarbanes-Oxley Act of 2002, which prescribes minimum standards of professional conduct for attorneys who appear or practice before the SEC. This section imposes an "up the ladder" reporting obligation, in that a material violation should be reported to the audit committee or the full board of directors only if the attorney has first reported the violation to the Chief Legal Officer or the CEO and, after a reasonable amount of time, has not received an appropriate response.

(d) ROLE OF SECURITIES ANALYSTS. The highlights of the securities analyst's (SAs) function and role include:

- SAs' positive evaluation may lend credibility to a company's own disclosures or predictions.
- SAs test and interpret financial statements and corporate disclosures. Based on this information, they make their own extrapolations and predictions as to the corporation's future financial and operational performance. They then issue research reports after meeting with company management and holding discussions with industry elements such as customers and suppliers.
- SAs issue "buy," "hold," or "sell" recommendations to their customers and the public. These are often inconsistent with a company's actual performance levels due to fear of retaliation, job security (career prospects), groupthink (consensus earnings forecasts with peers), income potential, and conflict-of-interest situations.
- SAs should not make excessively optimistic financial forecasts about a company by overstating future earnings and inflating recommendations.
- SAs should act like gatekeepers, not like salespersons.

(e) ROLE OF CREDIT-RATING AGENCIES. The highlights of the credit-rating agencies (CRAs) function and role include:

- CRAs (e.g., Moody's and S&P) provide standardized and condensed information about the creditworthiness of various corporations' bonds.
- CRAs assign a letter rating ranging from AAA to D to a corporation's debt securities. The debt rating will influence the cost of capital for the debt-issuing firm.
- CRAs are hesitant to downgrade a company's rating because of possible effects on the martketplace. But CRAs should lead, not follow, the market.
- CRAs are paid by the companies that they rate, and they do not face severe competition in the marketplace.
- CRAs should not have consulting arrangements with any issuer whom they rate.

(f) ROLE OF INVESTMENT BANKERS. The highlights of the investment bankers (IBs) function and role include:

- In cash-out mergers, IBs deliver the fairness opinion. The opinion assures the minority shareholders of the company that they have received a "fair" price.
- IBs must conduct a reasonable investigation of the accuracy of the statement filed by an issuer when registering securities for public sale. This is called due diligence review. They should not solely depend on the audited financial statements and the "comfort letter" from the external auditors.
- IBs should refuse to underwrite an issuer's securities if they find that the issuer's disclosures are materially deficient.
- IBs are paid by the corporation that hires them. This raises a conflict-of-interest situation because the party paying the gatekeeper will be the party that the gatekeeper is expected to monitor.

2.9 CORPORATE CONTROL FRAMEWORK

(a) DEFINITION OF CONTROL. Control is any positive or negative action taken by management that would result in accomplishment of the organization's goals, objectives, and mission. Controls should not lead to compulsion or become a constraint on employees. Controls should be natural and should be embedded in the organization's functions, operations, policies, and procedures. More so, controls should be accepted by the employees using or affected by them. Use and implementation of controls should be inviting, not inhibiting. Controls should be seen as beneficial from the employee's personal and professional viewpoints. Ideally, controls should facilitate the achievement of employee and organizational goals and objectives. In other words, any control that does not help or promote in achieving the goals and objectives should not be implemented. Controls should be effective, efficient, and should not cost more than the benefits derived.

(b) DEFINITION OF INTERNAL CONTROL. In 1992, the Committee of Sponsoring Organizations (COSO) of the Treadway Commission published in the United States an internal control-integrated framework to guide management.[10] Internal control is broadly defined as a process, affected by an entity's board of directors, management, and other

personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

The "internal control" definition—with its fundamental concepts of a process effected by people, and providing reasonable assurance—together with the categorization of objectives and the components and criteria for effectiveness, as well as the associated discussions, constitute this internal control framework.

KEY CONCEPTS IN INTERNAL CONTROL

- Internal control is a process. It is a means to an end, not an end in itself.
- Internal control is affected by people. It is not merely policy manuals and forms, but people at every level of an organization.
- Internal control can be expected to provide only reasonable assurance, not absolute assurance, to an entity's management and board.
- Internal control is geared to the achievement of objectives in one or more separate but overlapping categories.

(i) What an Internal Control Can and Cannot Do. Internal control can help an entity achieve its performance and profitability targets as well as prevent loss of resources. It can help ensure reliable financial reporting. And it can help ensure that the enterprise complies with laws and regulations, avoiding damage to its reputation and other consequences. In sum, internal control can help an entity get to where it wants to go, while avoiding pitfalls and surprises along the way.

WHAT CAN INTERNAL CONTROLS DO?

Internal controls promote efficiency, reduce risk of loss, and help ensure the reliability of financial statements and compliance with laws and regulations.

What internal control cannot do is provide absolute assurance of an entity's success or survival, or the reliability of financial reporting and compliance with laws and regulations.

(ii) Internal Control Is a Process. Internal control is not one event or circumstance but a series of actions that permeate an entity's activities. These actions are pervasive and are inherent in the way management runs the business. Internal control is most effective when it is built into the entity's infrastructure and is part of the essence of the enterprise. Controls should be "built in" rather than "built on." "Building in" controls can directly affect an entity's ability to reach its goals, and it supports a business's quality initiatives. In fact, internal control not only is integrated with quality programs, it is usually critical to their success.

(iii) Internal Control Is People. Internal control is promoted by a board of directors, management, and other personnel in an entity. It is accomplished by the people of an organization, by what they do and say. People establish the entity's objectives and put control mechanisms in place.

Similarly, internal control affects people's actions. Internal control recognizes that people do not always understand, communicate, or perform consistently. Internal control provides standards so that people have a common understanding of a process and a common language for communication. It enables them to perform consistently regardless of their unique backgrounds and technical abilities and varying sets of needs and priorities.

(iv) Components of Internal Control. Internal control consists of five interrelated components. These are derived from the way management runs a business and are integrated with the management process.

1. *Control Environment.* The core of any business is its people—their individual attributes, including integrity, ethical values, and competence—and the environment in which they operate. They are the engine that drives the entity, and the foundation on which everything rests. An entity's objectives and the way they are achieved are based on preferences, value judgments, and management styles. There often is a trade-off between competence and cost and between the extent of supervision and the requisite competence level of the individual. Companies can operate in a formal or informal mode. Formal documentation is not always necessary for a policy to be in place and to operate effectively. A more formally managed company may rely more on written policies, performance indicators, and exception reports.
2. *Risk Assessment.* The entity must be aware of and mitigate the risks it faces. It must set objectives that are integrated with sales, production, marketing, financial, and other activities so that the organization is operating in concert. It also must establish mechanisms to identify, analyze, and mitigate the related risks.

   Objective setting is a precondition to risk assessment. There must first be objectives before management can identify risks to their achievement and take necessary actions to mitigate the risks. Objective setting, then, is a key part of the management process. While not an internal control component, it is a prerequisite to, and an enabler of, internal control.
3. *Control Activities.* Control activities are the policies and procedures established and executed to help ensure that the actions identified by management as necessary to address risks to achievement of the entity's objectives are effectively carried out. Examples of control activities include approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, and segregation of duties. Control activities may be preventive or detective, manual or automated. Regardless of whether a policy is written, it must be consistently followed.

   Controls are also classified into two categories: (1) hard controls and (2) soft controls. Hard controls are formal, tangible, objective, and easier to measure and evaluate. Examples of hard controls include budgets, dual controls, written approvals, reconciliations, authorization levels, verifications, and segregation of

duties. By contrast, soft controls are informal, intangible, subjective, and difficult to measure and evaluate. Examples of soft controls include an organization's ethical climate, integrity, values, culture, vision, behavior and attitude of personnel, commitment to competence, tone at the top, management philosophy and operating style, level of understanding and commitment, and communication. Tools to evaluate hard controls include flowcharts, system narratives, testing, and counting. Tools to evaluate soft controls include self-assessments, questionnaires, control matrices, interviews, and workshops. Hard controls are easy to evidence and test, while soft controls may be more difficult to formally assess.

Generally speaking, senior managers most often use soft skills and soft controls to achieve their objectives; other managers most often use hard skills and hard controls. Soft skills include people skills such as interpersonal skills, motivation, negotiating, leadership, and communications skills. Hard skills include technical skills such as functional skills, analytical skills, problem identification and solving skills, and decision-making skills.

4. *Information and Communication.* Information and communication systems enable the entity's people to capture and exchange the information needed to conduct, manage, and control its operations. The information needs to flow to the right people that have the right information to make right decisions. Reliable internal financial measurements are also essential to planning, budgeting, pricing, evaluating vendor performance, and evaluating joint ventures and other alliances. Information can be obtained through questionnaires, interviews, broad-based market demand studies, or targeted focus groups. Information systems must provide the correct information, both on time and at the right place. Because of these requirements, information systems must be controlled due to their influence on control. Appropriate steps need to be taken to ensure that open communications channels exist for all employees.
5. *Monitoring.* The effectiveness of internal controls must be monitored and modifications made as necessary. In this way, the system can react dynamically, changing as conditions warrant. Monitoring is not a precondition to internal control, because it is a part of internal control. Monitoring activities include management or supervisory reviews, comparisons, and reconciliations. Emphasis should be put on "building in" rather than "adding on" controls. Monitoring can be done in two ways: through ongoing activities or through separate evaluations. Usually, some combination of ongoing monitoring and separate evaluations will ensure that the internal control system maintains its effectiveness over time.

(A) Tiered Approach

When there is a conflict between the choices, the COSO-based approach should not override the risk-based approach to audits. Self-assessment can be applied at any organizational level (first tier). The second tier is the activity level (e.g., process, subprocess, function, or department). Hard controls, such as documenting and testing control activities, are evaluated during the second tier. The best approach is analytical, starting from objectives, identifying risks and controls, evaluating the design of the controls, and testing control effectiveness.

(B) Limitations of Internal Control

No two entities will or should have the same internal control system. Companies and their internal control needs differ dramatically by industry and size, and by culture and management philosophy. Internal control has been viewed by some observers as ensuring that an entity will not fail—that is, the entity will always achieve its operations, financial reporting, and compliance objectives. In this sense, internal control sometimes is looked upon as a cure-all for all real and potential business ailments. This view is misguided. Internal control is not a panacea.

Even effective internal control operates at different levels with respect to different objectives. Also, internal control sometimes cannot provide reasonable assurance, due to differences in judgment, breakdowns in controls, management overrides, collusion, and problems in cost-benefit measurements.

(c) INTERNAL CONTROL ISSUES IN DERIVATIVES USAGE

(i) Overview. Derivatives are financial contracts that derive their value from the performance of underlying assets (such as a stock, bond, or physical commodity), interest or currency exchange rates, or a variety of indices, such as a composite stock index like the Standard & Poor's 500.[11]

Derivatives include a wide assortment of financial contracts, including swaps, futures, forwards, options, caps, floors, and collars, whose values are derived by means of defined formulas that apply to notional amounts (hypothetical reference amounts). Derivatives can also include certain assets and liabilities whose value and cash flows are directly determined by an underlying instrument or index, such as collateralized mortgage obligations, interest-only and principal-only certificates, and structured notes. Other types of derivatives include contracts traded on organized exchanges standardized by regulation, as well as contracts that are traded in unregulated over-the-counter (OTC) markets, including individually tailored contracts negotiated between two parties for a specific purpose.

Derivatives are associated with market, credit, and liquidity risk, among other technical risks. In addition, there is the fundamental risk that the use of these products may not be consistent with entity-wide objectives. Derivative use is sometimes misunderstood because, depending on the type of instrument and its terms, an instrument may be used to increase, modify, or decrease risk. As contract features increase in complexity, the value and effectiveness of a derivative in achieving objectives may become more difficult to ascertain before such positions are closed out or settled for cash. Derivative products and activities must be well understood in order for control systems to provide adequate assurance that derivatives use will support achievement of entity-wide strategies and objectives.

(ii) Action Steps. Actions that might be taken to better understand or apply the COSO Framework to derivatives will depend on the position and role of the parties involved. A board of directors, senior management, and others involved with derivatives may consider a number of actions, including:

- Initiating a self-assessment of entity-wide control systems, directing attention specifically to areas of derivative operations that are of primary importance

- Fully integrating management of derivative activities into the enterprise's overall risk management system by developing and implementing a comprehensive risk management policy
- Ensuring that policy objectives specifying the use of derivatives are clearly articulated and documented
- Requiring that any use of derivatives be clearly linked with entity-wide and activity-level objectives

(d) INTERNAL-CONTROL BEST PRACTICES. COSO defines the following objectives and tools for operations, marketing and sales, service, and financial and operational reporting areas.[12] We label these objectives and tools as best practices in internal control.

Operations

- Schedule operations to minimize inventory and to ensure sufficient availability of completed products in a timely manner.
- Minimize production downtime.
- Produce products in appropriate quantities and in accordance with specifications and production schedules.
- Comply with applicable laws and regulations during production of goods.
- Produce products in accordance with quality-control standards.

Marketing and Sales

- Design marketing strategies giving consideration to competitive, regulatory, and business environments, or other factors that may influence the entity's marketing activities and potential changes in those factors.
- Identify potential and existing customers, and develop marketing strategies to influence those parties to purchase the entity's products or services.
- Maintain delivery capabilities for delivery of products to customers on a timely basis at the least distribution cost.
- Address market needs for product, including introduction of new products, and continuance, changes to, or discontinuance of existing products.
- Implement marketing strategies effectively to manage sales activities.
- Meet or exceed sales targets in an efficient manner.
- Forward all sales orders to outbound activities (e.g., shipping) and service in a timely manner.

Service

- Handle customer inquiries expeditiously and efficiently.
- Satisfy customer service needs so as to further sales and marketing objectives.
- Make authorized installations correctly, efficiently, and on a timely basis.
- Ensure that warranty policies are consistent with marketing and financial strategies.
- Investigate and respond to requests for service on a timely basis and in accordance with warranties.

- Ensure that customer service representatives use up-to-date pricing and other product information to assist customers.
- Investigate and respond to requests for services in the most efficient manner and on a timely basis.

Financial and Operational Reporting

- Provide timely and accurate information needed by management and others to discharge their responsibilities.
- Prepare external financial reports (e.g., balance sheet, income statement, and cash flow statements) on a timely basis and in compliance with applicable laws, regulations, rules, or contractual agreements.
- Prepare internal operational reports (e.g., product-line profitability analysis, inventory turnover rates, and resource utilization statistics) on a timely basis and in compliance with management needs and schedules.
- Maintain confidentiality of financial and operational information.

2.10 FRAUD AND FRAUDULENT FINANCIAL REPORTING

(a) OVERVIEW. Fraud involves deception, confidence, and trickery done by one individual to get an advantage over another. Fraud is different from unintentional error because the former involves intent and the latter does not.

(b) TYPES OF FRAUD. The most common way to classify fraud is to divide frauds into those committed against an organization (occupational fraud) and those committed on behalf of an organization (management fraud). Occupational fraud includes employee embezzlement, vendor fraud, and customer fraud. Management fraud includes financial statement fraud and investment scams, with the former being the focus of this section.

In financial statement fraud, top management is involved and stockholders, creditors, and others who rely on financial statements are the victims. Here, financial information is misrepresented. The motivations behind fraudulent financial statements vary and include: (1) to support a high stock price on an ongoing basis, (2) to support a bond or stock offering, (3) to receive big bonuses from increased revenues, profits, and stock prices, (4) to protect management's personal net worth from the company stock ownership, and (5) to meet the stock market's higher expectations of financial results. One way to prevent and detect fraud is to conduct fraud audits, special management reviews and investigations, and fraud self-assessment reviews periodically and proactively to send a strong message to employees that fraud is not tolerated.

In this section, we will discuss COSO's research results on financial statement fraud, off–balance sheet accounting practices, financial restatements, and financial shenanigans, which can be collectively labeled as fraudulent financial reporting practices.

(c) FINANCIAL STATEMENT FRAUD

(i) Overview. Fraudulent financial reporting can have significant consequences for the organization and for public confidence in capital markets.[13] Periodic high-profile cases of fraudulent financial reporting raise concerns about the credibility of the U.S. financial

reporting process and call into question the roles of auditors, regulators, and securities analysts in financial reporting.

COSO sponsored a research project to analyze U.S. public companies between 1987 and 1997 to provide an extensive updated analysis of financial statement fraud occurrences. The focus of the research included cases that clearly involved financial statement fraud and excluded cases dealing with analysis of financial restatements due to errors or earnings management activities that did not result in a violation of the U.S. federal antifraud statutes.

(ii) Summary of Findings and Implications. Several key findings can be generalized from study of about 200 financial statement fraud cases. The findings were grouped into five categories describing the nature of the companies involved, the nature of the control environment, the nature of the frauds, issues related to the external auditor, and the consequences to the company and the individuals allegedly involved.

Fraud Category 1: Nature of the Companies Involved

Finding 1. Relative to public registrants, companies committing financial-statement fraud were relatively small. The typical size of most of the sample companies ranged well below $100 million in total assets in the year preceding the fraud period. Most companies (78% of the sample) were not listed on the New York or American Stock Exchanges.

Finding 2. Some companies committing the fraud were experiencing net losses or were in close to break-even positions in periods before the fraud. Pressures of financial strain or distress may have provided incentives for fraudulent activities for some fraud companies. Some companies were experiencing downward trends in net income in periods preceding the first fraud period, while other companies were experiencing upward trends in net income. Thus, the subsequent frauds may have been designed to reverse downward spirals for some companies and to preserve upward trends for others.

Implications. The relatively small size of fraud companies suggests that the inability or even unwillingness to implement cost-effective internal controls may be a factor affecting the likelihood of financial statement fraud (e.g., override of controls is easier). Smaller companies may be unable or unwilling to employ senior executives with sufficient financial reporting knowledge and experience. Boards, audit committees, and auditors need to challenge management to ensure that a baseline level of internal control is present.

Fraud Category 2: Nature of the Control Environment

Finding 1. Top senior executives were frequently involved. In 72% of the cases, the CEO was associated with the financial statement fraud, and in 43% the CFO was. Only 17% did not involve either. Other individuals involved include controllers, chief operating officers (COOs), and other senior vice presidents, and board members.

Finding 2. Most audit committees only met about once a year or the company had no audit committee at all. Audit committees for the fraud companies generally met only once per year. Twenty-five percent of the companies did not have an audit committee.

Most audit committee members (65%) did not appear to be certified in accounting (i.e., were not CPAs) or have current or prior work experience in key accounting or finance positions.

Finding 3. Boards of directors were dominated by insiders and "gray" directors with significant equity ownership and apparently little experience serving as directors of other companies. Approximately 60% of the directors were insiders or "gray" directors (i.e., outsiders with special ties to the company or management). Taking all the companies together, the directors and officers owned nearly one-third of the companies' stock, with the CEO/presidents personally owning about 17%. Nearly 40% of the boards did not have a single director who served as an outside or gray director on another company's board.

Finding 4. Family relationships among directors and/or officers were fairly common. In nearly 40% of the companies, the proxy provided evidence of family relationships among the directors and/or officers. In nearly half of all the companies, the founder and current CEO were the same person or the original CEO/president was still in place. In over 20% of the companies, there was evidence of officers holding incompatible job functions (e.g., CEO and CFO).

Implications. Monitoring the pressures faced by senior executives (e.g., pressures from compensation plans and investment community expectations) is critical. The involvement of senior executives who are knowledgeable about financial reporting requirements, particularly those unique to publicly traded companies, may help to educate other senior executives about financial reporting issues and may help to restrain senior executives from overly aggressive reporting. In other cases, however, board members and auditors should be alert for deceptive managers who may use that knowledge to disguise a fraud. In the smaller company setting, due to the centralization of power in a few individuals, it may be especially important to have a solid monitoring function performed by the board.

Fraud Category 3: Nature of the Frauds

Finding 1. Cumulative amounts of frauds were relatively high in light of the relatively small sizes of the companies involved. The average financial statement misappropriation or misstatement of assets was $25 million and the median was $4.1 million. While the average company had assets totaling $533 million, the median company had total assets of only $16 million.

Finding 2. Most frauds were not isolated to a single fiscal period. Most frauds overlapped at least two fiscal periods, frequently involving quarterly and annual financial statements. The average fraud period extended over 23.7 months, with the median fraud period extending 21 months. Only 14% of the sample companies engaged in a fraud involving fewer than 12 months.

Finding 3. Typical financial-statement fraud techniques involved the overstatement of revenues and assets. Over half of the frauds involved overstating revenues, either by recording revenues prematurely or fictitiously. Many of those revenue frauds affected only transactions recorded right at period end (i.e., quarter-end or year-end). About half the frauds also involved overstating assets by understating allowances for receivables; overstating the value of inventory, property, plant, and equipment and other tangible assets; or recording assets that did not exist.

Implications. It is important to conduct internal reviews of quarterly financial statements and the related controls surrounding interim financial statement preparation, as well as the benefits of continuous auditing strategies. Procedures affecting transaction cutoff, transaction terms, and account valuation estimation for end-of-period accounts and transactions may be particularly relevant.

Fraud Category 4: Issues Related to the External Auditor

Finding 1. All sizes of audit firms were associated with companies committing financial statement frauds. Fifty-six percent of the sample fraud companies were audited by a big CPA firm auditor during the fraud period and 44% were audited by a non-big CPA firm auditor.

Finding 2. All types of audit reports were issued during the fraud period. A majority of the audit reports (55%) issued in the last year of the fraud period contained unqualified opinions. The remaining 45% of the audit reports issued in the last year of the fraud period departed from the standard unqualified auditor's report because they addressed issues related to the auditor's substantial doubt about going concern, litigation and other uncertainties, changes in accounting principles, and changes in auditors between fiscal years comparatively reported. Three percent of the audit reports were qualified due to a GAAP departure during the fraud period.

Finding 3. Financial statement fraud occasionally implicated the external auditor. Most of the auditors (82%) explicitly named in the fraud cases were from non-big CPA firms. They were named either for alleged involvement in the fraud (54%) or for negligent auditing (46%).

Finding 4. Some companies changed auditors during the fraud period. Just over 25% of the companies changed auditors during the time frame beginning with the last clean financial-statement period and ending with the last fraud financial-statement period. A majority of the auditor changes occurred during the fraud period (e.g., two auditors were associated with the fraud period) and a majority involved changes from one non-big CPA firm auditor to another non-big CPA firm auditor.

Implications. There is a strong need for the auditor to look beyond the financial statements to understand risks unique to the client's industry, management's attitude toward aggressive reporting, and client internal control (particularly the tone at the top), among other matters. As auditors approach the audit, information from a variety of sources should be considered to establish an appropriate level of professional skepticism needed for each engagement. The auditor should recognize the potential likelihood for greater audit risk when auditing companies with weak board and audit committee governance.

Fraud Category 5: Consequences for the Company and Individuals Involved

Finding 1. Severe consequences awaited companies committing fraud. Consequences of financial statement fraud to the company often include bankruptcy, significant changes in ownership, and delisting by national stock exchanges, in addition to financial penalties imposed.

Finding 2. Consequences associated with financial statement fraud were severe for individuals allegedly involved. Individual senior executives were subject to class action

legal suits and Securities and Exchange Commission (SEC) actions that resulted in financial penalties to the executives personally. A significant number of individuals were terminated or forced to resign from their executive positions. However, relatively few individuals explicitly admitted guilt or eventually served prison sentences.

(iii) Off–Balance Sheet Accounting Practices. Off–balance sheet accounting practices involves hiding debt or underreporting liabilities on the balance sheet, thus increasing financial risk (a hidden risk) to a company and deceiving investors and creditors.[14]

The reason for corporations hiding their debt is that reporting lower amounts of liabilities on the balance sheet can bring lower interest rates, lower probability of bankruptcy, and higher bond ratings. With hidden debt, company management hopes to realize higher stock prices and higher bond prices. These unethical management practices result in misleading or fraudulent financial reporting, but they are permitted by GAAP and therefore legal.

However, greater amounts of liabilities will increase the probability of a company going bankrupt, a prospect that in turn increases the company's financial leverage. The financial leverage can act both in good and bad ways, depending on how it is viewed. Investors and creditors consider the increased financial leverage of a company and reflect it in lower stock and bond prices, leading to higher cost of capital, which is not good for the company.

Corporations have old and new methods for hiding their liabilities. Some of the older methods include equity method, lease accounting, pension accounting, take-or-pay contracts, and throughput arrangements. Newer methods include creating special-purpose entities, hiding debt from loan securitization, synthetic leases, and other borrowings.

Corporations should do the following:

- Insist that managers tell the truth to investors, creditors, and others.
- Encourage high-quality financial reporting, not high earnings.
- Use "conservative" accounting principles, methods, policies, and practices.
- Treat investors, creditors, and other financial statement users fairly and equitably.
- Cultivate honesty and integrity in financial accounting and reporting practices.
- Provide a fair and full disclosure of debts either in the footnotes or main body of financial reports.

Corporations should not do the following:

- Mask the quantity of debt a company possess on its balance sheet.
- Engage in "earnings management" to increase a company's stock prices and to receive big bonuses to management.
- Use "aggressive" accounting principles, methods, policies, and practices even though GAAP permits them.
- Report inadequate and misleading disclosures of financial information.
- Create conflict-of-interest situations and exhibiting ethical violations.
- Maintain off-the-book accounts.
- Value assets on a mark-to-market basis.

(iv) Financial Restatements. Public confidence in the reliability of financial reporting is critical to the effective functioning of the securities markets and capital markets, and various federal laws and entities help ensure that the information provided meets such standards.[15]

Although the number of public companies restating their publicly reported financial information due to financial reporting fraud and/or accounting errors remained a relatively small percentage of all publicly listed companies, the percentage of large companies announcing restatements has continued to grow. While large and small companies restate their financial results for varying reasons, change in cost- or expense-related items (including lease accounting issues) was the most frequently cited reason for restating. While both internal and external parties could prompt restatements, internal parties such as company management or internal auditors prompted the majority of restatement announcements. Exhibit 2.1 describes the financial restatement categories.

Cost or Expense. Restatements due to improper accounting for costs or expenses. This category generally includes understatement or overstatement of costs or expenses, improper classification of expenses, or any other number of mistakes or improprieties that lead to misreported costs. It also includes improper treatment of expenses related to tax liabilities and tax reserves. In addition, it includes improper treatment of financing arrangements, such as leases, when a related asset is improperly capitalized or expensed as part of the financing arrangement. Improperly reserved litigation restatements are also included in this category.

Revenue Recognition. Restatements due to improper revenue accounting. This category includes instances in which revenue is improperly recognized, questionable revenues are recognized, or any number of other mistakes or improprieties are committed that lead to misreporting of revenue. Also included in this category are ''round-trip'' transactions, in which colluding companies arrange the simultaneous purchase and sale of products so as to artificially inflate volume and revenues.

Securities-Related. Restatements due to improper accounting for derivatives, warrants, stock options, and other convertible securities.

Restructuring, Assets, or Inventory. Restatements due to asset impairment, errors relating to accounting treatment of investments, timing and amount of asset write-downs, goodwill and other intangibles, restructuring activity and inventory valuation, and inventory quantity issues.

Reclassification. Restatements due to improper classification of items on a financial statement—that is, current liabilities being classified as long-term debt on the balance sheet, or cash flows from operating activities being classified as cash flows from financing activities on the statement of cash flows.

Acquisition and Merger. Restatements due to improper accounting for—or a complete lack of accounting for—acquisitions or mergers. These include instances in which the wrong accounting method was used, or losses or gains related to acquisition were understated or overstated.

Related Party Transactions. Restatements due to inadequate disclosure or improper accounting of revenues, expenses, debts, or assets involving transactions or relationships with related parties.

In-Process Research and Development. Restatements resulting from instances in which improper accounting methodologies were used to value in-process research and development at the time of an acquisition.

Other. Any restatement not covered by the listed categories. Includes restatements due to inadequate loan-loss reserves, delinquent loans, loan write-offs, or other allowances for doubtful accounts or accounting estimates, and restatements due to fraud or accounting errors that were left unspecified.

Exhibit 2.1 Financial-Restatement Category Descriptions

A variety of reasons appear to have contributed to the increased trend in restatements, including increased accountability requirements for company executives, increased focus on ensuring internal controls for financial reporting, increased auditor and regulatory scrutiny (including clarifying guidance), and a general unwillingness on the part of the public companies to risk failing to restate, regardless of the significance of the event.

Companies that announce financial restatements generally continue to experience decreases in stock prices and market capitalization in the days around the initial announcement. The exact reason for this decline is unclear, but may include a variety of factors such as investors' inability to discern the reason for the restatement, varying reactions by investors about what the restatement means (e.g., whether the company is improving its disclosures), or investors' growing insensitivity to financial restatement announcements. Investors may believe either that the trend in restatements is part of a "cleansing process" (i.e., public companies strengthening their internal controls) or else that it merely reflects technical adjustments for compliance.

(d) FINANCIAL SHENANIGANS

(i) What Are Financial Shenanigans? Financial fraud causes great harm to individuals, to companies, and to society at large.[16] Financial shenanigans (a form of financial fraud) are actions or omissions to hide or distort the real financial performance or financial condition of a business entity. They range from minor deceptions (such as failing to segregate operating gains and losses from nonoperating gains and losses) to more serious misapplication of accounting principles (such as failing to write off worthless assets) and outright fraudulent behavior (such as recording of fictitious revenues to overstate an entity's real financial performance).

(ii) Why Do Shenanigans Exist? There are three general reasons for shenanigans:

1. *It pays to do it.* When a bonus plan encourages managers to post higher sales and profits (with no questions asked how those gains were achieved), it may create an incentive for using shenanigans. Misguided incentive plans should be revisited.
2. *It is easy to do it.* Honest managers select accounting methods from a variety of acceptable choices to portray fairly the company's financial performance. Unscrupulous managers use the flexibility offered by GAAP to distort financial reports.
3. *It is unlikely that perpetrators will get caught.* Companies may use accounting tricks because they believe that auditors or regulators will not catch them. Consider that only the annual financial statements of publicly held companies in the United States are audited by an independent, certified public accountant (CPA). Privately held companies are not required to be audited.

(iii) The Seven Shenanigans. Companies with a weak "control environment"—those that lack independent members of the board, a competent independent auditor, or an adequate internal audit function—have a greater tendency toward committing shenanigans than others.

Financial shenanigans, which permit companies to manipulate net income, may be separated into seven broad categories. The first five boost current year profits; the last two shift current-year profits to the future.

1. Recording revenue too soon to show more sales
2. Recording bogus revenue to show more income
3. Boosting income with onetime gains to show more income
4. Shifting current expenses to a later period to show more income
5. Failing to record or disclose all liabilities to show more assets
6. Shifting current income to a later period to minimize taxes
7. Shifting future expenses to the current period to show less income

(iv) Shenanigans Prevention Techniques. The primary shenanigan prevention strategies available to board of directors are to improve the company's incentive structure (to motivate) and to strengthen its control environment (to monitor). Specific prevention techniques include:

- Structure managers' incentives to reward honest financial reporting and to punish any activities that might constitute or contribute to financial shenanigans.
- Establish and encourage managers to adopt conservative accounting principles and policies.
- Appoint outside board members as watchdogs over senior management and corporate officers, with wide-ranging and early access to corporate financial data.
- Appoint both internal auditors and independent auditors and assign them the mission of preventing and detecting shenanigans.
- Grant internal auditors both the power and the security to communicate directly and freely with outside board members about their findings.
- Establish a senior-level audit committee with the mission of preventing and detecting shenanigans.

(v) Shenanigan Detection Techniques. Sometimes even the best intentions and the most comprehensive preventive measures fail and gimmicks begin to spread. Shenanigan detection approaches include both general-level attention to certain "red flags" and detailed review of particular data from the company's financial statements.

At a general level, warning signs ("red flags") of a financially troubled business that might be resorting to financial shenanigans or be prone to committing them include:

- Weak internal control environment
- Inadequate outside checks and balances
- Vulnerability to external influences
- Poor organizational culture
- Convoluted financial, legal, and organizational structure
- Shortage of "free" cash flows from operations
- Unusually low or high operating revenues
- Profits out of line with current sales and with previous quarters and years
- Inventories and receivables out of balance with sales
- Too many "irregular" events

(vi) Role of Corporate Directors in Controlling Corporate Fraud. Corporate directors have a direct liability in fraudulent activities perpetrated against a corporation. They have the power to control fraud with their position in the company. They should look for early warning signs from financial statements, such as uncollectibility of receivables, inadequate salability of inventory, improper valuation of investments, obsolescence of fixed assets, overstatement of intangibles, and unreported or underreported liabilities. By taking proper steps to prevent and detect shenanigans, the board of directors can shield themselves from undue liability and also contribute toward a more ethical corporate world.

2.11 CORPORATE RISK MANAGEMENT

Risk is pervasive throughout an organization as it can arise from any business function or process at any time without warning. Because of this widespread exposure, no single functional department management, other then the board of directors, can oversee the enterprise-wide risk-management program. This approach also supports the idea that risks cannot be identified, measured, and monitored on a piecemeal basis. A holistic approach is needed.

Since risks can arise in any business function or process, it makes good sense for business unit line management to accept full responsibility for risk management with the support of a centralized risk-management function. The business-unit line management must see that managing risk is an integral part of their mission (for example, manufacturing a product or delivering a service), with risks being linked to business objectives and strategy. The business-unit line managers are thus responsible for identifying, managing, and reporting risk matters upstream through the management hierarchy to the board members. The board then works with the audit committee or other committee members in coordination with the chief risk officer (CRO) to manage enterprise-wide risks. An enterprise-wide risk-management approach ensures that the organization's assets are safeguarded, its reputation is protected, and shareholder value is enhanced, with all this accomplished through managing risks. To obtain such results, management must link strategy, goals and objectives, risks, individual employee performance, and organization performance.

(a) ROLES AND RESPONSIBILITIES OF CHIEF RISK OFFICER. As a member of the senior management team, the roles and responsibilities of the CRO include:

- Monitoring the entire organization's risk profile
- Developing an enterprise-wide risk architecture or risk framework that is linked down to each business unit or division
- Developing an inventory of risks, both current and potential, with associated trigger points or events as guidance to employees
- Developing an inventory of controls or risk-mitigation action steps to address each of current and potential risks in order to bring risks to an acceptable level
- Acquiring property insurance and business insurance to protect business assets (tangible and intangible) from damage, destruction, accidents, fire, floods, theft, or loss
- Seeking alternative risk-transfer tools, as an option to traditional insurance, such as multiline or multiyear insurance, multiple-trigger policies, securitization, captives insurance, and finite risk insurance policies

- Coaching business-unit line managers and staff managers how to develop risk-versus-reward tradeoffs, especially when pursuing new business opportunities
- Anticipating potential new risks facing the organization after analyzing internal changes (e.g., new business, new products, new services, new processes, new customers, and new suppliers) as well as external changes (e.g., economic, political, technical, regulatory, and international)
- Developing organization-wide business continuity and contingency plans for addressing business disasters as well as information technology disasters
- Managing enterprise-wide risks so that there are no unpleasant surprises to senior management, audit committee, and board of directors of the firm
- Working with the internal audit department in developing audit plans to identify high-risk areas for audit
- Working with the legal department in understanding risks arising from lawsuits filed either internally or externally
- Conducting risk audits, special management reviews, and risk self-assessment reviews periodically and proactively to manage risks facing an organization

(b) WHAT IS RISK MANAGEMENT? Risk is the possibility of something adverse happening to an organization. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining the reduced level of risk. Risk management encompasses three processes: risk assessment, risk mitigation, and risk evaluation.

$$\text{Risk management} = \text{risk assessment} + \text{risk mitigation} + \text{risk evaluation}$$

Risk assessment includes identification and evaluation of risks and risk impacts, and recommendation of risk-reducing measures. *Risk mitigation* refers to prioritizing, implementing, and maintaining the appropriate risk-reducing measures recommended from the risk assessment process. *Risk evaluation* is a continual process for implementing a successful risk management program. Management is responsible for determining whether the remaining risk (residual risk) is at an acceptable level or whether additional controls should be implemented to further reduce or eliminate the residual risk.

A successful risk management program will rely on *critical success factors* such as (1) senior management's commitment, (2) the full support and participation of team members, (3) the competence of the risk assessment team, which must have the expertise to apply the risk assessment methodology to a specific process or system, identify mission risks, and provide cost-effective safeguards that meet the needs of the organization, (4) the awareness and cooperation of members of the user community, who must follow procedures and comply with the implemented controls to safeguard the mission of their organization, and (5) an ongoing evaluation and assessment of mission risks.

Minimizing negative effects on an organization and providing a sound baseline for decision making are the fundamental reasons that organizations implement a risk management process.

(c) RISK MANAGEMENT METHODOLOGY. As stated earlier, risk management encompasses three processes: risk assessment, risk mitigation, and risk evaluation.

(i) Risk Assessment. Risk assessment is the first process in the risk-management methodology. Organizations use risk assessment to determine the extent of the potential threat and the risk associated with a process or system. The output of the process helps to identify appropriate controls for reducing or eliminating risk during the risk-mitigation process. Major activities in the risk-assessment process include vulnerability identification, threat identification, control analysis, impact analysis, risk determination, and control recommendations.

(ii) Risk Mitigation. Risk mitigation, the second process involved in risk management, involves prioritizing, evaluating, and implementing appropriate risk-reducing controls recommended from the risk assessment process. Because the elimination of all risk is usually impractical or close to impossible, it is the responsibility of senior management and functional and business managers to use the least-cost approach and implement the most appropriate controls to decrease mission risk to an acceptable level, with minimal adverse impact on the organization's resources and mission.

(A) Risk-Mitigation Options

Risk mitigation is a systematic methodology used by senior management to reduce organization risks. Risk mitigation can be achieved through any one or combination of the following risk mitigation options:

- *Risk Rejection.* Risk rejection or risk ignorance is not a wise choice, as all major risks must be managed.
- *Risk Assumption (Acceptance).* Risk acceptance is recognizing a risk, and its potential consequences, and accepting that risk. This usually occurs when there is no alternate risk mitigation strategy that is more cost-effective or feasible.

  At some point, management needs to decide if the operation or the function or the system is acceptable, given the kind and severity of remaining risks. Risk acceptance is linked to the selection of safeguards since, in some cases, risk may have to be accepted because safeguards (countermeasures) are too expensive (for either monetary or nonmonetary reasons).

  Merely selecting safeguards does not reduce risk; those safeguards need to be effectively implemented. Moreover, to continue to be effective, risk management needs to be an ongoing process. This requires a periodic assessment and improvement of safeguards and reanalysis of risks.
- *Risk Avoidance.* A risk can be avoided by eliminating its cause and/or consequences (e.g., by adding controls that prevent the risk from occurring, removing certain functions of the system, or shutting down the system when risks are identified).
- *Risk Reduction (Limitation).* A risk can be limited by implementing controls that minimize its adverse impact (e.g., through use of supporting, preventive, and detective controls) or by authorizing operation for a limited time during which additional risk mitigation by other means is put into place. This option is also called risk reduction because it affords an opportunity to decrease the likelihood a risk will occur.
- *Risk Transfer.* A risk can be transferred by using other options to compensate for the loss (for example, by purchasing insurance or coinsurance, or by outsourcing).

Risk transfer is finding another person or organization that can manage the project risk(s) better. Risk protection can be viewed as insurance against certain events. It involves doing something to allow the project to fall back on additional or alternate resources should the scheduled resource(s) fail.

- *Risk Contingency.* Proper planning is done to define the necessary steps needed if an identified risk event should occur.
- *Risk Compliance.* The necessary steps are taken to comply with all the applicable laws and regulations in a timely and proper manner in order to reduce compliance risk.

(B) Residual Risk

Organizations can analyze the extent of the risk reduction generated by the new or enhanced controls in terms of the reduced threat likelihood or impact. The risk remaining after the implementation of new or enhanced controls is the residual risk. Practically no system or process is risk free, and not all implemented controls can eliminate the risk they are aimed at or reduce the risk level to zero.

Implementation of new or enhanced controls can mitigate risk by:

- Eliminating some of the system's vulnerabilities (flaws and weaknesses), thereby reducing the number of possible threat-source/vulnerability pairs
- Adding a targeted control to reduce the capacity and motivation of a threat-source (e.g., if technical controls are expensive, then consider administrative and physical controls)
- Reducing the magnitude of the adverse impact (e.g., limiting the extent of a vulnerability or modifying the nature of the relationship between the IT system and the organization's mission)

If the residual risk has not been reduced to an acceptable level, the risk-management cycle must be repeated to identify a way of lowering the residual risk to an acceptable level.

(iii) Risk Evaluation. Risk evaluation, the third and final process of risk management, is a continual evaluation process since change is a constant thing in most organizations. Possible changes include: (1) new businesses are acquired, (2) new products are introduced, (3) new services are provided, (4) networks are updated and expanded, (5) network components are added or removed, (6) applications software is replaced or updated with newer versions, (7) personnel changes are made, and (8) security policies are updated. These changes mean that new risks will surface and risks previously mitigated may again become a concern. Thus, the risk evaluation process is ongoing and evolving.

(d) TYPES OF RISKS. The CRO must identify as many risk types as possible, covering both current and potential risks. Each risk alternative for satisfying the business requirements must be evaluated for the following risk types. The evaluator reviews each of these risks to determine the overall impact of significant variations from the original assumptions on which the expected success of the alternative is based.

This section discusses 26 types of risks and suggests best practices to reduce such risks. Most of these risks are interrelated and interconnected, which creates a magnifying

effect. For example, legal risk and regulatory risk would magnify the reputation (image) risk of an organization. Some risks have a cascading effect, for example, noncompliance with contractual terms and conditions can lead to financial risk (i.e., loss of money due to payment of penalties) and legal risk (lawsuits resulting from violation of contractual rights). Therefore, these 26 risk types should be viewed from a total business context instead of a piecemeal basis.

Four common best practices that are applicable to each type of risk include (1) acquiring traditional and nontraditional insurance coverage to protect tangible and intangible assets, (2) conducting surveys of employees, customers, suppliers, and the industry, (3) performing benchmarking studies to understand existing and new risks better, and (4) keeping the Chain of Knowledge strong and current through continuous acquisition of knowledge, skills, and abilities (KSAs) by all employees.

(i) Human Capital Risk. Human capital (people) risk is very significant and most risky one to watch for. Sources of people risk include employee carelessness, fatigue, memory lapses, inattention, destructive (sabotage) mind, collusion, unacceptable and uncontrolled behavior with negative attitudes, and disgruntled, unmotivated, and unhappy employees. A subtle cause includes cultural risk resulting from workforce diversity. Human resources management can play an important role in managing and controlling people risks.

Ineffective preemployment screening practices and improper employee reference-checking practices expose a company to greater people risk. But these practices must be conducted safely (i.e., legally and ethically) or they can lead to potential legal risks in the form of lawsuits over discrimination, retaliation, and defamation.

The goal is to conduct these practices without jeopardizing employees' privacy and legal rights. The scope of these practices include checking new employees' education, work experience, work habits, and reasons for leaving earlier employment, and discussing departed employees with companies that are thinking of hiring them. If these practices are conducted negligently or not conducted at all, they can lead to hiring incompetent employees with poor performance records or misconduct (e.g., sexual harassment), and increase the threat of workplace violence, theft, and fraud.

Best practices to reduce people risks include (1) installing a Chief People (Human Resources) Officer, (2) performing employee background checks, (3) establishing policies, controls, and procedures approved by the legal department to ensure consistency and fairness in handling employee reference requests (i.e., giving and getting references), (4) balancing between getting too much information and too little information when obtaining references about prospective employees, (5) balancing between giving too much information and too little information when responding to a reference request about former employees, (6) providing training, development, and educational programs or courses to employees taught by training consultants or corporate university staff, (7) installing coaching and mentoring methods, (8) establishing individual and/or group incentives, (9) providing fair and equitable pay and salaries, (10) respecting individuals while keeping diversity in mind, (11) empowering employees, (12) achieving a ranking as one of the best places to work, (13) installing a Chief Learning Officer to improve employees' performance and productivity, and (14) conducting human capital audits, special management reviews, and self-assessment reviews periodically and proactively to reduce people risks.

(ii) Managing Risk. If people are the major root cause of most problems in an organization, managing is next in line because managing is done by and through people. The need to manage risk stems from the inability or incompetence of managers and executives when it comes to controlling risks and managing and implementing new programs, new projects, new business acquisitions, new products, new policies, new procedures, new processes, and new technology. Managing risk also comes from not exhibiting leadership skills.

Best practices to reduce managing risks include (1) installing a General Manager for a business unit or division, (2) performing basic management functions such as plan, direct, organize, and control tasks, (3) learning and applying hard and soft skills, (4) learning time-management and leadership skills, and (5) conducting management audits, special management reviews, and self-assessment reviews periodically and proactively to reduce managing risks.

(iii) Strategic and Business Risk. Strategic risk comes from not executing the business strategic plan properly and in a timely fashion, and from managers and nonmanagers' pursuing goals that are incongruent with those of the organization. It also arises from changes in the internal and external environments. It is a big risk because of its especially large impact on an organization's mission.

Best practices to reduce strategic and business risks include (1) installing a Chief Strategist, (2) developing a strategic management process, (3) performing management functions such as plan, organize, direct, and control tasks, (4) learning and applying hard and soft skills, and (5) conducting strategic management process audits, special management reviews, and self-assessment reviews periodically and proactively to reduce strategic and business risks.

(iv) Financial and Economic Risk. Financial risk arises from many sources, since most corporate risks are eventually translated into money so senior management can understand the risks better. A financial risk is that cash inflows and outflows will not be synchronized.

Sources of financial and economic risks include (1) interest rate risk resulting from changes in interest rates, (2) credit risk resulting from changes in credit ratings for bonds, (3) exchange rate risk resulting from changes in foreign currency exchange rates, (4) investment risk resulting from off–balance sheet accounting practices (a hidden financial risk), (5) financial reporting risk resulting from financial restatements or misstated financial results, (6) fraud risk resulting from misconduct of managers, nonmanagers, and outsiders, (7) mergers-and-acquisition risks resulting from not executing the merger or acquisition properly or ethically leading to penalties and punishments, (8) tax risk resulting from misinterpretation of the tax code, paying less in taxes than required, or taking deductions that are not allowed by the tax code, resulting in a tax liability, (9) revenue risk resulting from overstated reporting of sales, management-misdirected sales, errors in sales reporting due to improper sales cutoff, (10) cost risk from project cost overruns due to low estimates at the start and unexpected additional costs later, (11) speculative risk, such as hedging techniques and use of derivatives, (12) audit risk resulting from the inability of the auditor to detect fraud, not considering the risks the audited organization is facing, issuing an incorrect opinion on the financial statements, and conducting the audit work negligently and unprofessionally, (13) liquidity risk resulting from the inability to pay bills and meet other financial obligations when due, (14) market risk, which

is the part of an investment security's risk that cannot be eliminated by diversification, (15) portfolio risk, which is connected with an investment when it is held in combination with other assets, and (16) leverage risk resulting from excessive debt.

Best practices to reduce financial and economic risks include (1) installing a Chief Financial Officer, (2) developing financial policies, procedures, and standards, (3) providing honest financial reporting with integrity attached, (4) conducting training classes on tax laws and code, (5) using forensic accounting and auditing techniques to detect and investigate fraud, (6) developing a culture of controls, and (7) conducting financial audits, compliance audits, management reviews, and control self-assessment reviews periodically and proactively to reduce financial and economic risks.

(v) Product and Service Quality Risk. Quality risk results from producing inferior quality products, which in turn, increases warranty costs and product recall costs. Risk also results from delivering poor quality services to customers.

Best practices to reduce product and service quality risks include (1) installing a Chief Quality Officer, (2) implementing ISO 9000 and 14000 Series Standards and Six-Sigma approaches, (3) installing statistical process control (SPC) techniques, (4) implementing quality-management tools, and (5) conducting product and service quality audits, management reviews, and quality self-assessment reviews periodically and proactively to improve product and service quality.

(vi) Production and Process Risk. Production risk results from not adhering to product design specifications and not following the generally accepted world-class manufacturing best practices. There could be a mismatch between the changes to engineering drawings (blueprints) and the final product design specifications. It also includes manufacturability risk, ignoring product safety requirements, manufacturing errors, delays due to unavailability of materials, and disruption in the supply chain. Purchasing risk results from purchasing wrong materials and parts, buying materials and parts that are of inferior quality, or buying more quantity than what is needed. Processes are used to manufacture a product, in that process design will affect the product design and vice versa.

Best practices to reduce production and process risks include (1) installing a Chief Manufacturing Officer, (2) installing a Chief Design Officer, (3) installing a Chief Procurement Officer, (4) designing for manufacturability, (5) designing for quality, (6) designing for environment, (7) designing for safety, (8) establishing long-term contracts with suppliers, (9) conducting training classes for production staff and product engineers, and (10) conducting operations audits, management reviews, and self-assessment reviews periodically and proactively to reduce production and process risks.

(vii) Service and Process Risk. Service risk results from providing poor or delayed service to customers, leading to dissatisfied customers and eventually lost customers. The net result is increased warranty costs and service cost refunds. Processes are used to deliver a service in that process design will affect the service design and vice versa.

Best practices to reduce service and process risks include (1) installing a Chief Service Officer, (2) installing a Chief Design Officer, (3) installing a Chief Procurement Officer, (4) implementing service industry standards, (5) conducting benchmarking studies, and (6) conducting service audits, management reviews, and self-assessment reviews periodically and proactively to reduce service and process risks.

(viii) Organizational Risk. Organizational risk is the mismatch between organizational structure and business strategy. It also deals with whether management is forward-looking or not or whether organizational culture meets the competitive environment. Organizational risk can also result from (1) goal-incongruent behavior by employees, (2) improper reporting relationships, and (3) unclear lines of responsibility and accountability.

Best practices to reduce organizational risks include (1) installing a Chief Organization Development Officer, (2) cultivating corporate culture, (3) designing proper organizational structure and reporting relationships, (4) encouraging innovation and creativity, (5) linking the business unit/division mission and strategy to the corporate mission and strategy through active employee participation and direct involvement, and (6) conducting organizational and culture audits, management reviews, self-assessment reviews, and employee surveys periodically and proactively to reduce organizational risks.

(ix) Contract Risk. Contract risk results from not complying with the contractual terms and conditions, leading to default, penalties, and late deliveries. Contract risk leads to financial and legal risks.

Best practices to reduce contract risks include (1) installing a Contract Officer, (2) involving the Chief Legal Officer and his/her staff in developing and reviewing the contracts for language, terms, and conditions, (3) installing project management controls, (4) monitoring the contractor's performance, and (5) conducting contract audits, project management reviews, and self-assessment reviews periodically and proactively to reduce contract risks.

(x) Information Risk. Information risk stems from lack of quality, objectivity, utility, and integrity in information and information technology (IT) systems, whether manual or automated. One example is that old technology will cease to meet the system requirements at some point during the system life. Another example is use of inappropriate hardware and software technologies and architectures. Information risk also includes general and application risks resulting from inadequate controls in IT and user functions. Intelligence-based company information can be stolen to blackmail the company for money or sold to competitors for financial gain.

Best practices to reduce information risks include (1) installing a Chief Information Officer, (2) developing an IT corporate governance framework, (3) conducting IT risk assessments and evaluations, (4) establishing general controls and application controls, (5) complying with the Information Quality Act (IQA), (6) installing strict controls over taking company data home even for business purpose, and (7) conducting technical IT audits, reviews of IT general and application controls, industry surveys, benchmarking studies, special management reviews, and technical self-assessment reviews periodically and proactively to reduce information risks.

(xi) Trade Risk. Trade risk results from violating transborder data-flow rules and not complying with trade laws and regulations, whether international or belonging to a specific country. Trade risks can increase tariff and nontariff costs to the importing country.

Best practices to reduce trade risks include (1) involving the Chief Globalization Officer in trade dealings, (2) complying with the international trade laws and regulations,

both for importing and exporting countries, (3) understanding the global economic, political, and cultural environments, and (4) conducting trade audits, management reviews, and self-assessment reviews periodically and proactively to reduce trade risks.

What are Transborder Data Flows and Privacy?

Transborder data flows can be defined as the movement and storage of data by automatic means across national or federal boundaries. These data flows deal with global privacy. International data networks, connecting thousands of terminals, make it possible to exchange all kinds of data within a minimum of time and without respecting national frontiers.

In general, such transborder activity is composed of three elements: (1) the database of origin (the initial system from where the data is communicated), (2) the transmission mechanism (a through-flow station), and (3) the database of destination (the final destination and storage of the transmitted data, ready for use). Often the flow of information passes through several stations. For instance, the land of destination sometimes has no facilities to process the information, so the data is first sent to another country.

As a result, data should not be encrypted when it is flowing over some borders. One approach taken is to transmit a copy of such data unencrypted along with the encrypted data without detracting from the telecommunications system's ability to preserve its integrity.

(xii) Control Risk. When controls are lax and not followed, fraudulent activities can take place and employees may take advantage of the system's weaknesses. Proper design and implementation of effective controls can reduce risks.

Best practices to reduce control risks include (1) installing a Chief Audit Executive to conduct internal audits within the company to evaluate and monitor the effectiveness of control systems, (2) installing a Controller position in business units or divisions for establishing and monitoring the effectiveness of accounting controls, (3) implementing controls such as directive, preventive, detective, corrective, and compensating controls, (4) motivating and educating employees to reduce the temptation to perpetuate fraud and to cultivate a culture of controls, and (5) conducting control audits, management reviews, and control self-assessment reviews periodically and proactively to reduce control risks.

(xiii) Research and Development Risk. Research and development (R&D) risk results when R&D staff and product engineers design and develop new products without a real understanding of the marketplace or of customers' needs. Lack of innovation or lack of encouragement for innovation also increase R&D risk.

Best practices to reduce R&D risks include (1) installing a Chief R&D Officer, (2) gathering information about customer requirements through the use of Voice of the Customer (VOC) and Quality Function Deployment (QFD) techniques, (3) informing the product development team about the results of VOC and QFD, (4) providing marketing training to R&D staff and product engineers, and (5) conducting R&D audits, management reviews, and technical self-assessment reviews periodically and proactively to reduce R&D risks.

(xiv) Technology Risk. Technology risk centers on whether the organization is using leading-edge technology or not. Technology risk can affect security risk because the technology could be new and unproven, which makes security difficult to implement. Leading-edge, bleeding-edge, cutting-edge, and whiz-bang technologies should be looked

at carefully, as they may not have real use, may not yield fair return on investment (ROI), or may cause implementation risks.

Best practices to reduce technology risks include (1) installing a Chief Technology Officer, (2) separating hype from help, (3) separating fact from opinion, (4) deploying proven technologies, (5) performing cost-benefit analysis, SWOT (strengths, weaknesses, opportunities, and threats) analysis, gap analysis, option analysis, and ROI analysis as part of initial justification, and (6) conducting technology audits, management reviews, and technology self-assessment reviews periodically and proactively to reduce technology risks.

(xv) Digital and Security Risk. *Digital risk* results from Internet activities such as cyber incidents and violation of intellectual property (IP) rights, copyrights, trademarks, and patents. *Security risk* arises when computer systems, networks, users, and outsiders are not complying with established security policies, procedures, rules, and standards, or when security policies, procedures, rules, and standards are not adequate or are not communicated properly to all employees. Digital risks and security risks are related to each other, which can lead to loss of revenues and reputation.

Best practices to reduce digital and security risks include (1) installing an Information Security Officer, (2) developing an IT security governance framework, (3) involving the Chief Risk Officer in the development and communication of digital policy, (4) deploying proven security technologies on the Internet, (5) conducting threat, vulnerability, and risk assessments periodically, (6) integrating physical security, network security, personnel security, and information security across the entire organization by creating a "culture of security," (7) developing consistent security procedures across business partners, suppliers, vendors, franchisees, and customers, (8) installing preventive, detective, and corrective security controls over facilities, employees, outsiders, systems, data, and processes, (9) communicating security policies to all employees in an easily understandable manner, (10) penetrating computer systems with the use of "red team" or "tiger team" security testing concepts, (11) implementing national and international security standards (e.g., NIST and ISO 17799 respectively), and (12) conducting digital and security audits, special management reviews and investigations, and self-assessment reviews periodically and proactively to reduce digital and security risks.

(xvi) Project and Program Risk. Project/program risk is viewed from schedule and technical aspects. *Schedule risk* is evaluated for the extent to which a project is subject to unexpected delays in meeting the technical objectives of the system, regardless of cost. Items of concern include lack of technical skills, lack of enough user/IT staff, or lack of physical facilities. Further, delays in budgeting and acquisition cycles must be considered.

Technical risk is evaluated for the probability that it will be difficult for a project to achieve all or part of the technical objectives due to unforeseen problems, regardless of cost or schedule. This includes management and user-acceptance risks as well as those of a purely technical nature. Generally, the alternative that is closest to the status quo and presents the least extension of the state of the art presents the least exposure to such risks.

Best practices to reduce project and program risks include (1) installing a Project/Program Manager, (2) developing work breakdown structure (WBS) techniques,

(3) using program evaluation and review technique/critical path method (PERT/CPM) project-planning methods, (4) issuing regular project status reports, (5) monitoring project team member and contractor performance, and (6) conducting project audits, project management reviews, and project self-assessment reviews periodically and proactively to reduce project and program risks.

(xvii) Communications Risk. Communications risk is the inability of employees or management to communicate or listen effectively, which leads to wrong interpretation of information and inappropriate actions.

Best practices to reduce communications risks include (1) installing a Chief Communications Officer or its equivalent, (2) developing multidimensional communication formats (e.g., top-down, bottom-up, diagonal, and horizontal directions), (3) providing training courses in effective listening and communication techniques, (4) issuing newsletters to employees to share company performance matters, and (5) conducting communication audits, management reviews, self-assessment reviews, and employee surveys periodically and proactively to reduce communications risks.

(xviii) Regulatory and Reputation Risk. Regulatory risk arises from noncompliance with laws, regulations, executive orders, directives, circulars, bulletins, or ordinances, with reputation risk being the chance of adverse publicity as a result of the noncompliance. Regulatory risk is related to reputation (image) risk in that noncompliance with laws and regulations will tarnish the reputation of an organization.

Best practices to reduce regulatory and reputation risks include (1) installing a Chief Compliance Officer or its equivalent, (2) thoroughly understanding the applicable laws and regulations, (3) establishing communication systems with regulators and government authorities, (4) conducting training classes in laws and regulations, and (5) conducting compliance audits, special management reviews, and self-assessment reviews periodically and proactively to reduce regulatory and reputation risks.

(xix) Environmental Risk. Environmental risk comes from not complying with laws and regulations regarding water contamination and air pollution.

Best practices to reduce environmental risks include (1) installing an Environmental Officer or its equivalent, (2) understanding environmental laws and regulations, (3) implementing ISO 14000 Standards and the industry standards, and (4) conducting environmental audits, special management reviews, and self-assessment reviews periodically and proactively to reduce environmental risks.

(xx) Outsourcing Risk. Outsourcing risks results from when the outsourced vendor delivers poor-quality products and services, delivers completed projects that do not meet requirements and specifications, or incurs cost overruns and time delays.

Best practices to reduce outsourcing risks include (1) establishing a Contract Officer for outsourcing projects, (2) developing fully executed contract in conjunction with corporate legal department, (3) inserting a "right to audit" clause in the contract, (4) monitoring the outsourced vendor with periodic progress reports and on-site visits, and (5) conducting outsourcing vendor audits, performance reviews, and vendor self-assessment reviews periodically and proactively to reduce outsourcing risks.

(xxi) Privacy Risk. Privacy risk originates from divulging or releasing personal financial information, personal medical information, trade secret formulas, and other sensitive information (e.g., salaries) about an individual to unauthorized parties.

Best practices to reduce privacy risks include (1) installing a Privacy Officer or its equivalent, (2) developing and communicating privacy policies that contain consequences for not complying with the policy, (3) understanding privacy laws and regulations, (4) implementing policies and procedures for controlling and releasing personal information to third parties, (5) subjecting new employees to orientation classes by the human resources department, and (6) conducting privacy audits, special management reviews, and privacy self-assessment reviews periodically and proactively to reduce privacy risks.

Some examples of U.S. privacy laws and regulations include (1) the Fair Credit Reporting Act, which protects consumer report information, (2) the Gramm-Leach-Bliley Financial Modernization Act of 1999, which protects nonpublic personal information collected and used by financial institutions, (3) the Health Insurance Portability and Accountability Act (HIPAA) of 1996, which protects health information collected by health plans, health care clearinghouses, and health care providers, and (4) the Federal Trade Commission, which is responsible for ensuring consumer protection and market competition.

An example of international privacy law is the European Union's directive concerning the transfer of data over countries. The directive mandates that companies engaging in transborder data flow maintain an "adequate level" of protection for such data.

(xxii) Implementation and Operational Risk. Implementation risk results from poor practices in installing a new business strategy, a new computer system, program, or project; establishing a new policy, procedure, or service; or assimilating a new business into an existing one. These risks also arise when a change is not properly and timely implemented. Also, when implementation efforts are inadequate, inefficient, or incomplete, operational risks will increase in that people may not use a new computer system or use it in a wrong way. Operational risks follow the implementation risks.

Best practices to reduce implementation and operational risks include (1) installing an Implementation or Operational Officer, (2) developing standard operating procedures (SOP) and instructions for employees to follow, (3) developing computer system design and operation manuals, (4) performing testing, validation, and verification methods for new computer systems, (5) providing training on how to use a new system, policy, or procedure, (6) providing due diligence guidelines for acquiring new businesses, and (7) conducting implementation and operational audits, management reviews, and self-assessment reviews periodically and proactively to reduce implementation and operational risks.

(xxiii) Marketing and Sales Risk. Marketing and sales risk stems from the inability to promote, advertise, or sell the products created, designed, or developed by scientists, researchers, or engineers. It also includes risks resulting from price fixing, disruption in the supply chain, or using illegal telemarketing practices.

Best practices to reduce marketing and sales risks include (1) installing a Chief Marketing Officer, (2) gathering information about customer requirements for products (i.e., use Voice of the Customer [VOC] and quality function deployment [QFD] techniques), (3) informing the product development and R&D teams about the results of VOC

and QFD, (4) providing product training to marketing and sales staff, (5) integrating marketing and sales functions, (6) establishing a Chief Telemarketing Officer, and (7) conducting routine marketing and sales audits, customer perception audits, special management reviews, and self-assessment reviews periodically and proactively to reduce marketing and sales risks.

(xxiv) Nature and Catastrophic Risks. Nature and catastrophic risks result from tornadoes, hurricanes, earthquakes, fire, floods, storms, rain, water leakages, power outages (e.g., blackouts and brownouts), wind-related accidents, and other emergencies.

Best practices to reduce nature and catastrophic risks include (1) installing a Contingency Officer or its equivalent, (2) developing crisis-management plans, (3) installing emergency-preparedness programs, (4) developing business continuity, contingency, and communication plans for the entire organization (i.e., Plan A, Plan B, or Plan C), (5) acquiring traditional insurance coverage, and (6) conducting catastrophic audits, crisis-management reviews, emergency-preparedness drills, and emergency-readiness self-assessment reviews periodically and proactively to reduce nature and catastrophic risks.

(xxv) Legal and Reputation Risk. Similar to financial risks, many sources for legal risks exist including (1) not complying with health and safety regulations (e.g., Occupational Safety and Health Act [OSHA] regulation in the United States), (2) employee and contractor sexual harassment complaints, (3) employee age discrimination suits, (4) inability to prevent employees from using illegal software, (5) patent violations, (6) contract-related lawsuits, (7) product liability suits, (8) product recalls, (9) product tampering, (10) employee criminal acts, (11) conflict-of-interest situations, and (12) other illegal activities.

Legal risk is related to reputation (image) risk, similar to that associated with regulatory risk, because of the adverse publicity that can arise from special investigations and government inquiries.

Best practices to reduce legal and reputation risks include (1) installing a Chief Legal Officer or its equivalent, (2) providing in-house training classes to employees by legal and human resource departments to comply with applicable laws and regulations, (3) providing guidelines on acquiring and installing software from reputable vendors, (4) providing guidelines regarding downloading of official software, (5) restricting employees bringing software to work from their home, (6) restricting employees taking company data and software to home even for company use, and (7) conducting legal audits, compliance audits, audits of illegal software, legal management reviews, and legal self-assessment reviews periodically and proactively to reduce legal and reputation risks.

(xxvi) International Risk. International risk is the combination of political, economic, and cultural risks associated with conducting business in a foreign country. Political risk pertains to government instability and the prospect of asset expropriation; economic risk pertains to currency fluctuations, interest rate changes, and the like; and cultural risk pertains to special problems that may be posed by a given country's way of life. For example, the cultures of some countries may prevent implementation of security controls

because people believe in trusting one another. More is said about international risks in Chapter 12.

Best practices to reduce international risks include (1) installing a Chief Globalization Officer, (2) working with government authorities in streamlining international trade laws and regulations, (3) providing training to employees in understanding international laws, regulations, and culture, and (4) conducting global audits, global management reviews, and global self-assessment reviews periodically and proactively to reduce international risks.

(e) RISK MANAGEMENT TOOLS. Measuring risk can be difficult, and in practice a variety of approaches are used. These include simply adjusting costs up or benefits down; adjusting risk levels, dollar amounts, and probabilities; and using statistical modeling and Monte Carlo simulation. A few of the more commonly used tools and techniques include business-impact analysis, cost-benefit analysis, SWOT analysis (situation analysis), sensitivity analysis, gap analysis, option analysis, economic analysis, expected-value analysis, and subjective scoring. It is a good business practice to combine quantitative methods with the qualitative techniques to obtain broad perspectives.

(i) Business Impact Analysis. A business impact analysis (BIA) is a critical step to understanding the impact of various threats, exposures, and risks facing an organization. This analysis can be applied to any business function, operation, or mission. The results of the BIA are then integrated into business strategies, plans, policies, and procedures.

(ii) Cost-Benefit Analysis. To allocate resources and implement cost-effective security controls, organizations, after identifying all possible controls and evaluating their feasibility and effectiveness, should conduct a cost-benefit analysis for each proposed control to determine which controls are required and appropriate for their circumstances.

The cost-benefit analysis can be qualitative and quantitative. Its purpose is to demonstrate that the costs of implementing the controls can be justified by the reduction in the level of risk. A cost-benefit analysis for proposed new controls or enhanced control encompasses the following:

- Determining the impact of implementing the new or enhanced controls
- Determining the impact of *not* implementing the new or enhanced controls
- Estimating the costs of the implementation. These may include hardware and software purchases; reduced operational effectiveness if system performance or functionality is reduced for increased security; cost of implementing additional policies and procedures; cost of hiring additional personnel to implement proposed policies, procedures, or services; training and maintenance costs.
- Assessing the implementation costs and benefits against system and data criticality to determine the importance of the organization of implementing the new controls, given their costs and relative impact

The organization will need to assess the benefits of the controls in terms of maintaining an acceptable mission posture for the organization. Just as there is a cost for implementing a needed control, there is a cost of not implementing it. By relating the result of not implementing the control to the mission, organizations can determine whether it is feasible to forgo its control implementation.

(iii) SWOT Analysis. The scope of situation or SWOT analysis includes an assessment of an organization's key Strengths (S), Weaknesses (W), Opportunities (O), and Threats (T). It considers several factors such as the firm itself, the organization's industry, the competitive position, functional areas of the firm, and management of the firm.

(iv) Sensitivity Analysis. Sensitivity analysis includes scenario (what-if) planning and simulation studies. Sensitivity analysis indicates how much change in outputs will occur in response to a given change in inputs. As applied to investments, it indicates how much an investment's return (or net present value, NPV) will change in response to a given change in an independent input variable, with all other factors held constant. This technique can be used on one variable at a time, or on a group of variables (sometimes referred to as scenario analysis). Typically, investment returns are more sensitive to changes in some variables than to changes in others.

(v) Gap Analysis. Gap analysis determines the difference between the actual outcome and the expected outcome. The gap can be reduced, though not eliminated, through strategies, contingency plans, and specific action steps after identifying the root causes of the gap.

(vi) Option Analysis. Options analysis is more a framework for critical thinking than a model. It requires analysts to ask if all options for managing uncertainty have been considered. Options analysis may be subdivided into sequential decision analysis and irreversible investment theory.

(vii) Economic Analysis. The scope of economic analysis includes break-even analysis, capital budgeting analysis (e.g., payback period, net present value [NPV], internal rate of return [IRR], and profitability index), and financial ratio analysis (e.g., return on investment [ROI], return on quality [ROQ], return on assets [ROA], and return on sales [ROS]). The analysis mainly deals with quantitative data in terms of dollars and ratios.

(viii) Expected Value Analysis. Expected value analysis involves the assignment of probability estimates to alternative outcomes and summing the products of the various outcomes. For example, the price of crude oil per barrel today is \$10.80 and there is a 25% probability of the price rising to \$11.50 in the next year, a 25% chance it will fall to \$10.50, and a 50% chance of a slight increase to \$11.00. The expected value (EV) of the future price of one barrel of crude oil would be:

$$\text{EV} = 0.25 \times \$11.50 + 0.25 \times \$10.50 + 0.50 \times \$11.00 = \$11.00$$

(ix) Subjective Scoring. Subjective scoring involves assigning weights to responses to questions addressing areas that may introduce elements of risk. The resulting risk score may be just one component of an overall subjective project or investment evaluation. Evaluation criteria are individually weighted to reflect their concept of inherent risk. Identified risk factors should be limited to a few points for manageability and understandability and for meaningful interpretation of the results.

(x) Quantitative and Qualitative Methods. Organizations should use both quantitative and qualitative methods to obtain a comprehensive picture of risks. *Quantitative methods* include five specific approaches: exposure factor, single loss exposure value, annualized rate of occurrence, probability of loss, and annualized loss expectancy.

(A) Exposure Factor

This risk metric provides a percentage measure of potential loss—up to 100% of the value of the asset.

(B) Single Loss Exposure Value

Single loss exposure value is computed by multiplying the asset value with the exposure factor. This risk metric presents the expected monetary cost of a threat event. For example, an earthquake may destroy critical information technology and communications resources, thereby preventing an organization from billing its clients for perhaps a week—until replacement resources can be established—even though the necessary information may remain intact.

Financial losses from a single event could be devastating. Alternatively, the threat of operational errors costing individually from hundreds to a few thousands of dollars—none devastating or even individually significant—may occur many times a year with a significant total annual cost and loss of operational efficiency.

(C) Annualized Rate of Occurrence

Threats may occur with great frequency, rarely, or anywhere in between. Seemingly minor operational threats may occur many times every year, adding up to substantial loss, while potentially devastating threats, such as a once-in-a-100-years flood, fire, or hack that destroys critical files, may occur only rarely. Annualizing threat frequency allows the economic consequences of threat events to be addressed in a sound fiscal manner, much as actuarial data for insurance enables insurance companies to provide valuable, and profitable, services to their clients.

(D) Probability of Loss

Probability of loss is the chance or likelihood of expected monetary loss attributable to a threat event. For example, loss due to operational error may extend from a 1/10 chance of losing $10 million annually to a 1/100 chance of losing $1 billion annually, provided the right combinations of conditions are met. Note that there is little utility in developing the probability of threat events for anything but relatively rare occurrences. The annualized probable monetary loss can be useful in budgeting.

(E) Annualized Loss Expectancy

The simplest expression of annualized loss expectancy is derived by multiplying the annualized rate of occurrence (i.e., threat frequency) with the single loss exposure value. For example, given an annual rate of occurrence of one-tenth and a single loss exposure of $10 million, the expected loss annually is $0.10 \times \$10 \text{ million} = \$1 \text{ million}$. This value is central in the cost-benefit analysis of risk mitigation and in ensuring proportionality in resources allocated to protection of assets.

Qualitative methods include the judgment and intuitive (gut feel) approach, checklists, self-assessments, focus groups, interviews, surveys, and the Delphi technique. In

the Delphi technique, subject matter experts (SMEs) present their own views of risks independently and anonymously, with the views then centrally compiled. The process is repeated until consensus is obtained. The Delphi technique is a method used to avoid *groupthink*, as SMEs do not meet face-to-face to make decisions.

(f) MANAGING CORPORATE RISKS. The following four best practices should be implemented to manage corporate risks on an ongoing basis.

1. *Manage Existing Safeguards and Controls.* The day-to-day management of existing safeguards and controls ranges from robust access control for information assets, to enforcement of systems development standards, to awareness and management of the physical environment and associated risks. Many other essential areas of safeguard and control must be administered and practiced daily. These include, but are not limited to, personnel procedures, change control, information valuation and classification, and contingency planning.
2. *Periodically Assess Risks.* In order to determine whether all necessary and prudent safeguards and controls are in place and efficiently administered, associated risks must be assessed periodically, preferably with quantitative risk assessment. An insecure information-technology environment may appear on the surface to be securely administered, but quantitative risk assessment can reveal safeguard or control inadequacies. Effective application of the results of that assessment, through risk mitigation and associated cost/benefit analysis, can lead to the assurance of efficient safeguard or control the organization assets and improved bottom-line performance.
3. *Mitigate Risks by Implementing and Efficiently Administering Safeguards and Controls.* It is important to remedy situations where risk assessment shows that safeguards or controls are not in place or are not effectively administered.
4. *Risk Assessment and Strategic Planning.* Quantitative risk assessment, applied in the consideration of alternative strategic plans, can reveal unacceptable risks in an otherwise sound business case. Failure to assess the risks associated with alternative strategic plans can result in the implementation of plans at significant monetary loss. That loss is a consequence of being unaware of, or inadequately considering, risks.

2.12 APPLICABLE LAWS, REGULATIONS, STANDARDS, AND PRINCIPLES

Organizations have a legal and ethical obligation to comply with the various federal, state, and local laws, regulations, circulars and bulletins, directives and executive orders, government orders, and ordinances pertinent to a specific business area. Noncompliance with these laws and regulations can lead to fines, civil and/or criminal penalties, probation, and jail punishments (prison time), thus creating reputation (image) risk. Compliance with industry and/or organization standards, including professional standards, can increase the quality of products and services, which, in turn, can enhance an organization's reputation and image in the marketplace. Adherence to generally accepted business principles and practices could have a similar effect as complying with standards.

A brief roundup of information about major laws, regulations, and standards is provided here as a reminder for checklist purpose. Note that these laws and regulations are subject to change as new ones are added and existing ones are amended or repealed. The reader is advised to obtain the original laws, regulations, and standards from the official sources for a better understanding of the provisions, requirements, and conditions of the laws, regulations, and standards (www.regulations.gov). Although some of the following laws, regulations, and standards directly affect the public sector organizations (i.e., government agencies), private-sector organizations can read, learn, and apply them to improve their business operations on a proactive basis.

U.S. organizations should comply with the following laws and regulations pertinent to corporate governance:

Sarbanes-Oxley Act. Exhibit 2.2 presents a summary of selected Sarbanes-Oxley (SOX) Act provisions affecting public companies and registered accounting firms. For a full text of the SOX act, visit www.aicpa.org or www.pcaobus.org.

Responding to corporate failures and fraud that resulted in substantial financial losses to institutional and individual investors, the U.S. Congress passed the Sarbanes-Oxley Act in 2002. As shown in Exhibit 2.2, the Act contains provisions affecting the corporate governance, auditing, and financial reporting of public companies, including provisions intended to deter and punish corporate accounting fraud and corruption. The SOX act generally applies to those companies required to file reports with SEC under the Securities Exchange Act of 1933 and the Securities Exchange Act of 1934.

Title I of the SOX act establishes the Public Company Accounting Oversight Board (PCAOB), a private-sector nonprofit organization to oversee the audits of public companies that are subject to the securities laws. PCAOB is subject to SEC oversight. The act gives PCAOB four primary areas of responsibility:

1. Registration of accounting firms that audit public companies in the U.S. securities markets
2. Inspections of registered accounting firms
3. Establishment of auditing, quality control, and ethics standards for registered accounting firms
4. Investigation and discipline of registered accounting firms for violations of law or professional standards

Title II of the Act addresses auditor independence. It prohibits the registered external auditor of a public company from providing certain nonaudit services to that public company audit client. Title II also specifies communication that is required between auditors and the public company's audit committee (or board of directors) and requires periodic rotation of the audit partners managing a public company's audits.

Titles III and IV of the Act focus on corporate responsibility and enhanced financial disclosures. Title III addresses listed company audit committees, including responsibilities and independence, and corporate responsibilities for financial reports, including certifications by corporate officers in annual and quarterly reports, among other provisions. Title IV addresses disclosures in financial reporting and transactions

Section 101: Public Company Accounting Oversight Board Establishment.
Establishes the Public Company Accounting Oversight Board (PCAOB) to oversee the audit of public companies that are subject to the securities laws.

Section 102: Registration with PCAOB.
Requires accounting firms that prepare or issue audit reports to public companies to register with PCAOB.

Section 103: Auditing, Quality-Control, and Independence Standards and Rules.
Requires PCAOB, by rule, to establish auditing and other professional standards to be used by registered public accounting firms in the preparation and issuance of audit reports.

Section 104: Inspections of Registered Public Accounting Firms.
Requires PCAOB to annually inspect registered public accounting firms that have more than 100 issuer audit clients, and to triennially inspect registered public accounting firms that have 100 issuer audit clients or fewer.

Section 105: Investigations and Disciplinary Proceedings.
Requires PCAOB to establish fair procedures for investigating and disciplining registered public accounting firms and associated persons, and authorizes PCAOB to investigate and discipline such firms and persons.

Section 201: Services Outside the Scope of Practice of Auditors.
Prohibits any given registered accounting firm from providing certain nonaudit services to a public company if the firm also serves as auditor of the public company's financial statements. Examples of prohibited nonaudit services include bookkeeping, appraisal or valuation services, internal audit outsourcing services, and management functions.

Section 301: Public Company Audit Committees.
Makes listed company audit committees responsible for the appointment, compensation, and oversight of the registered accounting firm, including the resolution of disagreements between the registered accounting firm and company management regarding financial reporting. Audit committee members must be independent.

Section 302: Corporate Responsibility for Financial Reports.
Establishes that, for each annual and quarterly report filed with the SEC, the company's CEO and CFO must certify (1) that they have reviewed the report, (2) that, based on their knowledge, the report does not contain untrue statements or omissions of material facts resulting in a misleading account, (3) and that, based on their knowledge, the financial information in the report is fairly presented.

Section 304: Forfeiture of Certain Bonuses and Profits.
Establishes that the CEO and CFO of an issuer have to reimburse the issuer for any bonuses or profits from sale of securities during the 12-month period following the filing of a financial document that required an issuer to prepare an accounting restatement due to misconduct.

Section 308: Fair Funds for Investors.
Allows civil penalties to be added to the disgorgement fund set up for victims of a security law violation. A disgorgement sanction requires the return of illegal profits.

Section 404: Management Assessment of Internal Controls.
Requires company management, when filing a company's annual report with the SEC, to state its responsibility for establishing and maintaining an internal control structure and procedures for financial reporting, and to assess the effectiveness of its internal control structure and procedures for financial reporting. The section also requires the registered accounting firm that audits a given company to attest to, and report on, management's assessment of the effectiveness of its internal control over financial reporting.

Section 407: Disclosure of Audit-Committee Financial Expert.
Requires public companies to disclose in periodic reports to the SEC whether their audit committee includes at least one member who is a financial expert, and to explain why if the committee does not.

EXHIBIT 2.2 SARBANES-OXLEY ACT SECTIONS

involving management and principal stockholders, and other provisions such as internal control over financial reporting. More specifically, Section 404 of the SOX Act establishes requirements for companies to publicly report on management's responsibility for establishing and maintaining an adequate internal control structure, including controls over financial reporting and the results of management's assessment of the effectiveness of internal control over financial reporting. Section 404 also requires the firms that serve as external auditors for public companies to attest to the assessment made by the companies' management and report on the results of their attestation and whether they agree with management's assessment of the company's internal control over financial reporting.

New York Stock Exchange Corporate Governance Rules. The New York Stock Exchange (NYSE) has issued its corporate governance rules, which were approved by the SEC in 2003. The 12 rules are:

1. Listed companies must have a majority of independent directors.
2. The definition of "independent director" must follow certain standards.
3. To empower nonmanagement directors to serve as a more effective check on management, the nonmanagement directors of each company must meet at regularly scheduled executive sessions without management.
4. Listed companies must have a nominating or corporate governance committee composed entirely of independent directors.
5. Listed companies must have a compensation committee composed entirely of independent directors.
6. Listed companies must have an audit committee that satisfies the requirements of Rule 10A-3 under the Securities Exchange Act of 1934.
7. The audit committee must have a minimum of three members.
8. Listed companies must adopt and disclose corporate governance guidelines.
9. Listed companies must adopt and disclose a code of business conduct and ethics for directors, officers, and employees, and promptly disclose any waivers of the code for directors or executive officers.
10. Listed foreign private issuers must disclose any significant ways in which their corporate governance practices differ from those followed by domestic companies under NYSE listing standards.
11. Each listed company CEO must certify to the NYSE each year that he is not aware of any violation by the company of NYSE corporate governance listing standards.
12. The NYSE may issue a public reprimand letter to any listed company that violates a NYSE listing standard.

For a full text of these rules, visit http://www.nyse.com/pdfs/finalcorpgovrules.pdf

NASDAQ Stock Market Corporate Governance Rules. The NASDAQ stock market has issued its corporate governance rules in 2004. The rules describe (1) criteria for independent directors, (2) qualitative listing requirements for NASDAQ national market and NASDAQ small-cap market issuers except for limited partnerships, (3) voting rights, (4) qualitative listing requirements for NASDAQ issuers that are limited partnerships.

For a full text of these rules, visit http://www.nasdaq.com/about/CorporateGovernance.pdf

National Association of Securities Dealers Rules and Regulations. The National Association of Securities Dealers (NASD) is a world leader in capital markets regulation. NASD licenses individuals and admits firms to the securities industry, writes rules to govern their behavior, examines them for regulatory compliance, and disciplines those whose compliance comes up short. It oversees and regulates trading in equities, corporate bonds, securities futures, and options. It provides education and qualification examinations to industry professionals while supporting securities firms in their compliance activities. For a full text of rules and regulations, visit www.nasd.com and www.finra.org/index.htm.

U.S. Securities Regulations. The primary purpose of U.S. federal securities regulation is to prevent fraudulent practices in the sale of securities and thereby to foster public confidence in the securities market. Federal securities law consists principally of two statutes: the Securities Act of 1933, which focuses on the issuance of securities, and the Securities Exchange Act of 1934, which deals mainly with trading in issued securities. These "secondary" transactions greatly exceed in number and dollar value the original offerings by issuers. The Securities and Exchange Commission (SEC) administers both of these securities acts. (www.sec.gov)

Foreign Corrupt Practices Act. In addition to anti-bribery provisions, the Foreign Corrupt Practices Act of 1977 (FCPA) contains provisions pertaining to accounting and internal control. These provisions require corporate management to maintain books, records, and accounts that accurately and fairly reflect the transactions and dispositions of the corporation's assets, and to devise and maintain a system of internal accounting control adequate to accomplish certain financial objectives. Thus, a key theme underlying the FCPA is that sound internal control should provide an effective deterrent to illegal payments.

Information Quality Act. The Information Quality Act (IQA) of 2001 requires the U.S. Office of Management and Budget (OMB) to issue government-wide guidelines to ensure the quality of information disseminated by federal agencies. The act ensures and maximizes the quality, objectivity, utility, and integrity of information, including statistical information, disseminated to the public. (www.omb.gov)

Sherman Antitrust Act. The Sherman Act of 1890 prohibits actions that are "in constraint of trade" or actions that attempt to monopolize a market or create a monopoly. Legal actions under this Act typically involve price-fixing or other forms of collusion among sellers. However, the law also prohibits reciprocity or reciprocal purchase agreements.

Clayton Antitrust Act. The Clayton Act of 1914 makes price discrimination illegal and prohibits sellers from exclusive arrangements with purchasers and/or product distributors.

Robinson-Patman Act. The Robinson-Patman Act of 1936 further addresses the issue of price discrimination established in the Clayton Act. It prohibits sellers from offering a discriminatory price where the effect of discrimination may limit competition or create a monopoly. There is also a provision that prohibits purchasers from inducing a discriminatory price. While a seller may legally lower price as a concession during

negotiations, the purchaser should not mislead or trick the seller, which would result in a price that is discriminatory to other buyers in the market.

Federal Trade Commission Act. The Federal Trade Commission Act of 1914 authorizes the Federal Trade Commission (FTC) to interpret trade legislation, including the provisions of the Sherman Act that deal with restraint of trade. The Act also addresses unfair competition and unfair or deceptive trade practices.

Goal-Congruence Principle. The goal-congruence principle states that the actions, wills, and needs of employees should be subordinated to the greater good of the organization they work for. An employee should ask himself whether his goals are consistent with the organizational goals.

National Association of Corporate Directors. The Corporate Directors Institute, an institution maintained by the National Association of Corporate Directors (NACD), offers the nationally recognized Certificate of Director Education, as well as continuing education programs for both new and experienced directors. Individuals can earn the Certificate by completing the Director Professionalism course. Certificates are maintained by completing eight credit hours of education annually (www.nacdonline.org).

American Institute of Certified Public Accountants. The American Institute of Certified Public Accountants (AICPA) is a professional organization and is the voice of the public accounting profession. It establishes professional certification (Certified Public Accountant, CPA) and professional standards, such as generally accepted accounting principles (GAAP), generally accepted auditing standards (GAAS), and a code of ethics for public accountants and independent auditors to follow (www.aicpa.org).

Institute of Internal Auditors. The Institute of Internal Auditors (IIA) is a professional organization and is the voice of internal auditing profession worldwide. It establishes professional certifications (CIA and CCSA), professional standards, and a code of ethics for internal auditors to follow. CIA is Certified Internal Auditor and CCSA is Certification in Control Self-Assessment (www.theiia.org).

Information Systems Audit and Control Association. The Information Systems Audit and Control Association (ISACA) is a professional organization and is the voice of the information systems auditing profession worldwide. It establishes professional certification (Certified Information Systems Auditor, CISA), professional standards, and a code of ethics for information systems auditors to follow (www.isaca.org).

Bank Administration Institute. The Bank Administration Institute (BAI) is a professional organization and is the voice of bank internal auditing and risk professionals worldwide. It establishes professional certifications (CBA and CRP), professional standards, and a code of ethics for bank auditors and risk professionals to follow. CBA is Certified Bank Auditor and CRP is Certified Risk Professional (www.bai.org).

Association of Certified Fraud Examiners. The Association of Certified Fraud Examiners (ACFE) is a professional organization and is the voice of fraud examiners. It establishes professional certification (Certified Fraud Examiner, CFE), professional standards, and a code of ethics for fraud examiners to follow (www.cfenet.com).

International Information Systems Security Certification Consortium Institute. The International Information Systems Security Certification Consortium (ISC2) Institute is a professional organization and is the voice of information security profession. It establishes professional certifications (e.g., CISSP and SSCP), professional standards, and a code of ethics for information security practitioners to follow. CISSP is Certified

Information Systems Security Professional and SSCP is Systems Security Certified Professional (www.isc2.org).

American Society for Industrial Security International. The American Society for Industrial Security (ASIS) International is a professional organization and is the voice of industrial security profession. It establishes professional certifications (e.g., CPP and PSP), professional standards, and a code of ethics for industrial security practitioners to follow. CPP is Certified Protection Professional and PSP is Physical Security Professional (www.asisonline.org).

Disaster Recovery Institute International. The Disaster Recovery Institute (DRI) International is a professional organization and is the voice of business continuity practitioners. It establishes professional certifications (e.g., CBCP and others), professional standards, and a code of ethics for business continuity practitioners to follow. CBCP is Certified Business Continuity Professional (www.drii.org).

Additional Resources

Anand, Sanjay. *Essentials of Corporate Governance*. Hoboken, NJ: John Wiley & Sons, 2007.

Anand, Sanjay. *Essentials of Sarbanes-Oxley*. Hoboken, NJ: John Wiley & Sons, 2007.

Charan, Ram. *Boards That Deliver: Advancing Corporate Governance from Compliance to Competitive Advantage*. San Francisco, CA: Jossey-Bass, 2005.

Lipman, Frederick D., with L. Keith Lipman. *Corporate Governance Best Practices: Strategies for Public, Private, and Not-for-Profit Organizations*. Hoboken, NJ: John Wiley & Sons, 2006.

Notes

1. *OECDs Principles of Corporate Governance*, pp. 17–25, 2004, Paris, France: OECD. Reprinted with permission from the Copyright Clearance Center (CCC), acting as authorized copyright administrator for OECD.
2. *Business Roundtable's Principles of Corporate Governance*, pp. 2–3, 2005, Washington, DC: Business Roundtable. Reprinted with permission.
3. This section is reprinted with permission. *OECD Principles of Corporate Governance* (Paris, France: OECD), 58–66. Copyright 2004 by OECD, http://www.oecd.org. Reprinted with permission from the Copyright Clearance Center (CCC), acting as authorized copyright administrator for OECD.
4. This section is reprinted with permission. *Principles of Corporate Governance*, 7–10. Copyright 2005, Washington, DC: Business Roundtable. Http://www.businessroundtable.org/publications/index.aspx.
5. This section is reprinted with permission. *Principles of Corporate Governance*, 10–12. Copyright 2005; Washington, DC: Business Roundtable, http://www.businessroundtable.org/publications/index.aspx.
6. This section is reprinted with permission. *OECD Principles of Corporate Governance* (Paris, France: OECD), 50. Copyright 2004 by OECD, http://www.oecd.org. Reprinted with permission from the Copyright Clearance Center (CCC), acting as authorized copyright administrator for OECD.
7. *The Professional Practices Framework* (Altamonte Springs, Fla.: Institute of Internal Auditors Research Foundation, 2007).
8. This section reprinted with permission. *Audit Committee Effectiveness*: *What Works Best*, third edition (Altamonte Springs, Fla.: Institute of Internal Auditors Research Foundation, 2005), xi–xiv. Copyright 2005.

9. This section is being excerpted by permission of Oxford University Press (OUP). *Gatekeepers: The Professions and Corporate Governance*, John C. Coffee Jr., Oxford University Press, copyright by John Coffee 2006.
10. This section is reprinted with permission. *Internal Control: Integrated Framework*, published by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission. Copyright 2003 by the Committee of Sponsoring Organizations of the Treadway Commission. Reprinted with permission from the Copyright Clearance Center (CCC), acting as authorized copyright administrator for COSO.
11. Portions of this section are reprinted with permission. Internal Control Issues in Derivatives Usage: Executive Summary, published by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission. Copyright 2003 by the Committee of Sponsoring Organizations of the Treadway Commission. Reprinted with permission from the Copyright Clearance Center (CCC), acting as authorized copyright administrator for COSO.
12. This section is reprinted with permission. *Internal Control: Integrated Framework*, published by the Committee of Sponsoring Organizations of the Treadway Commission. Copyright 2003 by the Committee of Sponsoring Organizations of the Treadway Commission. Reprinted with permission from the Copyright Clearance Center (CCC), acting as authorized copyright administrator for COSO.
13. This section is reprinted with permission. *Fraudulent Financial Reporting*, 1987–1997: An Analysis of U.S. Public Companies, published by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission, 1999. Reprinted with permission from the Copyright Clearance Center (CCC), acting as authorized copyright administrator for COSO.
14. J. Edward Ketz, *Hidden Financial Risk: Understanding Off–Balance Sheet Accounting* (Hoboken, NJ: John Wiley & Sons, 2003).
15. *Financial Restatements: Update of Public Company Trends, Market Impacts, and Regulatory Enforcement Activities* (GAO-06-678), July 2006, (Washington, DC: Government Accountability Office).
16. This section is reprinted with permission. Howard M. Schilit, *What Directors Can Do to Prevent and Detect Financial Shenanigans* (Washington, DC: National Association of Corporate Directors, 1994), http://www.nacdonline.org.

CHAPTER 3

CORPORATE-ETHICS BEST PRACTICES

3.1 OVERVIEW

Corporate ethics play an important role in ensuring good corporate governance and better corporate management. Corporate ethics and corporate governance support corporate management. Ethical lapses and dilemmas are one of the root causes of many problems that corporate management is facing today.

Ethics can be defined broadly as the study of what is right or good for human beings. It attempts to determine what people ought to do and what goals they should pursue. Business ethics, as a branch of applied ethics, is the study and determination of what is right and good in business settings. Unlike legal analyses, analyses of ethics have no central authority, such as courts or legislatures, upon which to rely; nor do they follow clear-cut, universal standards. Nonetheless, despite these inherent limitations, it is still possible to make meaningful ethical judgments.

Many business or government situations involve ethics questions, and considering the situations may help to clarify the definition of business and government ethics:

- In the interaction between a company management and investors and the stock market, the company management can manipulate earnings and profits (earnings management) to boost its stock prices and to receive big bonuses when the actual financial results are less than expected.
- In the interaction between a company management and the bond market and the stock market, the company management can hide its debt through off-balance sheet accounting practice to realize higher bond prices and higher stock prices. This practice is unethical although not illegal because GAAP allows it.
- In the interaction between a company management and the board of directors, the company management can pull off financial shenanigans (a form of financial fraud) against the company. The board of directors may not be able to prevent and detect such acts but they are legally liable for such unethical conduct on part of the company management.
- In the interaction between buyers and sellers of a company, both parties may be subject to unethical and illegal tactics to win or lose the business transaction of mergers and acquisitions.
- In the interaction between a pharmaceutical company and a medical researcher, the company management threatens the researcher if he releases negative test results (bad news) to the public about its drugs.
- In the interaction between government attorneys and government executive, attorneys are fired improperly for whistleblowing on government and not following

the executive's unethical instructions despite the Ethics in Government Act and the Whistleblower Protection Act.

- In the interaction between a local oil company and local government officials, the oil company was allowed to dump its toxic substances into a nearby lake, which is used for drinking water, in exchange for creating more local jobs when the oil company expands its plant processing capacity. The toxic substances kill fish and grow seaweed in the lake.
- In the interaction between federal environmental regulators and management of a coal-fired power plant, regulators relaxed rules to allow the very old plant to be reopened after it was closed earlier for generating excessive air pollution. The plant required modernization work to reduce air pollution, and the work was not completed when the plant was reopened.
- In the relationships between employees and employers, many issues arise regarding the safety and compensation of workers, their civil rights (such as equal treatment, privacy, and freedom from sexual harassment), and the legitimacy of whistleblowing. Previous employees working as contractors can raise tax and legal issues.
- In the relationships between business and its customers, ethical issues permeate marketing techniques, product safety, price discrimination, and consumer protection.
- In the relationships between business and its owners, ethical questions involving corporate governance, shareholder voting, and management's duties to the shareholders can pose problems.
- Relationships among competing businesses involve numerous ethical matters, including fair competition and the effects of collusion in matters such as price fixing.
- In the relationships between buyers and vendors, suppliers, contractors, and consultants, showing favors and receiving bribes and expensive gifts are common.
- In the interaction between gatekeepers (e.g., external auditors, attorneys, securities analysts, and investment bankers) and their owners, gatekeepers do not always discharge their professional responsibilities in the financial securities and capital markets due to conflicts of interest, job security, *groupthink*, and greed.
- The interaction between business and society at large presents additional ethical dimensions, such as pollution of the physical environment, commitment to the community's economic and social infrastructure, and depletion of natural resources.
- At the international level, issues such as bribery of foreign officials, exploitation of less-developed countries, and conflicts among differing cultures and value systems are difficult to control and monitor.

3.2 ROLES AND RESPONSIBILITIES OF THE CHIEF ETHICS OFFICER

The Chief Ethics Officer should develop an ethics manual describing policies and procedures on conflict of interests and code of conduct; restrictions regarding accepting or giving gifts and travel by procurement, contracting, marketing, and sales personnel; and rules requiring written disclosures of executives' financial condition and outside earned-income activities; forbidding employment of relatives; protecting the organization's property

and information; describing allowed political contributions and activities, and proper treatment of sale of stock acquired pursuant to exercise of stock options to comply with conflict-of-interest requirements; and restricting the sharing or use of insider information.

The Chief Ethics Officer is a key person in the C-level executive suite and has the following roles and responsibilities:

- Promote a positive ethical climate in the organization through his leadership skills.
- Develop an ethics manual describing company policy, codes of conduct, and expected behavior; reporting of ethical violations; and referencing to all the applicable laws and regulations.
- Annually require each and every employee in the organization to sign a corporate ethics document that lays out the organization's requirements concerning employee ethics and stipulates that the signer has received, read, and understood the document and agrees to abide by its requirements.
- Conduct training classes for managers and nonmanagers in ethical principles, with attention to actions and consequences.
- Work with the internal audit department in developing audit plans and identifying areas of audit that address ethical violations
- Work with the legal department in pursuing cases that violated ethical principles either inside the company (e.g., employees and management) or outside (e.g., customers, suppliers, vendors, and contractors).
- Conduct ethics audits, special management reviews, and self-assessment reviews periodically and proactively to ensure continuous improvement in ethical matters.
- Analyze outside-in views (i.e., views of stakeholders about company management) and inside-out views (i.e., views of company management about stakeholders) to identify disconnections between these views and to integrate them in a coherent manner.

3.3 ETHICAL AND LEGAL PRINCIPLES

(a) OVERVIEW. Ethical and legal principles such as due process, due care, due diligence, and due professional care (which are described below) apply to many business situations covered in this chapter, such as (1) handling shareholders, investors, and creditors, (2) handling stock markets and investment analysts, (3) handling employee complaints and grievances, and employee hiring, promotions, and disciplinary mechanisms, (4) handling labor unions, (5) handling regulators and government authorities, (6) handling suppliers, vendors, contractors, and customers, (7) handling purchasing agents, buyers, or commodity/service experts, and marketing and salespeople (8) handling related parties and third parties, (9) handling business mergers and acquisitions, and (10) addressing corporate social responsibility and accountability.

(b) DUE PROCESS. Due process means following rules and principles so that an individual is treated fairly and uniformly at all times. It also means fair and equitable treatment to all concerned parties. Two types of due process exist: procedural due process and substantive due process. Procedural due process ensures that a formal proceeding is carried out regularly and in accordance with the established rules and principles. Substantive due process deals with a judicial requirement that enacted laws may not contain

provisions that result in the unfair, arbitrary, or unreasonable treatment of an individual. Due process requires due care and due diligence.

(c) DUE CARE AND DUE DILIGENCE. The concepts of due care and due diligence are similar to the "prudent person" concept. Due care means reasonable care, which promotes the common good. It is maintaining minimal and customary practices. Due diligence requires organizations to develop and implement an effective system of controls, policies, and procedures to prevent and detect violation of policies and laws. In other words, due diligence is the care that a reasonable person exercises under a given set of circumstances to avoid harm to other persons or their property. Due diligence is another way of saying due care. Another related concept is good faith, which means showing "honesty in fact" and "honesty in intent."

Examples of due care and due diligence include:

- Acquiring a business insurance policy to protect physical assets against theft, loss, or damage
- Training employees in information security to show that a standard of due care has been taken in protecting information assets
- Requiring statements from employees acknowledging that they have read and understood computer-security requirements
- Good housekeeping in general

(d) DUE PROFESSIONAL CARE. As the name implies, due professional care applies to professionals such as business managers and executives, accountants, auditors, engineers, lawyers, doctors, and others. Individuals should apply the care and skill expected of a reasonable prudent and competent professional during their work. Due professional care does not imply infallibility. Having proper knowledge, skills, and abilities (KSAs) is the major issue here. Due professional care is related to due care and due diligence.

(e) CODES OF CONDUCT. Corporate governance objectives are also formulated in voluntary codes and standards (i.e., codes of conduct) that do not have the status of law or regulation.[1] While such codes play an important role in improving corporate governance arrangements, they might leave shareholders and other stakeholders with uncertainty concerning the codes' status and implementation. When codes and principles are used as a national standard or as an explicit substitute for legal or regulatory provisions, market credibility requires that their status in terms of coverage, implementation, compliance, and sanctions is clearly specified.

World-class organizations have developed a "code of conduct" for their organizations, which should comply with the definition of a "code of ethics" set out in Section 406 (c) of the Sarbanes-Oxley Act of 2002. In addition, the code must provide for an enforcement mechanism and protection for persons reporting questionable behavior (i.e., whistleblowing). The board of directors must approve any waivers of the code for directors, executives, or officers of the organization.

(f) FINANCIAL DISCLOSURES. In the U.S. federal government, the Ethics in Government Act of 1978 requires financial disclosure reporting, which is intended to identify and deter conflicts of interest between federal employees' duties and responsibilities and their personal financial interests and activities. Depending on such matters as the

position held or the amount of compensation, disclosure statements are either to be made available to the public or kept confidential.[2]

Similarly, executives, board of directors, consultants, and contractors working for a private company are required to submit financial information such as stocks and bonds that they hold in the company. They also need to disclose any other conflict-of-interest situations that could impair their independence and objectivity.

3.4 IMPLEMENTING AN ETHICS STRATEGY AND TRAINING PROGRAM

(a) ETHICS STRATEGY. Organizations have taken many different approaches to implementing an ethics strategy.[3] The choice of an approach to ethics in the organization depends, in part, on the objectives of management. Any one or a combination of the following objectives is common.

- To avoid any behavior, legal, or otherwise, that violates company policy and negatively affects its interests
- To satisfy the concerns of company stakeholders and thereby capture the benefits that derive from a reputation for ethical behavior
- To create a culture in which each employee and manager pursues a set of ethical and social values to which the company is firmly committed

The three corresponding approaches for implementing a corporate ethics strategy mark progressive stages in the development of a value-based organization: (1) managing for compliance, (2) managing stakeholder relations, and (3) creating a value-based organization.

(i) Stage 1: Managing for Compliance. Organizations see the tremendous damage that can be done to corporate reputation and momentum by incidents of illegal or blatantly unethical behavior. To prevent such occurrences, the organization establishes a program to ensure compliance with both the law and ethical standards demanded by the public and stakeholders. Such programs include prohibitions against conflicts of interest, theft of company property, and disclosure of trade secrets.

The *primary objective* is to prevent lawbreaking and scandals.

Standards for judging behavior include laws, regulations, and the rights of the corporation.

Strengths of the approach include clear standards and clear penalties for violations.

Weaknesses of the approach include addressing too few issues, hampering empowerment, and possibly implying that the company expects only the minimum.

Action steps include:

- Adopt a code of ethics, practice, or conduct to address specific behaviors.
- Ensure board-level and senior management support.
- Assign responsibility for the ethics and compliance strategy to an appropriate function in the organization.
- Identify and communicate compliance standards.
- Train employees to use compliance standards.
- Establish clear channels of communications.
- Ensure supervision to compliance standards.
- Make periodic reports to senior management and the board of directors.

(ii) Stage 2: Managing Stakeholder Relations. Organizations become increasingly sophisticated and see the long-term value to be gained from maintaining good relations with key stakeholders. Self-interest drives the organization to monitor its reputation among these stakeholders and to initiate programs to address their ethical concerns.

The *primary objective* is to create value by meeting stakeholder expectations.

Standards for judging behavior include stakeholder demands and expectations.

Strengths of the approach include clear payoffs for the organization; stakeholders can be surveyed for expectation and attitudes.

Weaknesses of the approach include the changeability of stakeholder views' with time and location, the probability that some expectations cannot be met, an absence of guidance on many issues, and a lack of clear values behind behaviors.

Action steps include:

- Define corporate stakeholders.
- Evaluate the attitudes and opinions of stakeholder groups.
- Design programs to address stakeholder concerns.
- Audit the effectiveness of stakeholder programs.

(iii) Stage 3: Creating a Value-Based Organization. Many organizations have found it difficult to manage compliance or stakeholder relations without creating a genuine change in corporate culture. As a result, instinct rather than strategy dominates responses to the breadth of ethical issues held important by stakeholders. Such organizations define their values and invest considerable effort and expense in making those values permeate all aspects of their work. They find it productive to make decisions consistent with these values even when short-term payoffs are not apparent. In reality, very few organizations reach this stage.

The *primary objective* is to create an organization that has enduring value.

Standards for judging behavior include the company's own values and beliefs.

Strengths of the approach include bolstering corporate culture, with desired behavior becoming instinctive.

Weaknesses of the approach include the need to wait for a long-term payoff, the high costs needed for implementation, and the possibility that empowered employees may interpret and misinterpret values in their own ways.

Action steps include:

- Define the organization's values.
- Communicate the organization's values.
- Create systems that support corporate values.
- Ensure supervision of corporate values.
- Establish an ethics or corporate values function.
- Assign responsibility for interpreting values.
- Recruit and promote employees of strong moral character.
- Train employees in ethical decision making and application of the values.
- Encourage employees to report behavior inconsistent with the values.
- Reward managers and employee behavior consistent with the values.
- Renew the values.
- Conduct policy and practice reviews.

The establishment of an ethical culture within an organization is essential, not only for the achievement of desired business goals, but also necessary for the proper management of key risks in its business environment.

(b) ETHICS TRAINING. Many organizations choose to design their own ethics-training program for the advantages it provides over other options such as consultant-led or purchased program. Doing so allows the organization to tailor the ethics training program to the industry, market, and company-specific factors that either exist within the organization or exert influence from outside. Regardless of the direction taken, some key considerations for designing an ethics-training program include:

- Define terms. What is an ethics-training program?
- Define objectives. What are the objectives of an ethics training program?
- Decide what to include. What makes up an ethics-training program?
- Decide where to start. How does the organization implement an ethics-training program?
- Decide on training methods. Who provides ethics training?
- Define your audience. Who is the ethics training program directed at?
- Avoid roadblocks. What issues are commonly encountered in designing ethics training programs?
- Test training effectiveness. How does an organization evaluate the effectiveness of its ethics training program?
- Follow up on training. What follow-up should take place after the ethics training program is initiated?

Even if an organization is already an ethical-value-based one that is managing for ethical compliance internally and for good stakeholder relations, adopting an ethics training program offers the opportunity to enhance the content and ensure greater influence in the direction and focus points of the training. As ethics training drives, among other things, the establishment and reinforcement of the organization's values and corporate culture, designing an effective ethics training program to communicate the organization's ethics strategy pays dividends well beyond simply encouraging compliance.

3.5 HANDLING SHAREHOLDERS, INVESTORS, AND CREDITORS

(a) OVERVIEW. Shareholders are investors (owners) of a company, whereas creditors are lenders of money to the company, who is the borrower of money.

(b) HANDLING SHAREHOLDERS AND INVESTORS. Equity investors have certain property rights. For example, an equity share in a publicly traded company can be bought, sold, or transferred. An equity share also entitles the investor to participate in the profits of the corporation, with liability limited to the amount of the investment. In addition, ownership of an equity share provides a right to information about the corporation and a right to influence the corporation, primarily by participation in general shareholder meetings and by voting.[4]

According to Business Roundtable, shareholder value is enhanced when a corporation treats its employees well, serves its customers well, fosters good relationships with

suppliers, maintains an effective compliance program and strong corporate governance practices, and has a reputation for civic responsibility.[5]

Business Roundtable suggests the following guidelines regarding relationships with shareholders and investors:

- Corporations have a responsibility to communicate effectively and candidly with shareholders. The goal of shareholder communication should be to help shareholders understand the business, risk profile, financial condition, and operating performance of the corporation and the board's corporate governance practices.
- Corporations communicate with investors and other constituencies not only in proxy statements, annual and other reports, and formal shareholder meetings, but in many other ways as well. All of these communications should provide consistency, clarity, and candor.
- Corporations should establish effective procedures for shareholders to communicate with the board and for directors to respond to shareholder concerns. The board, or an independent committee such as the corporate governance committee, should establish, oversee, and regularly review and update these procedures as appropriate.
- A corporation's procedures for shareholder communications and its governance practices should be readily available to shareholders. Information about the board's structure and operations, committee composition and responsibilities, corporate governance principles, and code of ethics should be widely disseminated to shareholders.
- The board should be notified of shareholder proposals, and the board or its corporate governance committee should oversee the corporation's response to these proposals.
- Directors should attend the corporation's annual meeting of shareholders, and the corporation should have a policy requiring attendance absent unusual circumstances. Time at the annual meeting should be set aside for shareholders to submit questions and for management or directors to respond to those questions.
- The board should respond appropriately when a director nominee receives a significant "withhold" or "against" vote with respect to his election to the board. The corporate governance committee should assess the reasons for the vote and recommend to the board the action to be taken with respect to the vote, which should be communicated to the corporation's shareholders.
- In planning communications with shareholders and investors, corporations should consider candor, need for timely disclosure, use of technology, and the ultimate goal of shareholder communications (e.g., honest, intelligible, meaningful, timely, and broadly disseminated information).

(c) HANDLING CREDITORS. Creditors can provide oversight feedback regarding achievement of an organization's objectives. For example, a bank may request reports on the organization's compliance with certain debt covenants and can recommend performance indicators or other desired targets or controls. Creditors should go beyond the credit rating issued by credit-rating agencies for a company; they should analyze financial statements for off–balance sheet transactions, and review annual reports and other documents to get a big picture of the company's products, services, and risk levels.

3.6 HANDLING STOCK MARKETS AND INVESTMENT ANALYSTS

(a) OVERVIEW. The U.S. stock markets issued corporate governance rules for listed companies to improve corporate governance practices. They also issued broker-dealer rules to control the behavior of investment analysts.

The aim of these rules is to bring integrity to the capital markets and confidence to investors.

(b) DEALING WITH STOCK MARKETS. Publicly traded companies with common stock issued on the New York Stock Exchange (NYSE), Nasdaq, and American Stock Exchange (Amex) are required to file an annual report containing audited financial statements.

Some examples of NYSE's rules include:

- Requiring research analysts employed by NYSE members to register with the NYSE, pass a qualification examination, and comply with a continuing education requirement
- Requiring broker-dealers to disclose the percentage breakdown of their "buy," "hold," and "sell" recommendations
- Forbidding retaliation by the firm against analysts for unfavorable or negative research or ratings
- Freeing securities analysts from the supervision and control of investment banking management regarding compensation, pending research reports, and the extent of coverage of a company
- Requiring disclosures of ownership of common shares by the broker-dealer firm and its analysts in the securities of a recommended issuer
- Requiring each participating investment bank to hire at least three independent securities analysts

(c) DEALING WITH INVESTMENT ANALYSTS. Investment analysts (also known as research analysts, financial analysts, or securities analysts) consider many factors relevant to an organization's worthiness as an investment opportunity. Investment analysts make buy, hold, or sell recommendations to current or potential investors. During this process, they analyze (1) management's strategies and objectives, (2) historical financial statements and prospective financial information, (3) actions taken in response to conditions in the economy and marketplace, (4) the potential for success in the short and long term, and (5) industry performance and peer group comparisons.

Investment analysts provide insights to a company management on how others perceive the organization's performance (outside-in perspective), risks that may impact the organization, operating or financing strategies that may improve performance, and industry trends.

This information is provided directly in face-to-face meetings of investment analysts and company management or through analyst reports issued to current and potential investors. In either case, company management should consider the observations and insights of investment analysts that may enhance the organization's overall performance.

Investment analysts are required to follow the rules established by the National Association of Securities Dealers (NASD), as it is the world's leading private-sector provider of financial regulatory services.

Some examples of NASD's rules include:

- Requiring research analysts employed by NASD members to register with the NASD, pass a qualification examination, and comply with a continuing education requirement
- Requiring broker-dealers to disclose the percentage breakdown of their "buy," "hold," and "sell" recommendations
- Forbidding retaliation by the firm against analysts for unfavorable or negative research or ratings
- Freeing securities analysts from the supervision and control of investment banking management regarding compensation, pending research reports, and the extent of coverage of a company
- Requiring disclosures of ownership of options by the broker-dealer firm and its analysts in the securities of a recommended issuer
- Requiring each participating investment bank to hire at least three independent securities analysts

3.7 HANDLING EMPLOYEES AND LABOR UNIONS

(a) OVERVIEW. Handling employees and labor unions is a sensitive matter because people are the most valuable asset of an organization. Management needs to be familiar with applicable laws and regulations in this matter.

According to Business Roundtable, the following guidelines apply when developing relationships with employees:[6]

- It is in a corporation's best interest to treat employees fairly and equitably.
- Corporations should have in place policies and practices that provide employees with compensation, including benefits, that is appropriate given the nature of the corporation's business and employees' job responsibilities and geographic locations.
- When corporations offer retirement, health care, insurance, and other benefit plans, employees should be fully informed of the terms of those plans.
- Corporations should have in place and publicize mechanisms for employees to seek guidance and to alert management and the board about potential or actual misconduct without fear of retribution.
- Corporations should communicate honestly with their employees about corporate operations and financial performance.

This section covers topics such as prohibited personnel practices, protecting whistleblowing employees, employees' joining labor unions, and other issues regarding employees.

(b) PROHIBITED PERSONNEL PRACTICES. In a high-performing workplace, employees must be able to pursue the missions of their organizations free from discrimination and should not fear or experience retaliation or reprisal for reporting—blowing the whistle on—waste, fraud, and abuse. Laws should protect employees from discrimination based on their race, color, sex, religion, national origin, age, or disability, as well as

retaliation for filing a complaint of discrimination. For example, U.S. federal employees are protected from 12 prohibited personnel practices conducted by their agencies.[7]

The following is a list of the 12 prohibited personnel practices:

1. Unlawful discrimination
2. Solicitation or consideration of improper background references
3. Coercion of political activity
4. Obstruction of the right to compete
5. Influencing withdrawal of applicants from competition
6. Unauthorized references
7. Nepotism
8. Reprisal for whistleblowing
9. Reprisal for the exercise of an appeal right
10. Discrimination based on off-duty conduct
11. Violation of laws or regulations implementing or concerning merit system principles
12. Violation of veterans' preference

(c) PROTECTING WHISTLEBLOWING EMPLOYEES. Whistleblower reprisal is generally defined as employers' taking or threatening to take personnel action against employees for reporting a violation of law, rule, or regulation, or for reporting gross mismanagement, gross waste of funds, abuse of authority, or a substantial and specific danger to public health or safety. Under the U.S. Whistleblower Protection Act of 1994 and the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 (No FEAR Act), federal agencies are responsible for the prevention of reprisal against their employees.[8]

Private-sector organizations, similar to public sector organizations, should develop policies and procedures to protect whistleblowing employees and to prevent the reprisal to their employees.

When employees report misconduct, possible negative responses by management include:

- Denial of an expected cash award or bonus
- Denial of an expected promotion
- Dismissal
- Reduction of duties or responsibilities
- Harassment
- Punitive performance appraisals
- Reassignment of work location
- Social isolation by peers
- Reassignment of work schedule

Possible positive actions by management, and the actions' positive consequences, include:

- Positive recognition
- Positive support by peers

- Promotion
- Employee self-satisfaction

(d) DEALING WITH LABOR UNIONS. Employees who belong to collective bargaining units represented by labor unions can also file grievances over discrimination and reprisal allegations under the terms of collective bargaining agreements. In those situations, the employee must choose to seek relief either under the statutory procedure or under the negotiated grievance procedure, but not both. U.S. employers must comply with the Wagner Act of 1935, which prohibits employers from undertaking unfair labor practices. For example, employers should not stop employees joining labor unions.

(e) ISSUES REGARDING EMPLOYEES. Companies are encouraged, and in some countries even obliged, to provide information on key issues relevant to employees and other stakeholders that may materially affect the performance of the company. Disclosure may include management and employee relations and relations with other stakeholders, such as labor unions.

Some countries require extensive disclosure of information on human resources. Human resource policies, such as programs for human resource development and training, retention rates of employees, and employee share ownership plans, can communicate important information on the competitive strengths of companies to market participants.[9]

3.8 HANDLING REGULATORS AND GOVERNMENT AUTHORITIES

(a) OVERVIEW. If new laws and regulations are needed—for example, to deal with clear cases of market imperfections—they should be designed in a way that makes them possible to implement and enforce in an efficient and evenhanded manner covering all parties. Consultation by government and other regulatory authorities with corporations, their representative organizations, and other stakeholders, is an effective way of doing this. Mechanisms should also be established for parties to protect their rights. In order to avoid overregulation, unenforceable laws, and unintended consequences that may impede or distort business dynamics, policy measures should be designed with a view to their overall costs and benefits. Such assessments should take into account the need for effective enforcement, including the ability of authorities to deter dishonest behavior and to impose effective sanctions for violations.[10]

According to Business Roundtable, the following guidelines apply when developing relationships with government:[11]

- Corporations, like all citizens, must act within the law. The penalties for serious violations of law can be extremely severe, even life threatening, for corporations. Compliance is not only appropriate—it is essential. Management should take reasonable steps to develop, implement, and maintain an effective legal compliance program, and the board should be knowledgeable about and oversee the program, including periodically reviewing the program to gain reasonable assurance that it is effective in deterring and preventing misconduct.
- Corporations have an important perspective to contribute to the public policy dialogue and should be actively involved in discussion about the development, enactment, and revision of the laws and regulations that affect the businesses and the communities in which they operate and their employees reside.

(b) SECURITIES AND EXCHANGE COMMISSION. Of all the regulators and government authorities, business corporations deal the most often with the Securities and Exchange Commission (SEC) staff due to federal securities laws such as the Securities Act of 1933, the Securities Exchange Act of 1934 (the Exchange Act), and the Sarbanes-Oxley Act of 2002 (SOX).

Federal securities laws help to protect the investing public by requiring public companies to disclose financial and other information. SEC was established by the Securities Exchange Act of 1934 to operationalize and enforce securities laws and to oversee the integrity and stability of the market for publicly traded securities. SEC is the primary U.S. federal agency involved in accounting requirements for publicly traded companies. Under Section 108 of SOX, SEC has recognized the accounting standards set by the Financial Accounting Standards Board (FASB)—generally accepted accounting principles (GAAP)—as "generally accepted" for the purpose of the federal securities laws. SEC reviews and comments on registrant filings and issues interpretive guidance and staff accounting bulletins on accounting matters.

(c) SEC ENFORCEMENT PROCESS. SEC investigates possible violations of securities laws, including those related to accounting issues. If the evidence gathered merits further inquiry, SEC will prompt an informal investigation or a formal order of investigation. Investigations can lead to SEC-prompted administrative or federal civil court actions. Depending on the type of proceedings, SEC can seek sanctions that include injunctions, civil money penalties, disgorgement (i.e., return of illegal profits), cease-and-desist orders, suspensions of registration, bars from appearing before the Commission, and officer and director bars. After an investigation is completed, SEC may institute either type of proceeding against a person or entity that it believes has violated federal securities laws. SEC can also initiate contempt proceedings and issue reports of investigation when appropriate. Because SEC has only civil enforcement authority, it may also refer appropriate cases to the U.S. Department of Justice for criminal investigation and prosecution. According to SEC, most enforcement actions are settled, with respondents generally consenting to the entry of civil, judicial, or administrative orders without admitting or denying the allegations against them.

3.9 HANDLING SUPPLIERS, VENDORS, CONTRACTORS, AND CUSTOMERS

(a) OVERVIEW. Companies are encouraged, and in some countries even obliged, to provide information on key issues relevant to stakeholders that may materially affect the performance of the company. Disclosure may include relations with stakeholders such as creditors, suppliers, and local communities. Because suppliers, vendors, contractors, and customers are outsiders of the organization, they can provide feedback, outside-in perspectives, and candid opinions about company products, services, or standard operating procedures and their deficiencies the way they see them. Organizations should view this feedback seriously and correct the deficiencies with due care and due diligence.

(b) DEALING WITH SUPPLIERS, VENDORS, AND CONTRACTORS. Most suppliers, vendors, and contractors are ethical and honest, but a few are not. Organizations must be vigilant regarding the possibility of vendor fraud, which can include overcharging

for purchased goods, shipping inferior goods, or not shipping goods even though payment was made. Also, there is a possibility of collusion on the part of buyers, vendors, suppliers, or contractors.

Organizations should note the following about their suppliers, vendors, and contractors:

- A vendor can provide information regarding completed or open shipments, which can be used in identifying and correcting discrepancies and reconciling account balances. The same thing may hold true with billings or invoices.
- A supplier can become a whistleblower and notify company management of a purchasing agent's or buyer's request for a kickback or bribe.
- A contractor may pose tax and legal problems if he worked for the company earlier.

Organizations should do the following when dealing with suppliers, vendors, and contractors:

- Develop a single, broad, goal-based supplier management policy.
- Balance between risks and rewards.
- Promote competition in managing multiple tiers of the supplier base, knowing that competition drives quality and innovation.
- Establish an accountability chain in the purchasing organization so that a manager's actions are linked to performance. Apply the same throughout the management hierarchy.
- Provide for a timely oversight role over the outsource vendor.
- Develop a flexible acquisition strategy for innovative products and services.
- Use vendor's past performance as the primary selection criterion to help ensure that poorly performing suppliers are not re-employed simply because they underbid other suppliers.
- Establish metrics that assess capabilities delivered and management of cost, schedule, and performance issues (e.g., earned-value management technique)
- Use competitive sourcing and best practices to increase innovation, efficiency, and effectiveness

Organizations should not use cost as a primary driver for selecting suppliers, vendors, and contractors.

(c) DEALING WITH CUSTOMERS. Most customers are ethical and honest, but a few are not. Organizations must be vigilant regarding customer fraud, such as not paying for goods shipped with the hope of getting something for nothing, or creating unnecessary disputes over billing with the hope that the company will eventually forgive and forget about the billing.

Some customers may inform a company about shipping delays, billing problems, inferior product quality, or poor service quality, or may express their overall dissatisfaction with products or services. These are examples of reactive style. Companies should respect customers and pay attention to their complaints and suggestions (i.e., outside-in perspective).

Proactive customers may work with an organization in developing new product or service requirements and/or product or service enhancements (i.e., voice of the customer or house of quality). This proactive style reflects doing things right the first time, which will help both the customer and the organization.

Customer surveys can help organizations to gather problem-related information at the right time in order to investigate the underlying source of the problem and correct it.

3.10 HANDLING PURCHASING AGENTS, BUYERS, OR COMMODITY/SERVICE EXPERTS, AND MARKETING AND SALESPEOPLE

(a) OVERVIEW. Corporate management can reduce unethical or illegal behavior on the part of purchasing agents, buyers, commodity/service experts, and salespeople by issuing a policy and codes of conduct statement while appropriately punishing those who conduct themselves improperly.

(b) DEALING WITH PURCHASING AGENTS, BUYERS, OR COMMODITY/SERVICE EXPERTS. Purchasing managers, more than any other management group within an organization, face enormous pressure to act in unethical way. This occurs for several reasons. First, purchasing has direct control over large sums of money. A buyer responsible for a multimillion dollar contract may find sellers using any means available to secure a favorable position. The very nature of purchasing means that a buyer must come in contact with outside sellers, who may occasionally be unethical. A second reason is due to the pressure placed on many salespeople. A seller who must meet aggressive sales goals might resort to questionable sales practices that, in turn, influence the buying practices.

Three rules must guide buyers. First, a buyer must commit his attention and energies for the organization's benefit rather than personal enrichment at the expense of the organization. Ethical buyers do not accept outside gifts or favors that violate their company's ethical policy. Ethical buyers are not tempted or influenced by the unethical practices of salespeople and do not have personal financial arrangements with suppliers. Second, a buyer must act ethically toward suppliers or potential suppliers. This means treating each supplier professionally and with respect. Finally, a buyer must uphold the ethical standards set forth by his profession. A code of professional ethics usually formalizes the set of ethical standards.

Organizations must do the following to enhance the ethical behavior of their purchasing personnel:

- Install buying teams to evaluate potential suppliers across different performance categories or selection criteria. Using a team approach to evaluate a supplier's capabilities limits the opportunity for unethical behavior.
- Develop a formal ethics policy defining the boundaries of ethical behavior, such as accepting gifts and receiving other favors.
- Communicate top management's message to buyers about whether unethical behavior is tolerated.
- Develop systems for internal reporting of unethical behavior, such as a fraud hotline.

- Rotate buyers among different purchasing items or commodities to prevent a buyer from becoming too comfortable with any particular group of suppliers. This is to prevent collusion by buyers, vendors, suppliers, and contractors.
- Develop a policy to limit a buyer's authority for awarding purchase contracts, say, to amounts of $10,000 or less. Contracts greater than $10,000 require a manager's signature, and the signature chain continues up the management hierarchy as the purchase amounts involved grow higher.
- Provide ethical training.

(c) DEALING WITH MARKETING AND SALESPEOPLE. A policy should be established prohibiting marketing and salespeople from distributing gifts and favors in the process of acquiring new customers or retaining current customers. This policy should be consistent with the policy prohibiting purchasing personnel from accepting gifts and favors from new or current suppliers. Other illegal and unethical practices that should be prohibited include price discrimination, misleading advertising, defrauding customers with false claims, unfair credit practices, price collusion with competing firms, and sexual harassment. This policy should be referred and linked to the company's codes of conduct statement.

3.11 HANDLING RELATED PARTIES AND THIRD PARTIES

It is important for the capital and stock market to know whether the company is being run with due regard to the interests of all its investors. To this end, it is essential for the company to fully disclose material related-party transactions to the market, either individually or on a grouped basis, including whether they have been executed at arm's-length and on normal market terms. In a number of jurisdictions this is indeed already a legal requirement. Related parties can include entities that control the company or are under common control with the company; significant shareholders and members of their families; and key management personnel.[12]

EXAMPLES OF RELATED-PARTY TRANSACTIONS

- Misreported sales between affiliates
- Unspecified intercompany transactions
- Failure to disclose and account for a compensation arrangement with a former CEO
- Personal loans to current CEO or other executives

Transactions involving the major shareholders (e.g., close family and relations), either directly or indirectly, are potentially the most difficult type of transactions. In some jurisdictions, shareholders above a limit as low as 5% of shareholdings are obliged to report transactions. Disclosure requirements include the nature of the relationship where control exists and the nature and amount of transactions with related parties, grouped as appropriate. Given the inherent opaqueness of many transactions, the obligation may need to be placed on the beneficiary to inform the board about the transaction, which in turn should make a disclosure to the market. This should not absolve the company from maintaining its own monitoring, which is an important task for the board.

3.12 HANDLING BUSINESS MERGERS AND ACQUISITIONS

In some countries, companies employ antitakeover devices or tactics during business mergers and acquisitions. However, both investors and stock exchanges have expressed concern over the possibility that widespread use of antitakeover devices may be a serious impediment to the functioning of the market for corporate control. In some instances, takeover defenses can simply be devices to shield the management or the board from shareholder monitoring. In implementing any antitakeover devices and in dealing with takeover proposals, the fiduciary duty of the board to shareholders and the company must remain paramount.[13]

Some of the terminology involved in takeovers is defined here:

- A golden parachute is a large payment made to the managers of a firm if it is acquired in a hostile takeover.
- A hostile merger is a merger in which the target firm's management opposes the proposed acquisition. Examples of defensive tactics include white knights, shark repellent, poison pills, greenmail, scorched earth, and tender offers.
    - A white knight is a friendly company that is more acceptable to the management of a firm under attack in a hostile takeover attempt.
    - Shark repellent is the acquisition of substantial amounts of outstanding common stock for the treasury stock or for retirement of stock, or the incurring of substantial long-term debt in exchange for outstanding common stock.
    - A poison pill is an action that will seriously damage a company if it is acquired by another firm. It may involve an amendment of the articles of incorporation or bylaws to make it more difficult to obtain stockholders' approval for a hostile takeover.
    - Greenmail is the acquisition of common stock presently owned by the prospective combiner at a price substantially in excess of the prospective combiner's cost, with the stock thus acquired placed in the treasury or given retired-stock status.
    - A scorched earth maneuver is the disposal, by sale or by a spin-off to stockholders, of one or more profitable business segments.
    - A tender offer is an offer by one firm to buy the stock of another by going directly to the stockholders, frequently over the opposition of the target firm's management.

3.13 ADDRESSING CORPORATE SOCIAL RESPONSIBILITY AND ACCOUNTABILITY

According to Business Roundtable, corporations have obligations to be good citizens of the local, national, and international communities in which they do business. Failure to meet these obligations can result in damage to the corporation, both in immediate economic terms and in longer-term reputational value.[14]

A corporation should be a good citizen and contribute to the communities in which it operates by making charitable contributions and encouraging its directors, managers, and employees to form relationships with those communities. A corporation also should be active in promoting awareness of health, safety, and environmental issues, including

any issues that relate to the specific types of business in which the corporation is engaged. Organizations must comply with the International Organization for Standardization (ISO) 26000 standard regarding social responsibility.

The four faces of corporate citizenship include economic responsibility, legal responsibility, ethical responsibility, and philanthropic responsibility.[15]

The *economic responsibility* is required of business by society, and includes things such as (1) being profitable, (2) maximizing sales, (3) minimizing costs, (4) making sound strategic decisions, and (5) beingattentive to dividend policy.

The *legal responsibility* is required of business by society, and includes things such as (1) obeying all laws and adhering to all regulations, (2) obeying the Foreign Corrupt Practices Act, (3) fulfilling all contractual obligations, and (4) honoring warranties and guarantees.

The *ethical responsibility* is expected of business by society, and includes things such as (1) avoiding questionable practices, (2) responding to the spirit as well as the letter of law, (3) assuming the law is a floor on behavior, (4) operating above the minimum required, (5) doing what is right, fair, and just, and (6) asserting ethical leadership.

The *philanthropic responsibility* is desired of business by society, and includes things such as (1) being a good corporate citizen, (2) making corporate contributions, (3) providing programs supporting community (e.g., education, health and human services, culture, arts, and civic duties), (4) providing for community development and betterment on a voluntary basis.

3.14 APPLICABLE LAWS, REGULATIONS, STANDARDS, AND PRINCIPLES

Organizations have a legal and ethical obligation to comply with the various federal, state, and local laws, regulations, circulars and bulletins, directives and executive orders, government orders, and ordinances pertinent to a specific business area. Noncompliance with these laws and regulations can lead to fines, civil and/or criminal penalties, probation, and jail punishments (prison time), thus creating reputation (image) risk. Compliance with industry and/or organization standards, including professional standards, can increase the quality of products and services, which, in turn, can enhance an organization's reputation and image in the marketplace. Adherence to generally accepted business principles and practices could have a similar effect as complying with standards.

A brief roundup of information about major laws, regulations, standards, and principles is provided here as a reminder for checklist purposes. Note that these laws and regulations are subject to change as new ones are added and existing ones are amended or repealed. The reader is advised to obtain the original laws, regulations, and standards from the official sources for a better understanding of the provisions, requirements, and conditions of the laws, regulations, and standards (www.regulations.gov). Although some of the following laws, regulations, and standards directly affect public sector organizations (i.e., government agencies), private-sector organizations can read, learn, and apply them to improve their business operations on a proactive basis.

U.S. organizations should comply with the following laws, regulations, standards, and principles pertinent to corporate ethics:

Compilation of Federal Ethics Laws. The U.S. Office of Government Ethics (OGE) in Washington, DC, has prepared the Compilation of Federal Ethics laws for the ethics

community. The compilation includes laws, statutes, and provisions to implement an effective ethics program for U.S. federal government agencies (www.usoge.gov).

Institute for Global Ethics. The mission of the Institute for Global Ethics is to promote ethical behavior in individuals, institutions, and nations through research, public discourse, and practical action. It publishes various guidelines and documents, such as research reports, white papers, and business dilemmas (www.globalethics.org).

Ethics in Government Act. Under the Ethics in Government Act of 1978, filers of financial disclosure statements must provide information about income, interest in properties, gifts and reimbursements, liabilities, and employment. The Act also requires subject matter experts and consultants to file financial disclosure statements. The Act requires that all filed public financial disclosure statements must be reviewed within 60 days of the filing date.

The Whistleblower Protection Act. In 1994, the Whistleblower Protection Act of 1989 was amended to require federal agencies to ensure that their employees are informed of the rights and remedies concerning whistleblower protection. In addition, Equal Employment Opportunity Commission's (EEOC) regulations require agencies to make written materials available to all employees and applicants informing them of the variety of equal employment opportunity program and administrative and judicial remedies available to them.

Notification and Federal Employee Antidiscrimination and Retaliation Act. The Notification and Federal Employee Anti-discrimination and Retaliation Act of 2002 (No FEAR Act). This Act requires that agencies notify employees in writing of the rights and protections available to them under the antidiscrimination and whisleblower statutes and post this information on their Internet sites. This provision reinforces existing requirements that employees be notified of rights and remedies concerning discrimination and whistleblower protection required of the Whistleblower Protection Act of 1994.

The No FEAR Act requires agencies to report the number of discrimination and whisleblower reprisal cases. It also requires the agencies to report the number of employees disciplined for discrimination, retaliation, or harassment.

Equal Employment Opportunity Commission. Equal Employment Opportunity Commission (EEOC) handles discrimination complaints against federal agencies filed by federal employees as well as complaints between private-sector employees and employers. Complaints are filed with and investigated by agencies, with hearings conducted by EEOC administrative judges. EEOC also hears appeals of agencies' and administrative judges' decisions on cases. EEOC regulations require that agencies take appropriate action against employees who engage in discriminatory conduct.

Foreign Corrupt Practices Act. In 1977, the U.S. Congress enacted the Foreign Corrupt Practices Act (FCPA) and amended it in 1998. The FCPA prohibits all U.S. domestic concerns from bribing foreign governmental or political officials to obtain business or licenses in foreign countries.

U.S. Federal Sentencing Guidelines. The U.S. federal sentencing guidelines for organizational defendants became effective in November 1991. These guidelines provide judges with a compacted formula for sentencing business organizations for various white-collar crimes. Included are federal securities, antitrust, and employment and

contract laws, as well as the crimes of mail and wire fraud, kickbacks and bribery, and money laundering.

U.S. Privacy Act. The Privacy Act was enacted in 1974 to provide for the protection of information related to individuals maintained in federal information systems and to grant access to such information by the individual. The Act establishes criteria for maintaining the confidentiality of sensitive data and guidelines for determining which data are covered.

The Act imposes numerous requirements upon federal agencies to prevent the misuse of data about individuals, to respect its confidentiality, and to preserve its integrity. Federal agencies can meet these requirements by the application of selected managerial, operational, and technical control procedures that, in combination, achieve the objectives of the Act.

The major provisions of the Act (1) limit disclosure of personal information to authorized persons and agencies, (2) require accuracy, relevance, timeliness, and completeness of records, and (3) require the use of safeguards to ensure the confidentiality and security of records.

Although the Act sets up legislative prohibitions against abuses, technical and related procedural safeguards are required in order to establish a reasonable confidence that compliance is indeed achieved. It is thus necessary to provide a reasonable degree of protection against unauthorized disclosure, destruction, or modification of personal data, whether intentionally caused or resulting from accident or carelessness.

Sherman Antitrust Act. The Sherman Act of 1890 prohibits actions that are "in constraint of trade" or actions that attempt to monopolize a market or create a monopoly. Legal actions under this Act typically involve price fixing or other forms of collusion among sellers. However, the law also prohibits reciprocity or reciprocal purchase agreements.

Clayton Antitrust Act. The Clayton Act of 1914 makes price discrimination illegal and prohibits sellers from exclusive arrangements with purchasers and/or product distributors.

Robinson-Patman Act. The Robinson-Patman Act of 1936 further addresses the issue of price discrimination established in the Clayton Act. It prohibits sellers from offering a discriminatory price where the effect of discrimination may limit competition or create a monopoly. There is also a provision that prohibits purchasers from inducing a discriminatory price. While a seller may legally lower a price as a concession during negotiations, the purchaser should not mislead or trick the seller, which would result in a price that is discriminatory to other buyers in the market.

Federal Trade Commission Act. The Federal Trade Commission Act of 1914 authorizes the Federal Trade Commission (FTC) to interpret trade legislation, including the provisions of the Sherman Antitrust Act that deal with restraint of trade. The Act also addresses unfair competition and unfair or deceptive trade practices.

New York Stock Exchange Corporate Governance Rules. The New York Stock Exchange (NYSE) has issued its corporate governance rules, which were approved by the SEC in 2003. The 12 rules are:

1. Listed companies must have a majority of independent directors.
2. The definition of "independent director" must follow certain standards.

3. To empower nonmanagement directors to serve as a more effective check on management, the nonmanagement directors of each company must meet at regularly scheduled executive sessions without management.
4. Listed companies must have a nominating or corporate governance committee composed entirely of independent directors.
5. Listed companies must have a compensation committee composed entirely of independent directors.
6. Listed companies must have an audit committee that satisfies the requirements of Rule 10A-3 under the Securities Exchange Act of 1934.
7. The audit committee must have a minimum of three members.
8. Listed companies must adopt and disclose corporate governance guidelines.
9. Listed companies must adopt and disclose a code of business conduct and ethics for directors, officers, and employees, and promptly disclose any waivers of the code for directors or executive officers.
10. Listed foreign private issuers must disclose any significant ways in which their corporate governance practices differ from those followed by domestic companies under NYSE listing standards.
11. Each listed company CEO must certify to the NYSE each year that he is not aware of any violation by the company of NYSE corporate governance listing standards.
12. The NYSE may issue a public reprimand letter to any listed company that violates a NYSE listing standard.

For a full text of these rules, visit www.nyse.com/pdfs/finalcorpgovrules.pdf.

NASDAQ Stock Market Corporate Governance Rules. The NASDAQ stock market issued its corporate governance rules in 2004. They give (1) criteria for independent directors, (2) qualitative listing requirements for Nasdaq national market and Nasdaq small cap market issuers, except for limited partnerships, (3) voting rights, and (4) qualitative listing requirements for Nasdaq issuers that are limited partnerships.

For a full text of these rules, visit www.nasdaq.com/about/CorporateGovernance.pdf.

National Association of Securities Dealers Rules and Regulations. The National Association of Securities Dealers (NASD) is a world leader in capital markets regulation. NASD licenses individuals and admits firms to the securities industry, writes rules to govern their behavior, examines them for regulatory compliance, and disciplines those who fail to comply. It oversees and regulates trading in equities, corporate bonds, securities futures, and options. It provides education and qualification examinations to industry professionals while supporting securities firms in their compliance activities. For a full text of rules and regulations, visit www.nasd.com and www.finra.org/index.htm.

U.S. Securities Regulations. The primary purpose of U.S. federal securities regulation is to prevent fraudulent practices in the sale of securities and thereby to foster public confidence in the securities market. Federal securities law consists principally of two statutes: the Securities Act of 1933, which focuses on the issuance of securities, and the Securities Exchange Act of 1934, which deals mainly with trading in issued securities. These "secondary" transactions greatly exceed in number and dollar value

the original offerings by issuers. The Securities and Exchange Commission (SEC) administers both of these securities acts (www.sec.gov).

The Golden Rule. The golden rule states putting oneself in others' shoes. It includes not knowingly doing harm to others.

The Means-Ends Cycle. The means-end cycle states that when ends are of overriding importance, unscrupulous means may be used to reach the ends.

Goal Congruence Principle. The goal congruence principle states that the actions, wills, and needs of employees should be subordinated to the greater good of the organization they work for. An employee should ask himself whether his goals are consistent with the organization's goals.

Prudent Person Concept. The prudent person, who is not infallible or perfect, has the ability to govern and discipline himself by the use of reason, does not neglect his/her duty, and applies his knowledge, skills, and sound judgment in the use of the organization's resources. The prudent person concept is related to the goal congruence principle.

ISO 26000. The International Organization for Standardization (ISO) is developing an international standard providing guidelines for social responsibility, known as ISO 26000. The goal is to encourage voluntary commitment by business organizations to social responsibility with common guidance on concepts, definitions, and methods of evaluation. The core issues that will be addressed in this standard include (1) the environment, (2) human rights and labor practices, (3) organizational governance and fair operating practices, and (4) consumer issues and community involvement and society development. For further information, visit www.iso.org.

Additional Resources

Cooper, Cynthia. *Extraordinary Circumstances: The Journey of a Corporate Whistleblower*. Hoboken, NJ: John Wiley & Sons, 2008.

Hartley, Robert F. *Business Ethics: Mistakes and Successes*. Hoboken, NJ: John Wiley & Sons, 2004.

Trevino, Linda K., and Katherine A. Nelson. *Managing Business Ethics: Straight Talk about How to Do It Right,* fourth edition. Hoboken, NJ: John Wiley & Sons, 2006.

Notes

1. Portions of this section are reprinted with permission. *OECD Principles of Corporate Governance* (Paris, France: OECD, 2004), 30. Reprinted with permission from the Copyright Clearance Center (CCC), acting as authorized copyright administrator for OECD.
2. U.S. General Accounting Office, *Government Ethics: HUD Financial Disclosure Reports Missing or Not Reviewed* (GAO/GGD-90-51), Washington, DC: 1990.
3. Portions of this section are reprinted with permission. Robert W. Walter, *Corporate Ethics for Financial Managers* (Jersey City, NJ: American Institute of Certified Public Accountants, 2003), 194–195, 212–214. Reprinted with permission from the Copyright Clearance Center (CCC), acting as authorized copyright administrator for AICPA.
4. *OECD Principles*, 32.
5. *Principles of Corporate Governance* (Washington, DC: Business Roundtable, 2005), 31–33, http://www.businessroundtable.org/publications/index.aspx.
6. *Id*., 33.

7. GAO, *Whistleblower Protection: VA Did Little Until Recently to Inform Employees about their Rights* (GAO/GGD-00-70), Washington, DC: April 2000.
8. *Id*.
9. *OECD Principles*, 53.
10. *Id*., 30.
11. *Principles* (Business Roundtable), 34.
12. *OECD Principles*, 52–53.
13. *Id*., 36.
14. *Principles* (Business Roundtable), 33–34.
15. Archie B. Carroll, "The Four Faces of Corporate Citizenship," *Business and Society Review* 100, no. 1 (1998): 1–7.

CHAPTER 4

GENERAL-MANAGEMENT BEST PRACTICES

4.1 OVERVIEW

General managers and senior managers, in harmony with the C-level executives, provide direction to organizations. They set goals and develop the strategies for their organization's members to attain those goals. An organizational goal is a desired state of affairs that the organization attempts to reach. A goal represents a result or end point toward which organizational efforts are directed. The choice of goal and strategy affects organization design.

Strategy is the plan of action that describes resource allocation and activities for dealing with the environment and attaining the organization's goals. The essence of formulating strategy is choosing how the organization will be different. Managers make decisions about whether the company will perform different activities or will execute similar activities differently than competitors do. Strategy necessarily changes over time to fit environmental conditions, but to remain competitive, companies develop strategies that focus on core competencies, develop synergy, and create value for customers.

Another aspect of strategic management concerns the organizational level to which strategic issues apply. Strategic managers normally think in terms of three levels of strategy: corporate, business, and functional.

4.2 ROLES AND RESPONSIBILITIES OF GENERAL MANAGERS AND SENIOR MANAGERS

General managers and senior managers are the next level in the management hierarchy below that of the C-level executives where the former reports to one of the C-level executives. These managers implement the mission, vision, goals, and objectives of the organization established and approved by the C-level executives of the organization. These general managers and senior managers implement the goals and objectives through the efforts of the line managers, middle-level managers, staff managers, and lower-level managers. If the management style of the general managers and senior managers is ineffective and inefficient, it will result in poor implementation efforts and unsuccessful day-to-day operations. Corporate goal congruence is really effected through the detailed plans, budgets, and actions of the line managers, middle-level managers, staff managers, and lower-level managers. In a way, general managers and senior managers are the change agents in the organization, requiring effective managing skills such as planning, organizing, directing, controlling, communication, and motivation skills. They develop business plans for business units, divisions, or groups of businesses, and report their progress to C-level executives.

General managers and senior managers must ensure that all employees focus on the right things at all times to achieve improved performance results and increased productivity levels.

As part of their roles and responsibilities, general managers and senior managers may:

- Integrate production, inventory, logistics, and transportation activities for maximum efficiency and effectiveness.
- Lower total manufacturing and service costs in order to lower selling prices, increase sales volume, and increase profits.
- Link production and service costs to cash flows and gross profits, operating profits, or net profits.
- Increase faster product and service deliveries to customers to achieve their total satisfaction (i.e., a shorter order-to-delivery cycle and faster time to market for new products and services).
- Introduce new production and service techniques and processes by leveraging technology to improve quality and to reduce costs.
- Eliminate non-value-added activities in production and service to trim waste and to lower costs.
- Focus more on value-added activities in production and services to provide a solid value to the customers and to the organization.
- Identify key drivers of cost, quality, risks, expenses, revenues, profits, business growth, competition, and performance. Focus on the root causes of these drivers and understand why these drivers go up and down.
- Seamlessly integrate the back-end systems with the front-end systems for (1) maximum data consistency, completeness, and accuracy, (2) better customer service and satisfaction, and (3) stronger connection of disparate and disconnected business processes.
- Build standardized, transparent, and repeatable production and service processes to provide the stable, consistent, and quality products and services that customers expect. First, streamline both upstream and downstream business processes involved in international licensing and franchising arrangements, and other operations; second, simplify; third, standardize; and then institutionalize.
- Understand that increases in sales velocity increase inventory velocity, which, in turn, increases production or service velocity, finance velocity, human capital velocity, and systems velocity. The goal is to synchronize these velocities in a cohesive manner.
- Implement the goal congruence concept by linking individual employee goals with those of the department/division and the organization, Remove or reduce the competing or conflicting goals.
- Implement crosscutting best practices across business units, divisions, departments, and functions through busting silos and building bridges.
- Link employee rewards, bonuses, and promotions to employees' true performance and tangible results, and empower employees.
- Build solid working relationships with C-level executives in manufacturing, marketing, finance, human resources, IT and other functions through formal and informal approaches at the workplace.

- Foster ethical values and cultural sensitivity in light of workforce diversity.
- Encourage employees to continuously acquire and improve their knowledge, skills, and abilities (KSAs) through targeted training courses, management development programs, and professional certifications.
- Establish a solid and sustainable chain of knowledge linked through the entire management hierarchy to ensure core knowledge competencies for all levels of employees in the organization.
- Invite production and service audits, management reviews, and self-assessments periodically and proactively to ensure continuous improvement in quality, cost, and delivery.
- Encourage employees at all levels of the organization to think differently and radically (i.e., out-of-the-box thinking) at all times, which can lead to new perspectives providing best-of-breed solutions.
- Participate in the succession-planning process for key positions.
- Analyze outside-in views (i.e., views of stakeholders about company management) and inside-out views (i.e., views of company management about stakeholders) to identify disconnections between these views and to integrate them in a coherent manner.

4.3 STRATEGIC MANAGEMENT

(a) OVERVIEW. A strategic management process (SMP) helps focus the attention of an organization or a department head on identifying and resolving key issues. Through the SMP, the executive can set a clear organization-wide direction and move the organization toward achieving its goals.[1]

Key or strategic issues are the most critical questions that affect an organization's future direction, its products, its services, and its basic values. Frequently, these issues involve more than one department or function. An SMP, however, does not encompass all the issues an organization faces on a daily basis. Instead, it focuses squarely on the issues that are the most appropriate for the organization head to address.

An SMP will enhance the organization's ability to address the following fundamental questions:

- Where is the organization going? (Direction)
- How well can it get there? (Strategies)
- What is its blueprint (Plan) for action? (Budget)
- How will it know if it is achieving its direction? (Accountability)

Systematically addressing these questions can help the organization executive proactively manage change and avoid crisis management. An SMP will provide for better-informed decision-making, based on a recognized, organization-wide direction. The organization managers then can better justify decisions by linking their proposed management actions to the organization's strategic direction. In this way, the needs of various stakeholders of the organization can drive the organization's activities. The result will be more effective and higher-quality products and services for customers.

The CEO or the President of an organization can play a lead role in articulating the SMP. Institutionalizing the SMP would give a CEO or President a mechanism for

identifying and addressing strategic issues and setting a management agenda for the organization. The CEO or the President is the linchpin of the SMP. He is the leader in obtaining the support of key groups and is responsible for articulating the organization's strategic direction and making decisions vital to the each element of the SMP. The CEO or the President should show strong, sustained support for the SMP to encourage its acceptance into the organizational culture.

(b) STRATEGIC-MANAGEMENT BEST PRACTICES. There are seven elements and seven associated best practices that come into play during SMP implementation. Although these seven elements present a sequential process, they are iterative in the sense that successful problem solving may require that some elements be revisited and refined.

Element 1: Commitment to Planning

Purpose: Obtain the support of key groups and stakeholders for the SMP.

Task: Agree on ground rules for conducting the SMP.

Best Practices: The initial agreement could cover critical aspects of the SMP, such as (1) its purpose, (2) who should participate, (3) how it will be conducted, (4) the roles and functions of key players and other participants, (5) a schedule for accomplishments, and (6) commitment of necessary resources.

Element 2: Scan Environment

Purpose: Obtain data to identify and analyze a range of possible strategic issues and support decision making throughout the process.

Tasks: (1) Assess external and internal environment and (2) Identify a range of possible strategic issues and their implications.

Best Practices: *External scanning* identifies and assesses external conditions that may affect the organization in the future, including economic, political, demographic, socioeconomic, and technological trends. *Internal scanning* identifies the organizational strengths and weaknesses, that is, the attributes or deficiencies that may help or hinder attainment of the organization's strategic direction. Sources for the internal scanning may include major management systems, performance-monitoring systems, management information systems, internal/external auditor reports, and independent management consultant reports.

Element 3: Articulate Organization's Strategic Direction

Purpose: Envision, in broad terms, the organization's future direction.

Tasks: (1) Establish a clear direction for the organization's future actions and (2) Select the strategic issues that the process will address.

Best Practices: From the data gathered and evaluated during the environmental scanning process, the CEO or the President, with representatives of key internal and external groups, should clarify and interpret the organization's mission (purpose) and values. The future direction, which is the most enduring aspect of SMP, provides the context for evaluating and selecting the strategic issues that must be addressed if the organization is to achieve its desired future. The few issues selected should be those that significantly influence the way the organization functions because focusing on

too many issues and objectives could result in a cumbersome, paperwork-intensive process. Emphasis should be placed on supporting goals that cut across more than one department or business unit, seeking collaboration for more effective use of resources.

Element 4: Develop Strategies

Purpose: Select the best approaches to address each strategic issue and achieve the strategic direction.

Tasks: (1) Identify alternate strategies to address each strategic issue, (2) Identify barriers to and consequences of implementing alternatives, and (3) Select the alternative with the greatest potential for success.

Best Practices: This is a multipart process of identifying, evaluating, and selecting strategies that will best address each strategic issue consistent with the organization's strategic direction. The number and identities of participants involved could change, depending on the issue under consideration. Alternate strategies, focusing at the opposite end of the spectrum, can range from in-house work to outsourcing or contracting out.

Element 5: Develop Action Plans and Link to Budget

Purpose: Develop action plans and obtain resources needed to implement selected strategies.

Tasks: (1) Develop detailed action plans based on selected strategies and (2) Ensure that action plans shape budget submissions.

Best Practices: Business-unit or division managers must translate selected strategies into specific short-term and longer-term action plans that will move the organization in the desired direction. Action plans should:

List in specific, measurable terms the outcome desired, so that it will be possible to determine whether the outcome has been achieved.

Provide a time frame to attain the desired outcome, so that results can be measured at a specific point.

Offer the expectation that, with the proper use of resources and staff, the desired outcome can be accomplished.

Relate directly to a strategic issue, consistent with the organization's strategic direction.

Action planning should be the responsibility of line managers, not staff planners. Line managers are the ones who must carry out the plans and their involvement and commitment are necessary if the organization is to change in response to its environment. Without linking the action plans to the budget, action plans will become nothing more than "wish lists," losing credibility and thereby losing the support of people necessary to make the process a success.

Element 6: Establish Accountability and Implement Action Plans

Purpose: Assure implementation of action plans with resources allocated.

Tasks: (1) Assign responsibility for implementing action plans, (2) Make action plans a reality by incorporating them into day-to-day operations, and (3) Link the individual reward system to action plan implementation.

Best Practices: At this point, the business unit's or division's line managers and general managers should take the responsibility for implementing the action plans, avoiding frustration resulting from paperwork drills. This responsibility leads to accountability for results. Personnel performance systems should link action plans with the personnel reward system, thus stimulating individual commitment to organization-wide initiatives. Performance awards, bonuses, employee appraisals, and executive employment contracts should be linked to the implementation of action plans.

Element 7: Monitor Implementation and Provide Feedback

Purpose: Evaluate projects or programs in implementing action plans and ensure that relevant information flows along the management hierarchy.

Tasks: (1) Monitor progress toward implementing action plans, (2) Periodically report progress and problems to the senior management, (3) Assess adequacy of action plans and take necessary corrective measures, and (4) Fine-tune the strategic management process as required.

Best Practices: Monitor the implementation of action plans to assess any obstacles to plan implementation and take corrective actions. In addition, monitoring could reveal the need to revise part(s) of the SMP. Effective review and monitoring do not require extensive controls. When monitoring becomes complex and involves excessive paperwork exercise, strong opposition results. The monitoring system should be flexible and not burdensome by keeping the paperwork to a minimum and by building on existing management reporting systems.

It should be noted that the above strategic planning elements 1 through 5 constitute the strategic planning aspects of the SMP, while elements 6 and 7 comprise the management functions, such as accountability and monitoring.

(c) ORGANIZATIONAL PLANNING PROCESS. Planning is the formulation of future courses of action. Being the primary management function, planning provides purpose and direction to the organization. The planning horizon consists of three types: strategic (long-term), tactical (intermediate), and operational (short-term). Plans and forecasts are interrelated, since the latter is used in the former. Forecasts are predictive in nature, while plans are goal-oriented.

The planning process (1) links organization strategic planning and departmental strategic planning, (2) uses information to maximize an organization's usefulness, (3) preserves information integrity, availability, and confidentiality, (4) encourages departments to meet anticipated needs, reflect budget constraints, and form the basis for budget requests, (5) examines the ultimate impact of information resources on operations through work process redesign, and (6) moves from traditional procedure-based and rule-based planning to mission-driven and broad-based strategic thinking.

Five types of planning exist: strategic planning, tactical planning, operational planning, contingency planning, and information systems planning. *Strategic planning* defines the mission, goals, and objectives of the organization. It also identifies the major activities to be undertaken to accomplish the desired direction. *Tactical planning* identifies, schedules, manages, and controls the tasks necessary to accomplish individual activities. It involves planning of projects, procurement, and staffing. *Operational planning* integrates tactical plans and supportive activities and describes the short-term tasks

that must be accomplished in order to achieve the desired results. *Contingency planning* refers to developing alternate plans (Plan B and Plan C) when the original plan (Plan A) does not materialize. This can include computer center contingency plans where plans for processing alternate systems will go into effect when the original computer center is inoperable due to disasters. *Information systems planning* provides a phased, structured approach to systematically define, develop, implement, and maintain all aspects of an organization's near- and long-term information system needs and information needs.

(d) APPROACHES TO MEASURING ORGANIZATIONAL EFFECTIVENESS. Contingency approaches to measuring effectiveness focus on different parts of the organization. Traditional approaches include the goal approach, the resource-based approach, and the internal process approach. The *goal approach* to organizational effectiveness is concerned with the output side and whether the organization achieves its goals in terms of desired levels of output. The *resource-based approach* assesses effectiveness by observing the beginning of the process and evaluating whether the organization effectively obtains resources necessary for high performance. The *internal process approach* looks at internal activities and assesses effectiveness by indicators of internal efficiency.

These traditional approaches all have something to offer, but each one tells only part of the story, A more recent *stakeholder approach* (also called the constituency approach) acknowledges that each organization has many constituencies that have a stake in its outcomes. The stakeholder approach focuses on the satisfaction of stakeholders as an indicator of the organization's performance.

4.4 KEYS TO MANAGING PEOPLE

Many private- and public sector organizations believe that the demand for faster, cheaper, and better service-delivery systems leads their organizations to develop new and more flexible ways of managing people. The following eight interrelated principles developed out of the changes world-class organizations had made and the lessons they had learned.[2]

Principle 1. Value people as assets rather than as costs or expenses.
Principle 2. Emphasize mission, vision, and organizational culture.
Principle 3. Hold managers responsible for achieving results instead of imposing rigid, process-oriented rules and standards.
Principle 4. Choose an organizational structure appropriate to the organization rather than trying to make "one size fit all."
Principle 5. Instead of isolating the personnel function organizationally, integrate human resource management into the mission of the organization.
Principle 6. Treat continuous learning as an investment in success rather than as a cost to be minimized.
Principle 7. Pursue an integrated rather than an ad hoc approach to information management.
Principle 8. Provide sustained leadership that recognizes change as a permanent condition, not a onetime event.

4.5 ORGANIZATIONAL CULTURE

(a) WHAT IS ORGANIZATIONAL CULTURE? Organizational culture is defined as the underlying assumptions, beliefs, values, attitudes, and expectations shared by an organization's members (i.e., managers and nonmanagers). An organization's beliefs and values affect the behavior of its members. Many organizations are actively trying to perpetuate some cultural values and change others to increase their chances for being competitive, efficient, or effective.[3]

An organization's decision to change its culture is generally triggered by a specific event or situation. Events such as a change in the world economic situation, an increase in domestic or international competition, or a severe budget reduction could provide the impetus for an organizational culture change. A culture change is a long-term effort that takes at least five to ten years to complete.

(b) TECHNIQUES FOR PERPETUATING OR CHANGING ORGANIZATIONAL CULTURE. Leading organizations use the following 15 techniques to change or perpetuate their organizational cultures, with the techniques ranked by degree of importance, such as "very great," "great," "moderate," and "some." Although top management support and training are the two most important techniques in making a successful culture change, it is generally agreed that using just these two techniques would not necessarily result in success. Rather, these two techniques are usually used in combination with the other 13 techniques, because these techniques vary in importance and use depending on an organization's needs.

The following is a summary of techniques for perpetuating or changing organizational culture, ranked in order of importance.

Very Great:

1. Display top management commitment and support for values and beliefs.
2. Train employees to convey and develop skills related to values and beliefs.

Great:

3. Develop a statement of values and beliefs.
4. Communicate values and beliefs to employees.
5. Use a management style compatible with values and beliefs.
6. Offer rewards, incentives, and promotions to encourage behavior compatible with values and beliefs.
7. Convey and support values and beliefs at organizational gatherings.
8. Make the organization's structure compatible with values and beliefs.
9. Set up systems, procedures, and processes compatible with values and beliefs.

Moderate:

10. Replace or change responsibilities of employees who do not support desired values and beliefs.
11. Use stories, legends, or myths to convey values and beliefs.
12. Make positive examples of employees who demonstrate correct values and beliefs.

Some:

13. Recruit employees who possess or will readily accept values and beliefs.
14. Use slogans to symbolize values and beliefs.
15. Assign a manager or group with primary responsibility for efforts to change or perpetuate culture.

(i) Technique 1: Display top management commitment and support for values and beliefs (very great). When a company is motivated to change its culture, strong top-management leadership and a display of commitment and support for desired beliefs and values are considered crucial to its success. Senior managers and executives must articulate and live by organizational values and beliefs to demonstrate to employees that top management is committed to making permanent cultural changes and is not merely paying lip service to them.

Organizations should do the following:

- Discuss organizational values and beliefs in meetings, internal publications, internal television programming, and videotapes.
- Implement employees' suggestions that support the organization's values and beliefs, and reward them for their accomplishments.
- Ensure that all facets of the organization—the reward and promotion system, the organizational structure and management style, training, communications, symbolism, and systems, procedures, and processes—reflect its values and beliefs.

(ii) Technique 2: Train employees to convey and develop skills related to values and beliefs (very great). Training has been used as a very important tool for promoting and developing skills related to an organization's beliefs and values.

Organizations should do the following:

- Make training the cornerstone of efforts to change to a culture that places a high value on quality.
- Train employees in quality awareness and provide courses in communications, problem solving, decision making, statistics, interpersonal, group participation, and management skills to enable them to work in the company's total quality environment.

(iii) Technique 3: Develop a statement of values and beliefs (great). Articulating an organization's values and distributing a written statement of those values to employees is an important technique.

Organizations should do the following:

- Develop a written statement of organization mission, values, and guiding principles.
- Ensure that culture flows from and is compatible with mission, and that all employees clearly understand what the mission is.

(iv) Technique 4: Communicate values and beliefs to employees (great). Communicating information to organizational members about company values and beliefs is a crucial step.

Organizations should do the following:

- Use newsletters, periodicals, questionnaires, pamphlets, magazines, in-house television networks, and videotapes to communicate values and beliefs.
- Administer a questionnaire to employees to measure their perception of the company's success in living up to its beliefs and values.

(v) Technique 5: Use a management style compatible with values and beliefs (great). Companies that are changing their culture often have to change their management style, sometimes drastically. The change could be from an authoritative to a participative management style (e.g., people-oriented).

Organizations should do the following:

- Delegate authority to employees and allow them to participate in the decision-process.
- Establish problem-discovery and problem-solving teams that include organizational members from the highest to the lowest levels of the company.
- Encourage and empower employees to contribute fully to the company's continuous improvement efforts.
- Change the organizational culture to emphasize quality so customer satisfaction is increased through the reduction of defects in all products and errors in all services
- Encourage employees to suggest better ways to do the work and make decisions that increase efficiency. This should be accompanied by a policy that employees will not lose their jobs because of suggestions for improvements.
- Empower employees by making the following changes:
    - With inspections removed, employees are responsible for quality.
    - Employees can stop the production line when they see problems in the quality of the products.
    - Work teams make decisions and select new team members when there are openings.
    - Employees conduct reviews of their peers' performance and comment on supervisors' performance (360-degree reviews).
    - Employees monitor their own attendance at work.

(vi) Technique 6: Offer rewards, incentives, and promotions to encourage behavior compatible with values and beliefs (great). Some companies offer rewards, incentives, and promotions to employees whose behavior supports the desired organizational culture. They believe that these rewards encourage similar behavior in other employees and help to perpetuate or change the culture.

Organizations should do the following:

- Establish a promotion system for technical staff (e.g., scientists and engineers) to rise to high levels in the company without becoming managers in order to allow them conduct innovative research.

- Reward employees who recommend improvements in processes or who provide innovative ideas for new products.
- Establish an "annual quality reward program" to recognize business units or divisions that exemplify total quality.
- Establish cash bonuses to hourly production workers when a plant meets its goals
- Establish cash bonuses to salaried employees based on overall corporate success, either financially or operationally.
- Give "thank you" cards and dinner vouchers at a local restaurant for employees to recognize their exemplary contributions quickly.

(vii) Technique 7: Convey and support values and beliefs at organizational gatherings (great). Some companies use organizational gatherings to explain their values and beliefs to employees.

Organizations should do the following:

- Establish milestone events and gather employees to explain the company's accomplishments by the chairperson of the board. The occasion could be improved quality, increased sales, acquisition of new businesses, increased profits, and increased market share.
- Ensure that all employees from the highest level to the lowest level of the organization have been informed about these milestone events.

(viii) Technique 8: Make the organization's structure compatible with values and beliefs (great). When developing a culture or considering a culture change, a company generally selects an organizational structure that will suit its desired culture. The structure could be centralized, decentralized, a combination, or a variation.

Organizations should do the following:

- Establish an organizational structure with few layers (say five) between the lowest-level employee and the chief executive officer (CEO).
- Demonstrate respect for the individual employee, service to the customer, and excellence in execution with reduced number of layers in the organizational structure.
- Emphasize that a flat organizational structure with few layers allows more employees to participate in decision making and problem solving and speeds the company's decision-making process.

(ix) Technique 9: Set up systems, procedures, and processes that are compatible with values and beliefs (great). Companies that are perpetuating or changing their cultures generally recognize that they must make their systems, procedures, and processes compatible with their values and beliefs.

Organizations should do the following:

- Emphasize that customer satisfaction begins with employee satisfaction.
- Increase customer satisfaction by reducing defects in products and mistakes in services while doing the work faster.

- To gain or increase customer confidence, provide customers with "out-of-the-box" quality, on-time product or service deliveries, and no early product failures.
- Develop systems, procedures, and processes to demonstrate (i) a no-layoff policy, (ii) promotions from within, (iii) semiannual performance reviews, and (iv) reviews to help employees identify training needs to improve their skills.
- Develop a program in which employees may air perceived problems with higher-level management without fear of repercussion.
- Develop a performance review system where employees rate their managers and supervisors to determine how well they manage employees.

(x) Technique 10: Replace or change responsibilities of employees who do not support desired values and beliefs (moderate). When employees do not support a culture change or do not help to perpetuate the values and beliefs that a company believes are important, some companies replace employees or change their responsibilities.

Organizations should do the following:

- Provide generous incentives to employees who agree to retire early.
- Appeal to some employees' sense of duty in asking them to move from key management positions. Do this appeal in a manner to avoid disrespect and humiliation for the individual.
- Reassign employees or change their responsibilities when management determines that certain employees are not suited for their positions. Do not attach a stigma to such a change.
- Conduct surveys to indicate whether employees are satisfied with their managers and supervisors.

(xi) Technique 11: Use stories, legends, or myths to convey values and beliefs (moderate). Some companies repeat success stories, legends, or myths to impress their values and beliefs on employees.

Organizations should do the following:

- Distribute success stories through notebooks or newsletters about the quality of products and services
- Request that each employee offer ideas for resolving quality issues or addressing quality-related problems in products and services.
- Establish performance targets for product delivery times and timeliness of operations, and incorporate these targets into standard operating procedures (SOPs).
- Tolerate employees' mistakes in their efforts to be creative and innovative, which will eventually bring success to the company.

(xii) Technique 12: Make positive examples of employees who demonstrate those values and beliefs (moderate). Some managers and executives believe that a good technique to encourage people to support a company's values and beliefs is to make them heroes or heroines of exemplars of those values.

Organizations should do the following:

- Establish a recognition system to single out employees who exemplify the company's beliefs and values, particularly those related to quality. Recognize these employees' contributions in front of the other colleagues to make their efforts well known.
- Establish a quality leadership award to employees who have made important contributions to improving quality. Announce these contributions in a quality milestone book or newsletter with employee pictures.
- Encourage other employees to emulate the employees whose accomplishments have been recognized, rewarded, and publicized.

(xiii) Technique 13: Recruit employees who possess or will readily accept values and beliefs (some). Some companies attempt to recruit people who believe in or are willing to accept the organizations' desired values and beliefs.

Organizations should do the following:

- Develop processes and procedures to hire people who will work well as team members and who are open and flexible.
- Involve team members in the employee-hiring process.
- Test prospective employees to see if they will fit into the culture. Look for people with the particular skills needed to perform or to learn to perform a job.
- Develop open and realistic communications with new hires about the organization's current and desired beliefs and values and both positive and negative aspects of a job.

(xiv) Technique 14: Use slogans to symbolize values and beliefs (some). Some companies use slogans to symbolically communicate their desired beliefs and values to employees.

Organizations should do the following:

- Develop company-specific, product-specific, or service-specific slogans as a means of communicating values and making employees proud of the company they work for.
- Target to achieve a ranking as one of the best places to work for.

(xv) Technique 15: Assign a culture manager or group with primary responsibility for efforts to change or perpetuate culture (some). Some companies assign a person or group to facilitate their culture change efforts.

Organizations should do the following:

- Assign a manager of corporate quality, as needed.
- Assign a manager of quality council, as needed.
- Assign a culture manager, as needed.

Organizations should not give the impression that managers of corporate quality, quality council, or culture can fix all the problems in the organization. Instill that all employees should be involved in culture change or perpetuation efforts.

4.6 BUSINESS CHANGE MANAGEMENT

(a) OVERVIEW. Business change management focuses on the future, which requires a proactive approach in order to be effective. The change will be brought about by several factors—change in the world economic situation, competition both nationally and internationally, declines in revenues, loss of market share, reductions in budgets, or a need to improve products and services. Use of appropriate technology and the right culture can result in a significant and positive impact in implementing change along with effective policies, procedures, and processes.

(b) CHANGE MANAGEMENT APPROACHES

(i) Cultural Changes. Culture has a major impact on a change management program. For example, purchasing managers may follow a risk-averse acquisition culture that must be changed to encourage them to balance risk with perfection and recognize that taking reasonable risk (i.e. calculated risk) is good management. In other words, cultural changes are necessary to balance value, price, and fairness and to produce a true timely and cost-effective acquisition process. This will not be easy and requires strong leadership on the part of managers.

INDICATORS OF CHANGE

Performance measures and metrics are important to monitor changes and to assess their effects on individuals.

(ii) Employee Empowerment. The movement to empower those ultimately responsible and accountable for the expenditure and acquisition decisions (i.e., managers) and those that are in the front line of operations (i.e., workers, supervisors) is relevant to whether the change management program succeeds. For example, empowering the employees in the purchasing department would put them in a position to develop acquisition strategies, conduct acquisitions, and administer their contracts, including negotiating for best quality, price, and delivery terms.

(iii) Role of Advanced Technologies

(A) OVERVIEW

Computer communication and information technology (IT) can contribute to greater economic performance by an organization. However, it is also obvious that technology alone is not enough. If an organization's or a nation's economy is to benefit from advanced networking technologies, a number of technological, organizational, and institutional criteria must be met. To the extent that policy measure fails to address all of these criteria, the chances for success will be diminished.

(B) TECHNOLOGICAL CTRITERIA

Versatile and open networks and applications. Versatile networks and applications will be increasingly critical in a global economy characterized by rapid technological and socioeconomic change and a greater variety in preferences, products, and business processes. To perform well, businesses will have to rapidly reconfigure their networks in

response to changing circumstances and market demands. Versatile networks will provide the leeway needed to customize applications and networks to support redesigned business processes and flexible working relationships. With the freedom to mix and match a variety of network components, businesses can use technology to add value and to develop new products and services.

Interoperability and seamless interconnection. To reap full economic benefits, communication and IT networks and network components will need to be interoperable and open for interconnection. Such networks can reduce transaction costs, whereas closed systems increase the cost of doing business and can create significant barriers to market entry. Interoperable components provide greater network flexibility, are easier to use, and reduce network costs. These capabilities encourage technology diffusion and equity of access. In addition, interoperable systems provide a standard platform for new components and applications.

Ubiquitous and even deployment. If the economic benefits of networking are to be broadly shared, technology must be deployed in a timely and ubiquitous fashion. Business networks can give rise to a significant "first mover" advantage. Networks benefit from considerable economies of scale and scope; therefore, latecomers may be unable to generate the critical mass of users and services to develop a network. Latecomers will also be disadvantaged because networking requires not only extensive expertise, but also considerable "learning by doing."

(C) Organizational Criteria

Technology deployment matched to business needs. Technology will not enhance business performance if it does not match business needs. Where technology has been introduced independently of a business plan, efficiency and effectiveness have often declined. Experience suggests that technology and businesses' needs will be most closely matched when: (1) business management takes the initiative in applying technology; (2) technology experts understand and practice business principles and participate in developing the technology plan, and (3) technology users, at all levels, have an opportunity to influence the technology design and deployment strategy.

Versatile organizational structure and role relationships. In the future, business organizations and processes will need to be more flexible to take advantage of the new opportunities available in a global, knowledge-based economy. Although information and communication technologies can foster and support such organizational change, they cannot substitute for it. Organizations can more easily employ technology to bring about organizational change when roles and routines are broadly defined, resources (especially knowledge and information) are widely shared, and relationships are flexible and loosely coupled.

Supportive and adaptive organizational cultures. Organizational cultures—like organizational structures—need to be adaptable and innovative if technology is to yield positive economic results. Relationships will need to be defined and reinforced less by contractual arrangements and rigid hierarchical rules and regulations, more by consensual group norms and trust. Interorganizational relations will need to be oriented as much

toward cooperation as competition. In addition, businesses will need to develop new and more broad-based criteria for assessing the performance of both individual employees and the enterprise itself.

(D) Institutional Criteria

Regulations are geared to national economic and social goals. If communication and information networks are to be deployed in a timely fashion, and with an appropriate architecture that will support improved economic performance, regulatory policy will need to be more responsive to, and consistent with, national economic and social goals. Regulators need to pay more attention to the economic impacts of technology choices. In addition, as information and communication technologies converge, greater attention must also be paid to the information, or content, aspects of networking technologies.

Need to reevaluate and revise the marketplace rules. Rapid advances in information and communication technologies, together with business response to new technological opportunities and constraints, are challenging many of the traditional notions that have governed the marketplace rules and practices of the industrial era. Major issues include intellectual property rights and other laws governing the ownership and use of information. For example, electronic commerce would challenge contract laws in terms of written signatures and paper documents. Given a global economy, a consensus regarding these rules needs to be developed on both national and international levels.

Support for long-term resource maintenance. It will be essential to maintain national capabilities in a global economy where knowledge and information, capital, and labor are not confined to national borders. Support for science, research and development, and an educated workforce will be important.

(iv) Linking Technology and Organizational Innovations. IT alone will not be enough to regain an organization's competitive position in a rapidly changing economic environment. In cases where technology has made a critical difference, it has been employed in conjunction with successful organizational change. Similarly, most obstacles to success have been organizational rather than technological. To develop appropriate technology-based strategies that are sufficiently responsive to the fundamental changes taking place around them, businesses will need to reengineer their business relationships and their ways of thinking about the nature of the business enterprise itself.

Change Direction

Organizational change can take place from both the top down and the bottom up. But, as in the case of all innovations, organizational changes will be redeveloped and reinterpreted to address the situation at hand.

Embodying social relations and supporting social interactions, communication, and IT are indeed powerful forces for change. However, if they are to have their intended effect, new technologies will need to be carefully integrated into their organizational environment, taking full account of employees' strengths and weaknesses. This means that the way people work, learn, and innovate must be understood by management. Successful systems development and networks require that trust be established over

time through a process of repeated successful transactions between suppliers, customers, and employees. It also requires a commitment and willingness to share all forms of information among business partners (i.e., suppliers and customers), a shift that is not easy to implement.

(v) Impact of Changing Technology. The impact of changing technology is difficult to assess, due to its effect on employees and humans in general. Worker involvement, combined with a total quality management (TQM) program, could help in reducing the negative impact of technology on employees. Fundamental to TQM is the assumption that, when things go wrong, the problem generally stems from organizational rather than human failures. To solve such organizational problems, TQM calls for employees, working in teams and closely with management, to identify the problems and find ways to overcome them. Work teams also need access to company-wide information to properly analyze issues and solve problems.

Although many organizations have taken formal steps to adopt team-based, quality-oriented approaches, many old behavioral patterns persist. To implement TQM, management must renounce its traditional hierarchical style—based on the specialization of task, workplace stability, productivity, obedience, and control—in favor of a more trust-oriented approach that calls for leaders who can inspire group motivation, loyalty, commitment, and worker pride. Workers, on the other hand, must not only be willing to learn new skills and adapt to different incentives and reward structures, they must also trust management's intentions. This will be hard to do, given years of adversarial relations between management and workers. It is even more difficult when TQM groups are established as part of a total business-reengineering process, in which case jobs may be at stake. Under such circumstances, it is not surprising that many quality management programs have yet to show clear-cut positive results.

Tools for Change Management

- Use workflow software to define problems.
- Use groupware products to facilitate workflow analysis and group computing.
- Reengineer the work process.
- Solicit employee involvement and commitment.
- Provide timely feedback to employee.

Technology, although by no means a panacea, offers one way of breaking out of this organizational impasse. There is a major problem in viewing technology in this way, however. Like organizational innovations, technology is viewed all too often as a "fix" to be implemented from the top down. Although technology plays a major role in structuring human relations, rarely do businesses, or the people working in them, play a major role in its design. The real choices about technologies are not made when vendors put them up for sale on the market, but when the problem to be solved is first defined. As experience with total quality groups demonstrate the task of identifying problems is often performed best by those who are doing the work. Use of work-flow software to redefine problems by workers is a workable and useful approach.

(vi) Change Implementation. Implementation of new advances in IT, and the birth of new organizational forms (e.g., downsizing, upsizing, flexsizing, and rightsizing) to make use of them, will probably make sure workforce change continues. Experience indicates that IT can both upskill and deskill jobs, which requires increased flexibility on the part of employees. Continuous improvement (kaizen), lean production, short cycle times, and just in time (kanban) manufacturing are the new standards of performance in production, distribution, and retail industries. Similarly, the forming of worker teams and *quality circles* to motivate employees is gaining momentum. This approach to work sees cooperation as a central goal. Employers recognize that encouraging employees to share the firm's goals is not only profitable in the long run, but also necessary for the development of flexible response processes.

IT supports these shifts to new ways of managing organizations. Electronic data interchange (EDI), for example, is a critical component in just-in-time distribution because it allows suppliers and customers to coordinate the flow of goods. "Concurrent" or "simultaneous" engineering is largely a computerized approach to team-oriented design. Manufacturers find lean production easier to implement with the development of computerized numerically controlled (CNC) machines.

However, actions such as layoffs, downsizing, and use of temporary workers cause some problems for worker motivation. By hiring temporary employees, employers avoid paying fringe benefits and can release workers in economic downturns. Such firms have less incentive to train their employees and upgrade their skills because the chance of recouping their investment is small.

All these actions by management are causing the workforce to undergo long-term structural changes in which workers are more fragmented from the workplace. Under these circumstances, IT can help management to monitor clerical workers, operators, and others working at computer terminals. New technologies can track areas of work that have traditionally been immune to monitoring. For instance, the location, status, and activity of workers, delivery personnel, and truckers can be more closely monitored through a global positioning system (GPS).

4.7 BUSINESS CONTRACT MANAGEMENT

(a) OVERVIEW. The amount of money used to contract for goods and services is continuing to increase for both private- and public sector organizations. Most organizations approach the acquisition of services differently than the acquisition of products. For example, researchers and scientists discover new products, engineers design them, and manufacturers produce them so there is a tight system in place with strict reviews and controls along the way. It takes a long time to define product requirements, establish measurable and performance-based outcomes, and assess contractor performance. Individual service acquisitions proceed through requirements, solution, and delivery more quickly. Further, delivery of service begins immediately or very shortly after the contract is finalized.[4]

The dollar amounts for product development and manufacturing are big, risky, and tied directly to mission accomplishment. However, service acquisitions are seen as less risky because many services are not tied directly to mission accomplishment and tend to be composed of far more numerous and lower-dollar-value contracts. Because of this reason, there is less seriousness in the acquisition of services than in the acquisition

of products despite the increase in funds allocated for service acquisition. If this trend continues, more and more service funds will be vulnerable to potential fraud, waste, and abuse unless effective controls are in place. A given organization's approach to buying services is largely fragmented and uncoordinated; responsibilities for acquiring services are generally spread among individual departments, offices, or functional units, with little visibility or control at the headquarters or central location. In other words, product acquisitions are controlled better than service acquisitions.

Definitions of Fraud, Waste, and Abuse

Fraud is any intentional deception taken for the purpose of inducing organizational action or organizational reliance on the deception. Fraud can be perpetrated by the organization's employees, third parties, or by contractors and their employees.

Waste is the extravagant, careless, or needless expenditure of organization funds, or the consumption of organizational property that results from deficient practices, systems, controls, or decisions. Waste includes improper practices not involving prosecutable fraud.

Abuse is the manner in which resources, projects, or programs are managed that creates or perpetuates waste or contributes to acts of fraud. Abuse is also called mismanagement.

Studies have shown that, generally speaking, the position that a perpetrator holds within an organization will tend to have the most significant effect on the size of losses in a fraud scheme. Trust and the access to funds and assets that comes with senior leadership and tenure can become an organizational vulnerability if the control environment in place is weak. Although waste and abuse are not as well defined as fraud, their effects can be just as profound.

The range of service acquisitions include major services such as advertising; IT systems development and maintenance and network support; construction, repair, and maintenance of facilities and equipment; professional, administrative, and management consulting and support services; and relatively simple services such as lawn mowing, medical services, cafeteria services, waste removal, and temporary clerical services.

(b) PRODUCT AND SERVICE ACQUISITIONS BEST PRACTICES. Organizations should implement the following five best practices to minimize or reduce the vulnerabilities to potential fraud, waste, and abuse in product and service acquisitions.

(i) Sustained Senior Leadership. Organization senior leadership is a critical factor in providing direction and vision as well as in maintaining the culture of the organization. As such, senior leaders have the responsibility to communicate and demonstrate a commitment to sound practices deemed acceptable for the acquisition function. Senior management's tone at the top allows a certain level of vulnerability to enter into the acquisition process. Senior management ultimately shape the environment that mid-level and frontline acquisition employees operate within, and it is that tone that clearly identifies and emphasizes the values deemed acceptable within the acquisition function.

(ii) Capable Acquisition Workforce. Organizations need to have the right skills in their acquisition workforce to effectively implement best practices and properly manage the acquisition of goods and services. In the ever-changing contracting environment, the acquisition workforce must be able to rapidly adapt to increasing workloads while

continuing to improve its knowledge of market conditions, industry trends, and the technical details of the goods and services they procure. Moreover, effective workforce skills are essential for ensuring that the organization receives fair and reasonable prices for the goods and services it buys. Sufficient and timely training and guidance on the use of contracts should be provided to the acquisition workforce.

(iii) Adequate Pricing. Organizations can face various risks associated with obtaining adequate contract pricing that can lead to vulnerabilities. These pricing risks stem from noncompetitive contract actions, delays in setting requirements for unfinalized contracts, failure to use available pricing information, and misclassification of capital items as expense items. A competitive environment provides more assurance of reasonable prices than a noncompetitive one does.

TYPES OF CONTRACTS

Indefinite Delivery or Indefinite Quantity Contract: A kind of contract used to acquire goods and services when the exact date of future deliveries is unknown but a recurring need is likely to arise. There are three types of indefinite delivery contracts: definite quantity contracts, requirements contracts, and indefinite quantity contracts. Indefinite quantity contracts provide for an indefinite quantity, within stated limits, of supplies or services during a fixed period.

Performance-Based Contract: Performance-based contracting emphasizes that all aspects of an acquisition be structured around the results of the work to be performed as opposed to the manner in which the work is to be performed. When using this type of contract, the contracting organization specifies the outcome or result it desires and leaves it to the contractor to decide how best to achieve the desired outcome.

Sole-Source Contract: A contract for the purchase of goods or services that is entered into by an organization after soliciting and negotiating with only one vendor.

Time-and-Materials Contract: A contract that provides for acquiring supplies or services on the basis of direct labor hours at specified fixed hourly rates that include wages, overhead, general and administrative expenses, profit, and materials at cost.

Organizations should avoid indefinite delivery or indefinite quantity contracts and sole-source contracts as much as possible due to their non-competitive nature when it comes to obtaining fair and reasonable prices. Instead, performance-based contracts should be encouraged.

(iv) Appropriate Contracting Approaches and Techniques. When selecting contracting approaches and techniques for an award, the organization's objective is to negotiate a contract type and price that will result in reasonable risk and provide the contractor with the greatest incentive for efficient and economical performance. The interdepartmental or interdivisional contracting approach enables organizations to leverage their buying power and provide a simplified and expedited method of acquiring goods and services. Adequate training and guidance should be provided to the acquisition employees on the use of interdepartmental or interdivisional agreements so that they can exercise effective management control and oversight over the contracts as well as on the contractors.

(v) Sufficient Contract Surveillance. The role of the acquisition function does not end with the award of a contract. It requires continued involvement throughout contract

implementation and closeout to ensure that contracted products and services are delivered according to the schedule, cost, quality, and quantity specified in the contract. If surveillance is insufficient, is not conducted, or is not documented, organizations risk paying contractors more than the value of the goods and services provided.

4.8 APPLICABLE LAWS, REGULATIONS, STANDARDS, AND PRINCIPLES

Organizations have a legal and ethical obligation to comply with the various federal, state, and local laws, regulations, circulars and bulletins, directives and executive orders, government orders, and ordinances pertinent to a specific business area. Noncompliance with these laws and regulations can lead to fines, civil and/or criminal penalties, probation, and jail punishments (prison time), thus creating reputation (image) risk. Compliance with industry and/or organization standards, including professional standards, can increase the quality of products and services, which, in turn, can enhance an organization's reputation and image in the marketplace. Adherence to generally accepted business principles and practices could have a similar effect as complying with standards.

A brief roundup of information about major laws, regulations, and standards is provided here as a remainder for checklist purpose. Note that these laws and regulations are subject to change as new ones are added and existing ones are amended or repealed. The reader is advised to obtain the original laws, regulations, and standards from the official sources for a better understanding of the provisions, requirements, and conditions of the laws, regulations, and standards (www.regulations.gov). Although some of the following laws, regulations, and standards directly affect the public sector organizations (i.e., government agencies), private-sector organizations can read, learn, and apply them to improve their business operations on a proactive basis.

U.S. organizations should comply with the following laws, regulations, standards, and principles pertinent to general management:

Sherman Antitrust Act. The Sherman Act of 1890 prohibits actions that are "in constraint of trade" or actions that attempt to monopolize a market or create a monopoly. Legal actions under this act typically involve price-fixing or other forms of collusion among sellers. However, the law also prohibits reciprocity or reciprocal purchase agreements.

Clayton Antitrust Act. The Clayton Act of 1914 makes price discrimination illegal and prohibits sellers from exclusive arrangements with purchasers and/or product distributors.

Robinson-Patman Act. The Robinson-Patman Act of 1936 further addresses the issue of price discrimination established in the Clayton Act. It prohibits sellers from offering a discriminatory price where the effect of discrimination may limit competition or create a monopoly. There is also a provision that prohibits purchasers from inducing a discriminatory price. While a seller may legally lower price as a concession during negotiations, the purchaser should not mislead or trick the seller, which would result in a price that is discriminatory to other buyers in the market.

Federal Trade Commission Act. The Federal Trade Commission Act of 1914 authorizes the Federal Trade Commission (FTC) to interpret trade legislation, including the provisions of the Sherman Antitrust Act that deal with restraint of trade. The Act also addresses unfair competition and unfair or deceptive trade practices.

Uniform Commercial Code. Article 2 of the Uniform Commercial Code (UCC) governs sales of goods and products in all states except Louisiana. The UCC essentially defines goods as tangible personal property, which is any property other than an interest in real property (e.g., land). All such transactions are governed by UCC Article 2, but where the UCC has not specifically modified general contract law, the common law of contracts continues to apply. In other words, the law of sales is a specialized part of the general law of contracts, and the law of contracts governs unless specifically displaced by the UCC.

Goal Congruence Principle. The goal congruence principle states that actions, wills, and needs of employees should be subordinated to the greater good of the organization they work for. An employee should ask himself whether his goals are consistent with the organizational goals.

Additional Resources

Axson, David A. J. *Best Practices in Planning and Performance Management*, second edition. Hoboken, NJ: John Wiley & Sons, 2007.

Baron, James N., and David M. Kreps. *Strategic Human Resources: Frameworks for General Managers*. Hoboken, NJ: Wiley & Sons, 1999.

Johnson, Hans V. A., and Per Erik Kihlstedt. *Performance-Based Reporting: New Management Tools for Unpredictable Times*. Hoboken, NJ: John Wiley & Sons, 2005.

Notes

1. U.S. General Accounting Office, *Management of VA (Veterans Administration): Implementing Strategic Management Process Would Improve Service to Veterans* (GAO/HRD-90-109), Washington, DC: Aug. 1990.
2. GAO, *Human Capital: A Self-Assessment Checklist for Agency Leaders* (GAO/GGD-99-179), Washington, DC: Sept. 1999.
3. GAO, *Organizational Culture: Techniques Companies Use to Perpetuate or Change Beliefs and Values* (GAO/NSIAD-92-105), Washington, DC: Feb. 1992.
4. GAO, *Contract Management: DoD Vulnerabilities to Contracting Fraud, Waste, and Abuse* (GAO-06-838 R), Washington, DC: July 2006.

CHAPTER 5

MANUFACTURING- AND SERVICE-MANAGEMENT BEST PRACTICES

5.1 OVERVIEW

A nation's economic prosperity is primarily dependent on three types of industries: manufacturing, service, and farming, with the latter not being discussed in this chapter. A nation's gross domestic product (GDP) is measured based on national outputs, the value of the total goods and services produced within the country's boundaries. GDP measures the annual production of the economy and excludes nonproduction transactions such as financial transactions (e.g., public and private transfer payments and security transactions such as buying and selling of stocks and bonds) and resales (e.g., automobiles and houses). In other words, whatever manufacturing and service organizations do or do not do directly affects a nation's GDP growth or decline, respectively.

Both manufacturing and service industries face many challenges and are going through dramatic changes while pursuing their mission to reduce product and service costs; increase quality of products and services; improve service to customers; comply with all applicable laws and regulations; increase market share, revenues, profits, and returns; and stay globally competitive. In this chapter, we attempt to provide key business principles and best practices to achieve this mission.

5.2 ROLES AND RESPONSIBILITIES OF THE CHIEF OPERATIONS OFFICER

The Chief Operations Officer (COO) or Chief Operating Officer (COO) is a key person in the C-level executive suite and is in charge of either manufacturing operations or service operations. His roles and responsibilities call on him to:

- Integrate production, inventory, logistics, and transportation activities for maximum efficiency and effectiveness.
- Lower total manufacturing and service costs in order to lower selling prices, increase sales volume, and increase profits.
- Link production and service costs to cash flows and gross profits.
- Speed up product and service deliveries to achieve customers' total satisfaction (i.e., shorter order-to-delivery cycle).
- Innovate new production and service techniques and processes by leveraging technology to improve quality and to reduce costs.
- Eliminate non-value-added activities in production and service to trim waste and lower costs.

- Focus more on value-added activities in production and services to provide a solid value to the customers and the organization.
- Identify key drivers of cost, quality, risks, expenses, revenues, profits, business growth, competition, and performance. Focus on the root causes of these drivers and understand why these drivers go up and down.
- Seamlessly integrate the back-end systems with the front-end systems for (1) maximum data consistency, completeness, and accuracy, (2) better customer service and satisfaction, and (3) stronger connection of disparate and disconnected business processes.
- Build standardized, transparent, and repeatable production and service processes to provide the stable, consistent, and quality products and services that both internal and external customers expect.
- Understand that higher sales velocity increases inventory velocity, which, in turn, increases production or service velocity, finance velocity, human capital velocity, and systems velocity. The goal is to synchronize these velocities in a cohesive manner.
- Implement the goal congruence concept by linking individual employee goals with those of the department/division and the organization. Remove or reduce the competing or conflicting goals.
- Implement crosscutting best practices across business units, divisions, departments, and functions through busting silos and building bridges.
- Link employee rewards, bonuses, and promotions to employees' true performance and tangible results, and empower employees.
- Build solid working relationships with C-level executives in marketing, finance, human resources, and other functions through formal and informal approaches at the workplace.
- Foster ethical values and cultural sensitivity in light of workforce diversity.
- Encourage employees to continuously acquire and improve knowledge, skills, and abilities (KSAs) through targeted training courses, management development programs, and professional certifications.
- Establish a solid and sustainable chain of knowledge linked through the entire management hierarchy to ensure core knowledge competencies for all levels of employees in the organization.
- Invite production and service audits, management reviews, and self-assessments periodically and proactively to ensure continuous improvement in quality, cost, and delivery.
- Encourage employees at all levels of the organization to think differently and radically (i.e., out-of-the-box thinking) at all times, which can lead to new perspectives providing best-of-breed solutions.
- Participate in the succession-planning process for key positions.
- Adhere to professional and ethical standards established by the relevant professional bodies.
- Analyze outside-in views (i.e., views of stakeholders about company management) and inside-out views (i.e., views of company management about stakeholders) to identify disconnections between these views and to integrate them in a coherent manner.

5.3 WORLD-CLASS MANUFACTURING MANAGEMENT

(a) MANUFACTURING STRATEGY. World-class manufacturing strategies include increasing productivity, decreasing costs, and improving quality by adding value to inputs through the transformation process and producing quality outputs. This approach fits with the concept that consumers purchase their products from the company that offers them the most value for their money. The manufacturing strategy should fit with the overall business strategy, such as less time-to-market new products; cost minimization; improved quality; and greater market share, revenues, profits, and returns.

Critical Success Factors for a World-Class Manufacturing Function

Critical success factors for a world-class manufacturing function include value creation to customers and the organization, product cost minimization, product quality improvement, faster and stabler production, low inventories, listening to stakeholder voices, leadership, organizational culture, customer service, organizational structure, technology, process, and people.

World-class manufacturing organizations implement various combinations of tools, techniques, practices, and standards to achieve excellence in manufacturing operations. Some examples of tools, techniques, and practices include Six Sigma quality, design of experiments (DOE), theory of constraints (TOC), statistical process control (SPC), Taguchi method, quality function deployment (QFD), voice of the customer (VOC), total quality management (TQM), just in-time (JIT) methods, quick response (QR) systems, lean manufacturing practices, and various design methods such as design for manufacturability, design for low cost, design for high quality, design for faster production, design for faster marketing, design for safety and ergonomics, design for better environment, design for serviceability, design for marketability (i.e., product appearance, esthetics, size and shape, packaging, container, and ease of operation and use), design for disassembly (i.e., taking a product apart easily for shipping and at the end of its life), design for forward logistics (i.e., flow of products from manufacturers to consumers through better methods of labeling, packaging, shipping and handling, and storing the original products), design for reverse logistics (i.e., flow of products from consumers to manufacturers through recycling, reconditioning, refurbishing, and remanufacturing of returned products), and design for supply management (i.e., materials sourcing, transportation, storage, supplier and carrier selection and evaluation, material handling, delivery of raw materials, and shipping of finished goods).

Some examples of standards include ISO 9000 series standards, ISO 14000 series standards, organization standards, and the industry standards. These tools, techniques, practices, and standards must be combined with management systems such as survey of customers, contractors, suppliers, vendors, employees, management, and the industry; self-assessments; industry research reports; audits; management reviews; and benchmarking studies.

(b) LISTENING TO STAKEHOLDER VOICES. Manufacturing management, as a maker of goods and products for the company, should pay close attention to the following "voices" to achieve organizational goals and improve overall performance. When these "voices" are heard together, they bring attention to new perspectives and creative conflicts, forcing new thinking that leads to new solutions (i.e., best-of-breed solutions). Listening to the

collective voice of many stakeholders at once will have a greater impact than listening to one voice at a time in isolation, because the former requires a balanced approach after considering all party's concerns.

For each content of each voice, a T-Column analysis should be prepared, with "what happens if I listen to this voice" in the left column (benefits) and "what happens if I don't listen to this voice" in the right column (costs and risks). A comparative analysis of each content in each column will point to new problems requiring new solutions.

- Voice of the customer (external customers such as suppliers, vendors, contractors, consultants, key customers, regulators, investors, creditors, the stock market, and media/press, and internal customers such as the board of directors, corporate management, and employees in other functional departments such as engineering, research and development, marketing, human resources, finance, and IT)
- Voice of the process (process flows, process variations, process delays and waste, and process inefficiencies)
- Voice of quality (TQM principles and practices, mistake-proofing, continuous improvement, cost of poor quality, quality engineering, quality assurance, quality control, quality audit, quality council, quality circles, certified vendors and suppliers, and quality control/management tools)
- Voice of standards (product design standards, product-manufacturing standards, product-testing standards, packaging standards, environmental standards, recycling standards, product safety and ergonomics standards, and industry/organization standards)
- Voice of partners (supply chain members, material-sourcing vendors, electronic commerce vendors, recycling vendors, raw materials and parts suppliers, packaging vendors, and outsourcing vendors)
- Voice of regulators (federal, state, and local laws and regulations)
- Voice of competitors (press releases, Web site pressrooms, industry magazines, daily business newspapers, advertising magazines, industry trade shows, product demonstrations and promotions, direct mail, e-mail campaigns, copyright/ trademark/ patent news, business intelligence news, banner advertising, billboard and street advertising, product sponsorships, and online events and chat rooms)

(c) MANUFACTURING-CYCLE TIME MEASURES. Cycle time reduction in manufacturing deals with reducing the order-to-delivery cycle and time-to-production cycle, which produces benefits such as increased productivity, improved utilization of human and machine resources, decreased costs, and improved customer service. To attain these benefits, organizations must:

- Eliminate or decrease non-value-added activities (e.g., material storage, handling, and movement steps; inspection steps; rework steps; waiting time; product recall time; product warranty time; and delays at the interdepartmental and interdivisional boundaries and at the intradepartmental work stations).
- Enhance or increase value-added activities (e.g., production pure-process time; ingredients-mix time; part-fabricating time; part- plating, -casting, -soldering, and -painting time; part subassembly time; part final assembly time; customer

order–processing time; customer order ship time; internal/external customer access points to manufacturing systems; manufacturing project hold points; manufacturing-management decision points and control points).

This requires having the right resources available at the right place and at the right time so that delays and waste in manufacturing operations are decreased.

Some examples of manufacturing-cycle time measures include:

- Percentage decrease in production cycle time, which is the time between two identical units being completed on a production line
- Percentage increase in manufacturing-cycle efficiency, which is calculated by dividing the total hours of value-added time in the production process by the total production cycle time, where the latter includes both value-added and non-value-added time
- Percentage decrease in machine setup time
- Percentage decrease in the inventory cycle time, which is the length of time between the placing of two consecutive orders
- Percentage decrease in the order-to-delivery cycle time, which is the time it takes from receiving the customer order to filling the order
- Elapsed time between the time an author's new book manuscript is submitted to production and the time the book is available in stock for sale by a book publisher. The longer the elapsed time, the greater the loss of sales and profits resulting from the delayed book. The goal is to reduce the cycle time for book production.

(d) MANUFACTURING METRICS. Manufacturing management should develop and track the following key performance indicators (KPI) and metrics to improve performance:

- Percentage increase in total throughput of a factory, which is measured by dividing the number of good units produced by the total production cycle time
- Percentage increase in plant capacity utilization
- Percentage increase in total plant capacity availability
- Percentage reduction in manufacturing transaction-processing costs due to electronic commerce (B2B) for ordering, purchasing, and payment
- Percentage decrease in inventory investment dollars
- Increase in the number of inventory turns for each inventory classification of A, B, and C
- Decrease in procurement lead times for acquiring parts, components, and raw materials
- Percentage reduction in procurement-operating costs due to use of automated purchasing systems
- Decrease in the number of suppliers from the total supplier base
- Increase in the number of supply chain partners participating in the manufacturing decision-making process
- Percentage decrease in the source-to-supply cycle time due to efficient supplier selection process and supply-chain management practices

- Percentage increase in customer-order fill rates
- Decrease in the number of transportation carriers from the total carrier base
- Number of product recalls reported by product category with financial impact this year and compared to previous years.
- Zero product recalls by product category in a given time period.
- Total product warranty costs expressed as a percentage of total product costs or sales this year and compared to previous years.

5.4 PRODUCT DESIGN AND DEVELOPMENT

(a) OVERVIEW. Manufacturing a product requires consideration of several factors, among them: listening to the VOC; designing for functionality, cost, quality, and manufacturability; and combining with engineering design and quality principles to achieve goals such as the lowest total cost, the shortest time-to-production, and the fastest time-to-market.[1] These factors should be measured and improved using performance metrics such as cost metrics (e.g., total cost to produce a product), time-to-market metrics (e.g., true time-to-market related to stable production), and efficiency metrics (e.g., cost per unit of output).

The following design factors should be emphasized early by the product design and development team since redesigns or major product design changes consume a great deal of design and manufacturing resources to implement the changes. The further into a design, the harder it is to start satisfying additional needs. Proactive management is the predominant rule here. One of the biggest payoffs of "do-it-right-the-first-time" product development is avoiding expensive and time-consuming engineering change orders, which should be closely controlled and minimized.

(b) DESIGN FOR MANUFACTURABILITY. Design for manufacturability (DFM) is the process of proactively designing products to (1) optimize all the manufacturing functions such as fabrication, assembly, test, procurement, shipping, delivery, service, and repair, and (2) assure the best cost, quality, reliability, regulatory compliance, safety, time-to-market, and customer satisfaction.[2] DFM alone may make the difference between being competitive or noncompetitive. DFM takes less effort to achieve benefits in cost, quality, and time-to-market because products are designed right the first time.

Concurrent engineering (CE) is the proactive practice of designing products to be built according to standard processes, or concurrently developing new processes while developing new products. Quality is designed in with process simplicity, optimal tolerances, quality parts, mistake-proofing, concurrent design and selection of robust processes, and specification of quality parts to minimize the cumulative effect of part quality on product quality. Products are designed for lean production and build-to-order with aggressive standardization, elimination of setup by design, and the concurrent engineering of versatile-product and flexible processes.

(i) Summary of Key Principles for the Design for Manufacturability. Key principles suggest doing things right the first time, avoiding duplication of effort, maximizing synergies by working as a team and working with other projects, and balancing performance, cost, quality, and safety factors.

The following is a summary of key DFM principles:

- Avoid late engineering changes, because the same change can cost ten times what it would have cost earlier in the stages of production.
- Specify good parts to begin with, because at each subsequent stage of production it can cost ten times more to find and repair a defect.
- Use standard parts for new designs.
- Optimize the utilization of off-the-shelf parts from a catalog before designing new parts.
- Define the product well in advance to satisfy the voice of the customer.
- Use proven features and modules from previous designs to avoid reinventing the wheel.
- Proactively manage product variety by designing for lean production, build-to-order, and mass customization.

(ii) Summary of Methodologies for the Design for Manufacturability. Product development management ensures that:

- Selection of product development projects is based on rational product portfolio planning.
- Diverse teams have the resources so that all relevant specialists are actively involved early in the design process.
- The team leader has leadership skills and abilities, experience, empowerment, and a thorough understanding of the DFM methodologies.
- Vendor partnerships are determined ahead of time to encourage early vendor participation. No low-bidding practices should be allowed after design.

Plan for a thorough concept or architectural phase with the following deliverables:

- VOC is captured and applied to quality function deployment (QFD) through house of quality (HOQ).
- Concept simplification is applied at the product and process level.
- Optimal utilization is achieved using off-the-shelf parts.
- Manufacturing strategy and modular strategy are determined and optimized early in the process.
- Architectural optimization is achieved for product families, processes, and supply chains.
- Outsourcing strategy is optimized for concurrent engineering, manufacturability, cost, quality, and responsiveness.

Ensure that products are designed after considering all aspects of manufacturability, meaning:

- The product is designed as total system, not just a collection of individual parts.
- Quality, reliability, and mistake-proofing targets are achieved by design.
- Standard parts lists are determined and used for new designs.
- Cost is computed by total cost measurements.

- Time is measured to stable and trouble-free production.
- Documentation is complete and accurate.

(iii) Key Tasks, Results, and Tools for the Design for Manufacturability. Exhibit 5.1 describes key DFM tasks, results, and tools.

(iv) Summary of Benefits for the Design for Manufacturability. Implementation of DFM principles, methodologies, and tools provides the following benefits:

- From an overall perspective, (1) lower production costs, (2) higher-quality products, (3) quicker time-to-market, (4) lower capital equipment cost through better

Tasks	Results	Tools
Get voice of the customer Perform QFD analysis	Meaningful and rational product specifications Best resource prioritization	Input from customer, QFD, and teamwork
Raise and resolve issues early	All issues raised early All issues resolved early	Strong team leadership Team consensus
Simplify product concepts	Inherently low product cost Inherently high quality Inherently high reliability	Thorough up-front work Creative culture Teamwork
Optimize product architecture and system design	Ensure lowest cost Ensure quick product development Ensure trouble-free product launch	Thorough up-front work Cross-functional teams Architecture focus
Standardize, modularize, and reuse engineering	Minimum material overhead Quicker product designs Flexible operations	Standardization lists Motivation and discipline Cross-functional team cooperation
Quantify total costs	Best decisions Proper product costing and pricing	Activity-based costing Total cost thinking
Establish vendor/supplier partnerships	Manufacturable part designs Lowest vendor cost and time Quality assured at the source	Vendor/supplier partnerships Total cost measurements Teamwork
Measure and compensate to encourage teamwork and achieve total goals	Minimum total cost Minimum time to market Best decisions	Metrics and compensation based on total cost and the real time to market
Optimize product and process design	Manufacturable designs Optimized processing Quality designed in	CE, DFM, and quality guidelines
Management supports and understands the DFM and CE concepts	Product development becomes a potent competitive advantage	Executive education

Exhibit 5.1 Tasks, Results, and Tools for Design for Manufacturability

utilization of assets, (5) greater use of automation, (6) early production, (7) fewer engineering changes, (8) less chance of redesign, (9) fewer parts to purchase from fewer vendors, and (10) greater factory efficiency and availability due to faster production and fewer production problems.

- Design time is saved (1) by using purchased parts, (2) by using standard common parts, (3) by reusing previously designed work, (4) by farming out part design to part vendors, (5) by using modular (building block) design, (6) by more quickly converging on the optimal design, (7) by minimizing test development with higher product quality, (8) by reducing involvement in factory troubleshooting, (9) by reducing the number of engineering changes to write, and (10) by avoiding redesigns.
- Doing things right the first time means (1) no need for costly changes or redesigns, (3) quick and easy product introduction and ramp-up, (3) trouble-free production, and (4) lower product cost, higher quality, and faster delivery of goods.
- Designing for lean and build-to-order approaches helps engineering because (1) design time will be reduced with maximum use of standard parts and previous engineering work, (2) documentation time will be reduced, (3) prototyping and testing will be reduced, (4) design cost will be lower, and (5) cost estimating will be more accurate.
- Designing for lean and build-to-order helps manufacturing because (1) with similar parts built without setup, setup times will be reduced, (2) with setup reduced, lot (batch) sizes will be smaller, (3) work in process (WIP) inventories will be reduced, (4) with less WIP inventory, throughput will be higher, (5) quality will improve from more rapid feedback, (6) plant layout will be better, (7) less floor space will be needed, (8) product flow will be improved, (9) with less setup, machine utilization will be higher, (10) product and part scheduling will be better, (11) responsiveness to customers will be improved, (12) new product introduction will be quicker, (13) new-product introduction costs will be lower, (14) purchasing leverage for better price and delivery will increase, and (15) product cost will be lower.
- Benefits of modular design include (1) lower engineering cost with greater use of standard modules, (2) quicker time-to-market for modular products, (3) quicker delivery on standard products assembled from standard modules, (4) lower inventory from modular assembly, (5) easier servicing with module replacement, (6) wider product line with module combinations, (7) easier product upgrading with modular upgrades.
- Benefits from standardization affecting the cost factor include (1) lower purchasing costs with economies of scale, (2) lower inventory costs, (3) reduced floor space, and (4) reduced overhead.
- Benefits from standardization affecting the quality factor include (1) product quality better with fewer parts, (2) continuous improvement focused better, and (3) supplier reduction from fewer part types.
- Benefits from standardization affecting the flexibility factor include (1) easier machine setup because fewer parts have to be changed, (2) inventory reduction, (3) simpler internal material logistics, (4) faster possible deliveries of products,

and (5) support for lean-production, build-to-order, and mass-customization approaches.

- Benefits from standardization affecting the responsiveness factor include (1) greater possibility of building to order, (2) greater parts availability, (3) quicker deliveries from suppliers, and (4) stronger suppliers.
- Cost savings of purchased parts include (1) lower design costs because purchased parts do not need to be designed, (2) with fewer new designs to document, documentation cost is less, (3) prototyping and testing cost may be eliminated for purchased parts, (4) debugging and correction of part designs may not be necessary, (5) purchasing costs of purchased parts will be less than for the constituents of their manufactured counterparts, (6) the part cost will be less because of more efficient and specialized manufacture by the supplier, (7) with fewer manufactured parts to administer, administrative expense will be less, (8) with more refined parts, quality costs will be less, (9) suppliers may share warranty costs for their parts, and (10) overhead costs will be less because of all of the above.
- Time savings involving purchased parts include (1) less time spent designing parts that are available from a catalog, (2) less time spent documenting unnecessary designs, (3) less time spent building and testing prototypes, (4) less time spent debugging and redesigning parts, and (5) less time spent by manufacturing on parts that suppliers are more efficient in producing.

(c) DESIGN FOR LOW COST.[3] Because design determines more than three-fourths of a product's cost, the goal is to minimize the design cost as well as the total cost of a product. Some measures to achieve this goal include maximizing factory efficiency, lowering overhead costs through flexibility, minimizing customization and configuration costs, minimizing the cost of variety, minimizing materials management costs, minimizing marketing costs, minimizing sales and distribution costs, minimizing supply chain costs, minimizing cost of quality (COQ), and minimizing design life cycle costs, including engineering-change-order costs.

(d) DESIGN FOR HIGH QUALITY.[4] Quality must be built into the product first, instead of inspecting for it later. Quality problems must be corrected in the plant or factory before a product is shipped to customers. Like cost, quality and reliability are determined more by the design than is commonly realized. The type of part, the number of parts, and the part tolerance specifications all determine the inherent quality of the parts. Designers must ensure that parts are designed so they cannot be assembled in a wrong way (i.e., mistake proofing). The use of SPC techniques, ISO 9000 series standards, Six Sigma quality, TQM, and Taguchi methods, in part, can achieve the quality goal.

(e) DESIGN FOR FASTER PRODUCTION.[5] In concurrent engineering, multifunctional product development teams design products for the production or concurrently design products and new processes. When companies embark on flexible manufacturing strategies, concurrent engineering is crucial to the success of lean production, build-to-order, and mass customization approaches.

(i) Lean Production. Lean production or lean manufacturing accelerates production while eliminating many types of waste, such as setup time, excess inventory, unnecessary equipment handling and material movement, waiting time, low equipment utilization, defects, and rework.

(ii) Build-to-Order. Spontaneous build-to-order is the capability to quickly build standard products upon receipt of spontaneous orders without forecasts, inventory, or purchasing delays.

(iii) Mass Customization. Mass production deals with stable demand and little or no product variety. Mass customization deals with unstable demand and a variety of products targeted for niche markets or individual customers in a fast, cost-effective, and no-delays manner to handle various models, options, configurations, and customizations.

(iv) Design for Lean Production, Build-to-Order, and Mass Customization. Best practices for designing for lean production, build-to-order, and mass customization include the following:

- Design around standard parts.
- Design to reduce raw material variety.
- Design around readily available parts, components, and raw materials.
- Design for no or quick setup of machines.
- Design for use of computer numerically controlled (CNC) machine tools.

(v) Benefits of Lean Production, Build-to-Order, and Mass Customization. Benefits of lean production, build-to-order, and mass customization include cost advantage, customer responsive advantage, customer satisfaction, competitive advantage, and profit advantage.

(f) DESIGN FOR FASTER MARKETING. Design for marketing considers several factors, such as (1) customers' needs as gauged by QFD and VOC techniques, (2) breadth of product line brought about by lean production and build-to-order principles, (3) product customization using processes designed for mass customization, and (4) reduction of time-to-market using techniques to introduce new products early to the market.[6]

(g) DESIGN FOR SAFETY AND ERGONOMICS. Safety should not wait to be considered after product recall or the first lawsuit.[7] Careful design and simulations should be utilized to prevent safety-related problems before they manifest. Designers should make every effort to design safe products the first time as a moral and legal obligation.

Human factors and ergonomics are social considerations that should be considered at the very beginning, since ergonomic changes would be difficult or costly to implement after the design is complete. Good human-factors design of the product and process will reduce errors and accidents during its manufacture and use. Similarly, appearance and style should be considered as an integral part of the design, not something that is added later.

(h) DESIGN FOR A BETTER ENVIRONMENT. Environmental design considerations include handling product and process pollution, utilizing recycling products, handling air and water pollution, disposing hazardous waste materials, complying with laws and regulations (e.g., U.S. Environmental Protection Agency, EPA), and adhering to international environmental standards (e.g., ISO 14000 series standards).[8]

(i) DESIGN FOR SERVICEABILITY. Design for serviceability focuses on a product's post-sales activities, such as parts/modules repair and maintenance work performed either at the factory or in the field site.[9] The goal is to facilitate an ease of repair and ease of maintenance of parts and modules.

An ease-of-repair strategy is to simply replace the worn, damaged, or nonfunctional part or module or that is to be repaired, discarded, or recycled. An ease-of-maintenance strategy depends on the reliability of the product and demands for uptime, (i.e., how much time the product needs to be available for use). Maintenance is performed either on an unscheduled basis after some parts or modules fail (unscheduled maintenance) or on a scheduled basis to replace parts and modules before they are likely to fail (preventive maintenance). The product designer must consider both parts/modules repair and maintenance needs well before the product is fully designed.

Following is a summary of guidelines concerning design for ease of repair or ease of maintenance:

Design for Ease of Repair

- Provide ability for tests to diagnose problems.
- Make sure the most likely repair tasks are easy to perform.
- Ensure repair tasks use the fewest tools.
- Use quick disconnect features.
- Ensure that failure- or wear-prone parts are easy to replace with disposable replacements.
- Provide inexpensive spare parts with the product.
- Ensure availability of spare parts.
- Use modular design to allow replacement of modules.
- Ensure modules can be tested, diagnosed, and adjusted while in the product.
- Allow protection of sensitive adjustments from accidental changes.
- Protect the product from repair damages.
- Provide part-removal aids for speed and damage prevention.
- Protect parts with fuses and overloads.
- Ensure any module or subassembly can be accessed through one door or panel.
- Make sure access covers cannot be removed and are self-supporting in the open position.
- Make sure connections to modules or subassemblies are accessible and easy to disconnect.
- Make sure repair service or maintenance tasks pose no safety hazards.
- Make sure subassembly orientation is obvious or clearly marked.
- Provide means to locate subassemblies before fastening.
- Provide unobstructed access to parts and tools.

- Make parts independently replaceable.
- Order assembly so the most reliable part goes in first, the most likely fail part goes in last. This is to ensure that the most likely parts to fail are the easiest to remove.

Design for Ease of Maintenance

- Design products for minimum maintenance.
- Design self-correction capabilities into products.
- Design products with self-test capability.
- Design products with test ports.
- Design-in counters and timers to aid preventive maintenance work.
- Specify key measurements of wear and tear for preventive maintenance programs.
- Include warning devices to indicate failures (e.g., alarms, lights, buzzers, and beeps).
- Use plug-in modules (plug and play) to facilitate field maintenance work and to allow modules to be repaired off-line, where there are better repair and diagnostic facilities available.

5.5 INVENTORY AND LOGISTICS MANAGEMENT

(a) OVERVIEW. Inventories of raw materials, ingredients, components, parts, and finished goods constitute a major portion of current assets for both private-sector and public sector organizations. For example, the U.S. Department of Defense (DoD) has several billion dollars worth of inventories stored either at their own facilities or at the defense contractors. In addition to reducing inventory levels and logistics costs, best practices will provide inventory users with a capability to order supplies as they are needed and then delivering those items directly to the customer within hours after the order is placed. Ordering supplies only as they are needed, combined with quick logistics response times, enables companies to reduce or eliminate inventory levels, buy only the items that are currently needed, reduce or eliminate the possibility of inventory spoilage or obsolescence, and reduce overall supply system costs.[10]

(b) INVENTORY AND LOGISTICS MANAGEMENT BEST PRACTICES. Implementing the following best practices can reduce logistics costs and improve inventory management systems. Not all best practices are suited to all organizations, and each organization should select and implement those best practices that fit its business operations.

(i) Best Practice 1: Establish the concept of a prime vendor. A single vendor (prime vendor) buys inventory from a variety of suppliers and stores the inventory in its warehouse. This concept is characterized by a close partnership between the prime vendor and the customer. The customer orders supplies from the prime vendor, using electronic ordering systems that, in some cases, are provided by the prime vendor. The prime vendor then delivers inventory items to the customer within hours of receiving the order.

(ii) Best Practice 2: Establish the concept of local distribution centers or supplier parks. One or more suppliers locates a distribution center within close proximity to customers. From this location, the supplier delivers items to the customer within 24 hours or less of receiving an order. The supplier is linked electronically with the customer. In some cases, the supplier can perform the receiving function for the customer in the local distribution center before the inventory leaves the facility.

(iii) Best Practice 3: Establish the concept of an integrated supplier. An integrated supplier assumes almost total inventory management responsibilities for a customer. This is the most aggressive form of a supplier partnership, with a supplier representative working in the customer's facility, ordering supplies as they are needed, and replenishing storage locations. Inventory is stored by the supplier in the supplier's warehouse until ordered and then delivered on a just in time (JIT) basis. An integrated supplier can also perform quality inspections, maintain data on usage, test the quality of parts, prepare parts kits, establish electronic data interchange (EDI) links and bar coding, and provide vendor selection management.

(iv) Best Practice 4: Establish the concept of direct vendor delivery. Some organizations practice direct vendor delivery concepts by using long-term contracts and electronic data systems to enable certain suppliers to deliver items directly to the customer instead of having the items delivered to company warehouse. Although the direct delivery program eliminates the need to store and distribute inventory from the company warehouse, lowering the cost to the company customer, it does not provide a quick response to customer orders. Using the prime vendor or integrated supplier concepts reduces average delivery times for inventory far more effectively than the direct vendor delivery concept.

(v) Best Practice 5: Reengineer the logistics systems and operations. Many firms have radically changed or reengineered their logistics systems and operations to meet customer needs and retain profitability. For example, commercial airlines have cut costs and improved customer service by streamlining their logistics operations. The most successful improvements include using highly accurate IT systems to track and control inventory, employing various methods to speed the flow of parts through the pipeline, shifting certain inventory management tasks to suppliers, and letting third parties handle parts repair and other functions.[11]

For example, a major airline firm has reengineered its practices in five general areas such as corporate focus and culture, information technology, material management, repair processes, and facilities. Each of these areas is presented next.

Corporate Focus and Culture

- Top management champions of change with full authority to make changes
- Integrated pipeline management
- Performance measures aligned with corporate goals
- Successful continuous improvement
- Use of third parties to reduce complexity and cost of pipeline

Information Technology

- Accurate information on amount, location, condition, and usage of inventory
- Real-time inventory data
- Extensive use of data systems to track and manage flow of parts
- Timely development of new computer systems

Material Management

- Supplier partnerships, reduced supplier base
- Supplier-operated local distribution centers to delay purchase of inventory until needed
- Fast, reliable deliveries
- Reduction in layers of inventory
- High fill rates
- Reduction of just-in-case inventory

Repair Processes

- Cellular process, fast turnaround times
- Repair of individual parts as they break
- Availability of parts when required for repairs

Facilities

- Facilities reflecting new business practices
- Green-field sites reflecting the most aggressive changes

(vi) Best Practice 6: Reengineer transportation systems and operations. Corporate shippers committed to improving their transportation practices share common elements in their management strategies. Commercial shippers recognize that top management commitment and support to improve transportation management are important. Shippers are taking a number of actions to reduce costs and achieve efficiencies, such as integrating transportation functions with the entire logistics chain, reducing the number of carriers they use and focusing on the highest performing carriers to promote stability and enhance leverage, and using IT to aid in transportation decision making. In addition, shippers are increasingly contracting out certain transportation functions to take advantage of lower costs and attain flexibility during market swings.[12]

Organizations should do the following:

- Understand that top-management commitment drives quality transportation management efforts.
- Integrate transportation systems into a logistics chain to promote process efficiencies.
- Use a smaller number of carriers to achieve quality and cost benefits. This requires (1) focusing on quality, (2) tracking carrier performance data supplied by carriers, (3) conducting on-site inspections to support carrier qualification efforts, and (4) simplifying the carrier selection process through the use of contractual arrangements, which can promote cost efficiencies for carriers and shippers.

- Use IT systems in transportation decision-making efforts. This includes automating functions such as preauditing, freight rating, and shipment tracking to improve operations and reduce costs.
- Use outsourcing, benchmarking, and third parties to reduce costs and improve service.
    - Commercial shippers have *outsourced* functions from freight bill payments and carrier performance analysis to entire logistics operations. Outsourcing provides the following benefits (1) savings from not investing in an internal transportation staff, (2) savings from not investing in fixed assets, (3) the flexibility to get in and out of markets, (4) a ready source of expertise, capability, and technology, and (5) the ability to gain cost advantage from an outsourcer's business volume.
    - Commercial shippers are using *benchmarking* as a technique to improve logistics practices. These practices include (1) developing a simplified rating system for motor carriers, (2) reassessing freight bill payment operation, and (3) streamlining the motor carrier base.
    - Commercial shippers are actively using *third-party* logistics firms to perform particular transportation functions. These functions include payment of freight bills and associated freight payments duties, along with electronic data interchange (EDI) system functions.

(vii) Best Practice 7: Increase inventory turnover rate. The inventory turnover rate is a measure of how efficiently a business uses its inventory investment and can be expressed as the ratio of the dollar value of cost of goods sold, or sales, to the average inventory value.

(viii) Best Practice 8: Instead of using the economic order quantity formula, use alternative methods such as quick response. Leading companies do not rely on the economic order quantity (EOQ) formula to make purchase decisions. They do not the use the EOQ formula because of its assumption that the demand rate is constant. These companies operate in environments where demand for their items varies over time. In addition, the EOQ formula assumes that replenishment is instantaneous, even though it is rare for a vendor to replenish an item the same day that it is requested. Hence, the EOQ formula is more theoretical than practical.

Leading companies are using "quick response" purchasing methods that, while based on EOQ principles, have been tailored to their operations so that items are delivered just before they are needed. The shift to alternative purchasing methods depended heavily on companies being able to motivate suppliers and employees. Companies are retraining their own employees so that they no longer maintain excess inventory.

(ix) Best Practice 9: Use automated tools and systems for managing inventory, customer orders, and customer payments. Automated tools and systems provide several benefits, including shorter procurement lead times, less paperwork, greater accuracy in forecasting future item demands, and reduced inventory levels.

Organizations should do the following:

- Implement an electronic data exchange or interchange (EDI) system to receive price quotes from suppliers, transmit orders, and award notifications. This automated system reduces paperwork, lead times, and mailing costs.
- Develop paperless order-placement and payment systems to place orders, submit invoices, and pay invoices between suppliers and the organization.
- Implement quick response (QR) systems for faster delivery of goods between suppliers, producers, and consumers

5.6 SUPPLY CHAIN MANAGEMENT

(a) OVERVIEW. Companies today are facing a competitive environment characterized by global competition, shortened product life cycles, increased customer demands, and technological innovations. The transition from transactional, adversarial business relationships to partnership-oriented, cooperative, longer-term relationships is one strategy that companies are pursuing to remain competitive in this new environment. A partnership between organizations is a relationship that requires an understanding of each other's needs, common goals, commitment, trust, communication, and a willingness to work through problems.[13]

Leading companies have become increasingly aware that they cannot do everything on their own, including reducing costs. Therefore, companies are rethinking their business relationship and taking steps such as developing closer relationships with strategic suppliers and evaluating the possibilities of contracting out noncore functions. Companies have found that cooperative business relationships improve their ability to respond to the new economic environment by allowing them to focus on their core businesses and reduce costs in their business processes.

Partnership relationships are occurring in all areas of business, including logistics, inventory, manufacturing, and research and development. The decision to use a partnership approach in a business relationship is based on whether the potential partners believe that they can benefit from such a relationship and that the benefits outweigh the costs. Partnerships are not developed with every supplier and are carefully considered to make sure the factors needed for success are present. These relationships require an investment of resources and may not be appropriate for obtaining goods and services, for example, when price is the primary selection criterion. Also, companies that have achieved benefits from partnerships demonstrate common characteristics, including strong top management support, an organizational culture that values cooperative behavior (such as open communications, information sharing, and trust), and a commitment to work toward mutual benefits and longer-term goals.

These relationships, however, can pose risks. A company can become too dependent on one or two suppliers, or it may become complacent in holding the relationship to its goals and accountability standards, possibly resulting in noncompetitive prices. It is necessary to develop strong management best practices to ensure the relationship is meeting its goals and to minimize the risks. These practices include contract terms, intensive management involvement, performance monitoring, internal controls, problem-solving procedures, and periodic evaluations. Partnering that has been successfully implemented by some companies has resulted in reduced costs, improved service,

better quality, and increased business opportunities for both partners. The net result is a shorter order-to-delivery cycle through streamlining business processes and focusing on core businesses. Some companies have achieved improved cost, schedule, and performance goals.

(b) SUPPLY-CHAIN BEST PRACTICES

(i) Best Practice 1. Companies should evaluate needs and goals before forming partnerships. Leading companies are forming closer, collaborative partnerships, but only when they believe they will benefit from investing in the relationship in terms of reducing cost and improving quality. The process for selecting partners is based on obtaining a clear understanding of the needs and capabilities of the potential partners to help ensure that the parties meet the goals of the relationship.

(A) Companies should Weigh Benefits and Costs When Deciding to Partner

The choice between a partnership and a traditional relationship depends on a company's business strategy and a comparison of potential benefits from a partnership to the investment of time and money. Partnership relationships should not be developed with every supplier or customer because partnerships require an investment of time and resources. Also, a closer relationship is not always appropriate for obtaining goods and services. For example, when price is the only criterion for purchasing a commodity or service, a partnership would not be worth the investment.

(B) Partners should be Carefully Selected

Once a company decides a partnership approach would be beneficial for obtaining a particular good or service, the process for selecting a partner begins. The process for selecting a partner should be structured to ensure the relationship will meet its intended goals. Some of the selection methods include up-front discussions with potential partners, unique selection criteria reflecting the goals of the relationship, and cross-functional input to the decision-making process.

Supplier Selection Criteria

If suppliers have to compete on price only, they have no incentive to make long-term investments for the relationship that can lead to reducing costs and improving quality and service.

The criteria used to select partners reflect the needs of the buyer, the capabilities of the supplier, and the potential to achieve benefits. Criteria can range from quality and service standards to more unique criteria such as a compatible corporate culture, business reputation, and willingness to invest resources in the relationship. Some companies evaluate suppliers on technology, quality, responsiveness, delivery, costs, and environmental concerns. Some companies use cross-functional teams to select partners from a quality as well as financial standpoint.

(C) Companies in Successful Partnerships should have Common Characteristics

Partnership arrangements are more likely to achieve benefits if the partner companies had top management support for partnering, an organizational culture that values cooperative behaviors such as open communications and the sharing of information, and a

commitment to mutual benefits and long-term goals. Achieving these benefits requires a different approach from traditional relationships. As this behavior occurs and companies can see some mutual benefit, trust among partners grows. Trust, in turn, nurtures further sharing of information and open communications, which lead to further mutual benefits and a commitment to longer-term goals.

Common Characteristics of Successful Partnerships

- Mutual benefits
- Top management support
- Compatible organizational culture
- Sharing of information
- Strong and open communications
- Commitment to longer-term goals
- Trust

(ii) Best Practice 2. Management practices should keep partnerships on track and minimize risks. Strong management practices, which also provide continuous oversight of the relationship, help to ensure accountability of the relationship and minimize the risks of partnership arrangements. The specific management practices used by leading companies vary, but generally include contract terms, intensive management involvement, performance monitoring, internal controls, problem-solving procedures, and periodic evaluations. In addition to these practices, a big incentive that helps prevent fraud and abuse from occurring in partnerships is that a company's reputation will be severely damaged if the company has violated the integrity of a partnership.

Possible risks faced in partnership arrangements include becoming dependent on one or two suppliers and sinking into complacency, with one or both partners becoming lax in holding the relationship to its goals and accountability standards. Companies are also concerned that these relationships can lead to noncompetitive prices, since the relationship is intended to last for a longer period.

(A) A Written Contract should be Developed with Important Clauses and Specifications

Leading companies in partnership arrangements use contracts to guide the relationship and ensure that both parties understand each other's needs and goals, rather than to dictate and restrain the relationship. Contracts and agreements that guide partnership relationships last for at least a year, but they more commonly last for a longer period, such as five years. Typically, both parties agree to renew the contract as long as the performance and benefit goals are being met.

The form of the contract depends on the service or commodity, and some are more detailed than others are. Traditional contracts, having many contingency clauses and specifications to prescribe action for every conceivable event, could hinder a partner-oriented relationship because too many specifications could discourage open discussion, which could lead to initiating and making changes that reduce costs or improve quality. However, contracts may contain clauses to safeguard information or resources. It is good to include a nondisclosure clause in each contract to protect sensitive and proprietary information.

(B) Management Involvement should be Intensive

Successful implementation and operation of a partner relationship depend on having in place a supportive management framework that includes participation by all parties impacted by the relationship from top management to frontline employees. Most companies organize cross-functional teams that may include representatives from the partner organization. These teams, which are similar to the cross-functional teams used to select partners, ensure that all functions impacting a partnership, such as logistics, purchasing, finance, and production, are coordinated to maximize benefits from the relationship. These teams may manage the day-to-day operations of the relationship, solve problems as they arise, and address strategic aspects of the relationship.

Top management involvement varies depending on the strategic importance of the concerns that need to be addressed. Companies may form a management board or executive board consisting of top management from both partner companies to oversee their service or commodity arrangements. These top managers should meet three to four times a year, switching the location of the meeting between the two companies to send the message that they are equal partners.

(C) Partner Performance should be Monitored

Leading companies stress the importance of having performance- monitoring systems to ensure that the relationship's goals are being met, prevent problems, and identify opportunities for additional benefits. Performance measures can include quality standards, service standards, price and cost comparisons, and financial condition. Some companies use service-level agreements to establish daily service-level goals, such as number of outages and response times with a monthly reporting system. Monitoring the relationship minimizes the risks of dependency on fewer suppliers, complacency, and noncompetitive pricing.

Even though companies face a risk in depending on one or two suppliers for a particular good or service, companies also can better monitor a smaller supply base and identify suppliers with problems. With ongoing monitoring, companies have more time to develop a remedy, such as assisting the supplier or identifying an alternative source.

(D) Information and Resources should be Protected with Internal Controls

Internal controls are used to protect information and resources from fraudulent or questionable practices. For example, a purchasing requisition requires approval from the user and accounting departments before a supplier is paid for an order.

(E) Procedures should be Developed to Solve Problems

Problem solving is accomplished faster with less animosity in a partnership. In traditional relationships, a problem created a confrontation that hindered the individual firms in reaching a solution. In an uncooperative environment, distrust was usually due to miscommunication because each company was looking out for itself, suspecting the other company would take advantage of the situation, and not seeing the impact of the relationship on each other's bottom line. In a cooperative environment, the buyer and the supplier work together to solve problems.

Leading company employees are encouraged to communicate problems as they arise and work toward resolving the problem together rather than pinpointing blame. Furthermore, recognizing a problem and finding a solution are often left to the people

directly involved rather than passed on to a third party, unless the problem requires attention from upper management or another department.

(F) Periodic Evaluations should be Conducted

It is important to periodically evaluate the need for continuing, changing, or ending the relationship because relationships evolve over time and face unforeseen changes in conditions. Companies usually continue the relationship as long as both continue to benefit. Leading companies conduct annual performance reviews of suppliers, carriers, and partners instead of rebidding the business every year. Two additional opportunities are given to a poor performer to improve performance before the relationship is terminated. In general, when one or both companies no longer continue to benefit from the added investment needed to maintain a partnership relationship, then the companies may choose either to continue in a more traditional, transactional arrangement or end the relationship.

5.7 WORLD-CLASS SERVICE MANAGEMENT

(a) SERVICE STRATEGY. The U.S. service economy is growing at a more rapid rate than the manufacturing economy. Many services have characteristics that are strongly different from manufacturing of goods or products. Consequently, specialized and different management techniques are employed in services than are employed in many manufacturing firms. For example, knowledge and experience gained from studying manufacturing settings does not always transfer to services.

Some of the ways in which services are said to be different from goods include (1) intangibility, (2) simultaneous production and consumption, (3) closer proximity to the customer, and (4) lack of inventory.

Critical Success Factors for a World-Class Service Function

Critical success factors for a world-class service function include value creation to customers and the organization, service cost minimization, service quality improvement, faster and stable service, quick response to customers, spend analysis, listening to stakeholder voices, leadership, organizational culture, customer service, organizational structure, technology, process, and people.

Strategies for world-class service organizations include focus on a target market, determination of a service concept, development of an operating strategy, and implementation of a service delivery system linked to a service level agreement (SLA). These specific strategies can be combined with overall corporate and competitive strategies such as cost leadership, differentiation, focus, quality, speed, and flexibility.

World-class service organizations implement various combinations of tools, techniques, practices, and standards to achieve excellence in service operations. Some examples of tools, techniques, and practices include Six Sigma quality, statistical process control (SPC), quality function deployment (QFD), voice of the customer (VOC), TQM, lean service practices, and various design methods such as design for serviceability, design for low cost, design for high quality, design for faster processing, and design for faster marketing. For organizations that handle both manufacturing and service operations, product quality affects service quality due to their interconnection.

Some examples of standards include ISO 9000 series standards and the industry standards. These tools, techniques, practices, and standards must be combined with management systems such as survey of customers, contractors, consultants, employees, management, and the industry; self-assessments; industry research reports; audits; management reviews; and benchmarking studies.

(b) LISTENING TO STAKEHOLDER VOICES. Service management, as a provider of services for the company, should pay close attention to the following "voices" to achieve organizational goals and improve overall performance. When these "voices" are heard together, they bring attention to new perspectives and creative conflicts, forcing new thinking that leads to new solutions (i.e., best-of-breed solutions). Listening to the collective voice of many stakeholders at once will have a greater impact than listening to one voice at a time in isolation, because the former requires a balanced approach after considering all party's concerns.

For each content of each voice, a T-Column analysis should be prepared, with "what happens if I listen to this voice" in the left column (benefits) and "what happens if I don't listen to this voice" in the right column (costs and risks). A comparative analysis of each content in each column will point to new problems requiring new solutions.

- Voice of the customer (external customers such as suppliers, vendors, contractors, consultants, key customers, regulators, investors, creditors, stock market, and media/press, and internal customers such as board of directors, corporate management, and employees in other functional departments such as marketing, human resources, finance, and IT)
- Voice of the process (process flows, process variations, process delays and waste, and process inefficiencies)
- Voice of quality (TQM principles and practices, mistake-proofing, continuous improvement, cost of poor quality, quality engineering, quality assurance, quality control, quality audit, quality council, quality circles, certified vendors and suppliers, and quality control/management tools)
- Voice of standards (service design standards, service-testing standards, service delivery standards, and industry/organization standards)
- Voice of partners (service technology partners, service-sourcing vendors, supply chain members, electronic commerce vendors, packaging vendors, and outsourcing vendors such as call center)
- Voice of regulators (federal, state, and local laws and regulations)
- Voice of competitors (press releases, Web site pressrooms, industry magazines, daily business newspapers, advertising magazines, industry trade shows, product demonstrations and promotions, direct mail, e-mail campaigns, copyright/ trademark/ patent news, business intelligence news, banner advertising, billboard and street advertising, product sponsorships, and online events and chat rooms)

(c) SERVICE-CYCLE TIME MEASURES. Cycle time reduction in service deals with reducing the order-to-delivery cycle, with associated benefits such as increased productivity,

improved utilization of human and machine resources, decreased costs, and improved customer service. To attain these benefits, organizations must:

- Eliminate or decrease non-value-added activities (e.g., fully paper-driven manual systems; number of handoffs; rework time; redundant tasks; too many approvals; waiting time; customer call hold time; customer hassle factors; and delays at the interdepartmental and interdivisional boundaries and at the intradepartmental work stations).
- Enhance or increase value-added activities (e.g., pure service time; task process time; customer interaction time, response time to customer; service completion time; internal/external customer access points to service systems; service project hold points; and service management decision points and control points).

This requires having the right employees available at the right place and at the right time so that delays and waste in service operations are decreased.

(d) SERVICE METRICS. Service metrics deals with post-sales activities such as part/module repairs and maintenance. Service management should develop and track the following key performance indicators (KPI) and metrics to improve performance:

- Number of abandoned customer calls at the call center due to excessive "hold time"
- Percentage increase in the quality-assurance scores for customer service representatives
- Percentage increase of customer problems resolved on the initial call
- Percentage increase in meeting service levels as defined in the service level agreements (SLAs)
- Number of repeatable tasks automated
- Number of redundant tasks eliminated
- Number of unnecessary handoffs removed
- Number of unnecessary approvals from supervisor/manager removed
- Percentage increase in product uptime, which is measured by the mean time between failures (MTBF)
- Percentage decrease in product downtime, which is measured as mean time to repair (MTTR) plus the mean restore time (MRT)
- Percentage increase in product availability time, which is (uptime)/(uptime + downtime)
- Percentage decrease in part-repair time for a homogenous group of parts
- Percentage decrease in part-maintenance time for a homogenous group of parts
- Percentage increase in spare parts/modules availability rate
- Number of products designed with self-correction and self-test capabilities such as test ports
- Number of products designed with devices to indicate failures such as alarms and lights and with self-diagnostic capabilities
- Percentage increase or decrease in the number of customer complaints by service category this year and compared to previous years.

- Total service warranty costs expressed as a percentage of total service operating costs or revenues this year and compared to previous years.

5.8 SERVICE DESIGN AND DEVELOPMENT

(a) OVERVIEW. Similar to product design and development, services must be designed and developed. Processes are used to render a service to customers. Since each organization's service activities are different, separate processes are needed to accomplish those activities. For example, policies, procedures, and processes for handling an automobile accident claim by an auto insurance company can be totally different from that of a medical claim handled by a health-care insurance company. The identified processes must be simple and intuitive whether they are handled through paper or online. Service processes must be streamlined to eliminate non-value-added activities and to reduce hold (wait) time and handoff time. Customer convenience and total customer satisfaction must be carefully considered, designed, and developed into policies, procedures, and processes.

(b) CALL-CENTERS AND CUSTOMER-SERVICE OPERATIONS BEST PRACTICES. Since people provide services with the help of technology and computer systems and equipment, we will focus here on two common service areas such as call centers and customer service operations. Leading service organizations have established three goals for their telephone customer service operations. First, human capital needs are determined, with skill mixes and the number of staff depending on service-level goals, which drive call center staffing and budgeting levels. Second, call center goals should be embraced by top management, which must understand the role of telephone customer-service operations in meeting overall organizational goals and objectives and is willing to commit the resources needed to meet them. Third, managers should regularly reassess human capital needs in the context of a changing environment, using a strategic planning process to predict changing conditions for the long and short term and respond to these changes in a positive manner.[14]

CAVEATS IN ESTABLISHING CALL CENTER SERVICE-LEVEL GOALS

Call center service-level goals measure the percentage of calls of all types that are answered within a given time period. Service-level goals are not the only goals that are important for call centers to establish. For example, these goals do not address the quality of the telephone service provided in terms of quality of responses. Certainly, a call center could meet appropriate service-level goals and still provide poor service, with callers receiving inaccurate information, discourteous treatment, or answers to questions that they never asked. This fact notwithstanding, service-level goals are the first goals that call centers need to set.

Organizations should do the following:

- Establish service-level goals as a basis for human capital needs, with supportfrom leaders and regular reassessment. This should include (1) basing of staffing needs on clearly articulated service-level goals, (2) supporting call center goals by top leaders, (3) assessing human capital needs in the context of a changing environment, such as changes in technology, caller demographics, and service goals, and (4) using flexible staffing options to handle short-term changes in call volumes.

- Provide effective leadership and competitive compensation as keys to successful human capital management. This includes (1) showing respect for employees and communicating openly, (2) maintaining effective working relations with labor unions, (3) providing training for a broad overview of operations, and (4) defining individual performance standards using qualitative and quantitative measures.
- Evaluate performance of call centers and individual customer service representatives using metrics such as:
  - Quality assurance scores of X% on the basis of the results of monitoring a sample of telephone calls
  - Customer satisfaction scores of X%
  - X% of calls answered within Y seconds
  - X% of call abandonment rate
  - Call handling time of X minutes and Y seconds

  Call center performances should be evaluated through regular surveys of customers and employees. Customer satisfaction should be evaluated through telephone surveys of a random sample of callers and postcard mailings. The surveys should be analyzed to provide information on
  - The demographic profile of customers
  - How well caller expectations are being met
  - Caller satisfaction with the automated voice response system
  - Satisfaction with telephone customer service representatives' performance in core competency areas
  - Factors most important to achieving overall caller satisfaction

  Postcard mailings to customers can help to measure telephone customer service representatives' professionalism, courtesy, knowledge, and problem resolution skills.

  Customer service representatives should be surveyed annually to determine how satisfied they are with their jobs, and allowed to participate in quarterly forums with management to address any issues they want to raise, ranging from allocation of parking spaces to work schedules. The results of the surveys and forums should be provided to all call center managers and employees for "lessons learned."
- Use the results of evaluations to make improvements in human-capital management strategies and practices. These improvements include (1) identifying, implementing, and evaluating the need for continuous improvement, (2) hiring more people, changing training-course content and delivery, (3) improving recruiting and hiring strategies, and (4) doing evaluations of call centers.

5.9 SERVICES ACQUISITION MANAGEMENT

(a) OVERVIEW. Private-sector organizations are increasingly reliant on services, in that the majority of purchasing dollars for some companies now goes to acquiring a range of services, from complex services such as advertising, information technology (IT), and professional consulting services, to relatively simple services such as lawn mowing, waste removal, and temporary clerical services. Similarly, the public sector organizations

spend billions of tax dollars to buy services ranging from clerical support and consulting services to IT services such as system development, maintenance, and network support, to the management and operation of facilities.[15]

Leading private companies have been examining alternative ways to manage their service spending to stay competitive, respond to market and stockholder pressures, and deal with economic downturns in key overseas markets. In looking at their service acquisition, these companies discovered that they did not have a good grasp of how much was actually being spent and where these dollars were going. They found that responsibility for acquiring services resided largely with individual business units or functions, such as finance, human resources, manufacturing, engineering, or maintenance, which hindered efforts to coordinate purchases across the company. They also came to realize that they lacked the tools needed to make sure that the service they purchased met their business needs at the best overall value. To turn this situation around, leading companies reengineered their approach to buying services.

The leading companies made a number of dramatic changes to the way they bought services and found that these changes, in turn, resulted in significant cost savings and service improvements. These changes generally began with a corporate decision to pursue a more strategic approach to acquiring services. Taking a strategic approach involves a range of activities from developing a better picture of what the company is spending on services, to taking an enterprise-wide approach to procuring services, to developing new ways of doing business.

Once top leaders were committed to taking a strategic approach, the companies took a hard look at how much they were spending on services (using spend analysis) and from whom. By arming themselves with this knowledge, the companies could identify opportunities to leverage their buying power, reduce costs, and better manage their suppliers. The companies also instituted a series of structured process and role changes aimed at moving away from a fragmented acquisition process to a more efficient and effective enterprise-wide process. Some companies have established or expanded the role of the corporate procurement department to help business unit managers acquire key services, making extensive use of cross-functional teams to help the companies better identify service needs, select providers or suppliers, and manage contractor performance.

What is Spend Analysis?

Spend analysis is a tool that provides companies with knowledge about how much is being spent for what goods and services, who the buyers are, and who the suppliers are, thereby identifying opportunities to leverage buying, save money, and improve performance.

Some obstacles faced by the leading companies during this transition include resistance from individual business units reluctant to share decision-making responsibility and to involve staff that traditionally did not communicate with each other. To change this mindset of business unit management required a strong commitment from their senior leadership in terms of communicating the change's rationale, its goals, and the expected results from the reengineering efforts, including feedback through a measurement system and metrics.

Taking a strategic approach paid off, as companies found that they could save millions of dollars and improve the quality of services received by instituting the changes.

In some cases, thousands of suppliers were reduced to a few, enabling the companies to negotiate lower rates. In other cases, new IT systems enabled companies to better match their business managers' needs quickly with potential suppliers or providers.

(b) PRINCIPLES AND BEST PRACTICES IN SERVICE ACQUISITIONS. There are four principles, such as commitment, knowledge, change, and support, along with their best practices in service acquisitions. These principles and practices largely reflect a common-sense approach toward almost any business venture, that is, providing good leadership, developing and harnessing knowledge, making sure business processes maximize return, and measuring results.

(i) Principle 1: Secure up-front commitment from top leaders. **Best Practices**: (1) Recognize and communicate the urgency to change services spending practices, and (2) Provide clear and strong executive leadership, including goals and targets.

In general, successful reengineering efforts are spearheaded by a company's senior management since they have the authority to require employees to accept reengineered roles, the responsibility to set the corporate agenda and to define the organization's culture, and the ability to remove barriers that block changes to the organization's corporate mindset. Exhibit 5.2 describes changes in senior management's involvement in the purchase of services.

(ii) Principle 2: Obtain improved knowledge on service spending. **Best Practices**: (1) Develop information systems to identify how much is being spent with which service provider for what services, and (2) Analyze the data to identify opportunities to reduce costs, improve service levels, and provide better management of service providers.

Leading companies analyzed their spending on services to answer the basic questions of how much was being spent and where the dollars were going. After conducting the analyses, the companies realized that they were buying similar services from numerous providers, often at greatly varying prices. Such knowledge brought home the need for companies to become more strategic in planning and managing their service acquisitions to maintain a competitive edge. Exhibit 5.3 compares the traditional and strategic approaches to spending data.

Leading companies used spend analyses to identify opportunities to rationalize their supplier base and reduce costs. At a minimum, a basic spend analysis should identify the following:

Traditional Involvement	Strategic Involvement
Services are viewed as ancillary to core business	Services are viewed as central to core business
Senior managers are not actively involved in pursuing changes to how the company acquires services	Senior managers provide direction and vision for change, establishes goals and targets, and devotes increased attention to services

EXHIBIT 5.2 CHANGES IN SENIOR MANAGEMENT'S INVOLVEMENT IN THE PURCHASE OF SERVICES

Traditional Approach to Spending Data	Strategic Approach to Spending Data
Financial and IT systems focus on raw materials, parts, and components used to make products, but do not provide data needed to effectively manage the company's service spending	IT systems are developed to provide credible, reliable, and timely data on acquired services
Data is used principally for ''after the fact'' reporting purposes	Data is used to identify opportunities to rationalize supplier base and reduce costs

EXHIBIT 5.3 COMPARISON OF TRADITIONAL AND STRATEGIC APPROACHES TO SPENDING DATA

- What types of services are being acquired?
- How many suppliers are involved in providing a given service?
- How much is being spent for that service, in total and with each supplier?
- Which business units within the company are purchasing the service?

Some companies augmented this basic information with more detailed data, such as the number of labor hours purchased, the hourly wage rate paid, and the amount of overhead paid. In addition, they used spend analyses as part of their process to identify additional targets of opportunity, measure compliance with preferred supplier agreements, respond to customer input, and track progress toward meeting annual performance goals and objectives.

(iii) Principle 3: Create supporting structures, processes, and roles to support an enterprise-wide perspective. **Best Practices**: (1) Create or identify departments responsible for coordinating or managing service purchases, (2) Establish proactive business relationships between end users, purchasing units, and other stakeholders, (3) Implement more integrated team-based sourcing processes, and (4) Create commodity or service experts in the organization.

Leading companies found it necessary to change how they acquired services, principally in terms of business processes, organizational structures, and roles and responsibilities. These changes were meant to take the companies from a fragmented way of doing business to one that was more coordinated and strategically oriented. The end goal was to institute an enterprise-wide perspective—one that would ensure that the company was getting the best overall value. Among other changes, companies elevated or expanded the role of the procurement department; designated full-time dedicated commodity managers to oversee key services; and made extensive use of cross-functional teams to help identify the company's service needs, conduct market research, evaluate and select providers, and manage their performance. Exhibit 5.4 describes the changing role of purchasing.

In making such changes, the companies positioned themselves to more effectively manage and coordinate their service purchases. These changes transformed the role of their purchasing units from one focused on mission support to one that was strategically important to the company's bottom line.

Traditional Purchasing	Strategic Purchasing
Independent, local functions with limited visibility over the company's total service spending	Central/matrixed functions responsible for coordinating or managing service purchases
Reactive support role to business units	Proactive business relationships
Limited coordination between business and purchasing units and other functions such as legal or finance	Procurement process based on cross-functional teams
Buyers or agents	Commodity or service experts

Exhibit 5.4 Changing Role of Purchasing

(iv) Principle 4: Enable success through sustained leadership, communication, and metrics. **Best Practices**: (1) Obtain sustaining support from senior leadership to facilitate change, (2) Establish clear lines of communication between all affected parties, and (3) Demonstrate the value and credibility of new processes through use of metrics.

Leading companies have found that three ingredients were critical to overcoming resistance, cultural barriers, and other impediments to their reengineering efforts: sustained leadership, communication, and measurement. Exhibit 5.5 describes characteristics promoting successful strategic reengineering efforts.

Metrics increases the likelihood that reengineering efforts will be successful. Companies typically measure total savings, cost avoidance, or some other financial measure, which are often reported to senior corporate management. Senior managers set targets for its procurement function at the beginning of the year and regularly reviews progress reports. One company has established a three-tiered system to measure the performance of the procurement function.

- The first tier consists of top-level metrics to assess the procurement function's progress in meeting financial, customer satisfaction, and business operation objectives
- The second tier is used for performance monitoring and internal/external benchmarking purposes

Traditional Purchasing	Strategic Purchasing
Corporate leaders not actively engaged in improving service acquisitions	Senior leaders actively reinforce commitment to achieve change
Business units and purchasing units do not clearly communicate or cooperate	Clear lines of communication between all affected parties
Performance measures do not exist	Performance measures are used to demonstrate value and credibility of new reengineered processes

Exhibit 5.5 Characteristics Promoting Successful Strategic Reengineering Efforts

- The third tier is used at the local site level to manage day-to-day activities, including compliance with best practices.

Performance measurements need to be credible to prevent disagreements over numbers that could undermine the value of the process itself.

5.10 APPLICABLE LAWS, REGULATIONS, STANDARDS, AND PRINCIPLES

Organizations have a legal and ethical obligation to comply with the various federal, state, and local laws, regulations, circulars and bulletins, directives and executive orders, government orders, and ordinances pertinent to a specific business area. Noncompliance with these laws and regulations can lead to fines, civil and/or criminal penalties, probation, and jail punishments (prison time), thus creating reputation (image) risk. Compliance with industry and/or organization standards, including professional standards, can increase the quality of products and services, which, in turn, can enhance an organization's reputation and image in the marketplace.

A brief roundup of information about major laws, regulations, and standards is provided here as a reminder for checklist purposes. Note that these laws and regulations are subject to change as new ones are added and existing ones are amended or repealed. The reader is advised to obtain the original laws, regulations, and standards from the official sources for a better understanding of the provisions, requirements, and conditions of the laws, regulations, and standards (www.regulations.gov). Although some of the following laws, regulations, and standards directly affect only the public sector organizations (i.e., government agencies), private-sector organizations can read, learn, and apply them to improve their business operations on a proactive basis.

U.S. organizations should comply with the following laws, regulations, standards, and principles pertinent to manufacturing and service management:

Laws of Agency. The laws regarding agency are concerned with governing the relationship of principals and agents. The purchasing manager or the buyer is typically considered to be a general agent for the buying firm (the principal). That means that a supplier dealing with this manager or buyer has a right to rely on the individual's statements, both in written form and verbally.

Uniform Commercial Code. The U.S. federal purchasing law is composed of three distinct sources:

Written law, which originates in the legislative branch of government
Administrative law, which is derived by the executive branch through the issuance of rules and regulations
Common law, which stems from judicial branch rulings and court decisions

The Uniform Commercial Code (UCC) that is in use today consists of the following ten articles: (1) general introductory provisions, (2) sales of goods and products, (3) transactions in commercial paper, (4) bank deposits and collections, (5) letters of credit, (6) bank transfers, (7) warehouse receipts, bills of lading, and other documents of title to goods, (8) transfers in investment securities, (9) secured transactions, and (10) technical matters.

The most basic elements of Article 2 (sales of goods and products) within the UCC involve the following four issues: warranties, transportation terms and risk of loss, sellers' rights, and buyers' rights.

Foreign Corrupt Practices Act. The U.S. Foreign Corrupt Practices Act (FCPA) of 1977 prohibits payments (such as bribes) that might benefit a foreign official personally. While the law usually pertains to sellers, purchasers should understand its provisions so they can recognize situations addressed by the act.

Motor Carrier Act. The transportation industry has undergone major changes since passage of the Motor Carrier Act of 1980. The Act reduced regulation in the domestic motor carrier industry and resulted in increased industry volatility and expanded price and service options. This environment made the motor carrier industry more competitive and attractive to shippers looking for cost reductions. In response, private-sector organizations began exercising more control over their transportation activities in order to reduce costs and promote efficiencies.

Truth in Negotiations Act. The Truth in Negotiations Act was enacted to put the government on an equal footing with vendors in sole-source negotiations and to provide a basis for ensuring that the government pays reasonable prices when competition is not available. It requires a contractor to provide certified cost or pricing data.

National Environmental Policy Act. The National Environmental Policy Act of 1969 established the U.S. Environmental Protection Agency (EPA) to deal with organizations that create pollution. The mission of the EPA is to protect human health and the environment for a cleaner, healthier environment for the American people. The EPA is responsible for researching and setting national standards for a variety of environmental programs, covering water, air, land, and hazardous substances (www.epa.gov). More than a dozen statutes or laws form the legal basis for the programs of the EPA. Some of these include:

National Environmental Policy Act of 1969
The Clean Air Act of 1970
The Clean Water Act of 1977
The Occupational Safety and Health Act of 1970
The Pollution Prevention Act of 1990
The Toxic Substances Control Act of 1976

In addition to U.S. environmental laws and regulations, organizations can follow international environmental standards (e.g., ISO 14000 series), which are discussed later.

Occupational Safety and Health Act. In 1970, Congress enacted the Occupational Safety and Health Act (OSHA) to ensure a safe and healthful working environment for every worker. The Act established the Occupational Safety and Health Administration to develop standards, conduct inspections, monitor compliance, and institute enforcement actions against those found not in compliance.

Design of Experiments. The design of experiments (DOE) is a branch of applied statistics dealing with planning, conducting, analyzing, and interpreting controlled tests to evaluate the factors that control the value of a parameter or group of parameters. The DOE is used to establish tolerance specifications and to conduct statistically significant tests for products.

Theory of Constraints. Eliyahu M. Goldratt coined the term "theory of constraints" (TOC), which deals with tools and techniques used for identifying and eliminating the constraints (bottlenecks) in a manufacturing process, steps that increase production throughput and employee productivity.

Taguchi Method. Genichi Taguchi of Japan emphasizes reducing variation in the production process and in the final product as the principal way of improving quality. He believes this can be done by designing products that perform in a consistent manner, even under conditions of varying or adverse use. He also believes that one can make this happen at the design stage by appropriate statistical experimental design methods.

Taguchi views quality engineering as composed of three elements: system design, parameter design, and tolerance design. He developed a quality-loss function to measure quality in monetary units that reflect both short-term and long-term losses.

Taguchi's approach to quality is relatively precise. Conventional quality-control activities center on final inspection sampling or on control charts and process control. This is called on-line quality control. Taguchi pushed the process upstream to focus on product and process design. This is called off-line quality control.

Voice of the Customer. "Voice of the customer" (VOC) means organizations should listen to and understand the external customers' needs, wants, and expectations (i.e., customers' voice) and provide products and services that truly meet such needs, wants, and expectations. The same thing applies to internal customers' needs (i.e., departments or functions within an organization).

Quality-Function Deployment. Quality function deployment (QFD) is a structured method in which customer requirements are translated into appropriate technical requirements for each stage of product development and manufacturing. The input to the QFD process is listening to the voice of the customer.

House of Quality. The house of quality (HOQ) is a diagram that clarifies the relationship between customer needs and product features. It helps correlate market or customer requirements and analysis of competitive products with higher-level technical and product characteristics. The diagram makes it possible to bring several factors into a single figure. The diagram is named for its house-shaped appearance but sometimes is referred to as QFD, a sign of the connection between the three approaches of VOC, QFD, and HOQ.

Voice of the Process. "Voice of the process" means understanding and evaluating the nature of process flows, process variations, and process characteristics and capabilities for both products and services. The goal is to reduce process variations in order to make the process stable and predictable and to reduce cycle time.

New work processes must be designed to reduce the cycle time by eliminating stop points, chokepoints, pain points, or fault points in a process that enjoys the support and availability of resources such as tools, technology, people, equipment, and information. Existing work processes must be (1) streamlined by reviewing the upstream and downstream work steps, (2) simplified by removing unnecessary handoffs, stop points, chokepoints, pain points, or fault points, (3) standardized based on "lessons learned," and (4) institutionalized by being rolled out to the entire organization.

Total Quality Management. Total quality management (TQM) is a relatively new approach in business management. It seeks to improve product/service quality and increase customer satisfaction by restructuring traditional management practices. TQM is an endless journey, a striving for perfection in products and services.

Cost of Quality. The cost of quality (COQ) measurement identifies areas for process improvement. The focus of this measurement is to express quality in terms of quantitative and financial language, that is, costs, return on investment, cost of poor quality, cost of rework, and so on.

The COQ definition includes the following three items:

1. COQ is the cost of making a product conform to quality standards (i.e., quality goods).
2. COQ is the cost of not conforming to quality standards (e.g., waste and loss).
3. COQ is a combination of item 1 and 2.

$$\text{COQ} = \text{the cost of conformance (A)} + \text{the cost of nonconformance (B)}$$

where (A) includes cost to prevent and detect a failure and (B) includes cost to correct a failure.

ISO 9000 Standards. ISO 9000 consists of a series of generic standards with appropriate guidelines published by the International Organization for Standardization (called ISO) for vendor certification programs. ISO 9000 addresses quality-system processes, not product performance specifications. In other words, the ISO 9000 covers how products are made but not necessarily how they work. ISO 9000 focuses on processes, not on products or people. It is based on the concept that one will fix the product by fixing the process. The ISO 9000 is a standard to judge the quality of suppliers. It assumes that suppliers have a sound quality system in place and it is being followed. ISO 9000 can be used as a baseline quality system to achieve TQM objectives (www.iso.org).

The standards are becoming an acceptable worldwide approach to vendor certification and international trade. The real push is from companies throughout the world who are requesting that their suppliers become certified. The ISO 9000 standards are equally applicable to manufacturing and service industries, and remove the nontariff barriers that arise from differences and inadequacies among national, local, or company standards. Major categories of nontariff barriers include quantitative import restrictions such as quotas, voluntary export restraints, and price controls.

There are two kinds of standards: (1) product standards dealing with technical specifications and (2) quality standards dealing with management systems. Quality measures for ISO 9000 include leadership, human resources development and management, management of process quality, and customer focus and satisfaction.

ISO 14000 Standard. ISO 14000 is the international standard for environmental management. The scope of the standard includes all efforts to minimize waste and redesign manufacturing processes, products, and packaging to prevent pollution. More attention should be given to pollution prevention rather than correction. To achieve these goals, environmental protection, like quality and safety management, must be integrated into daily business operations (www.iso.org).

ISO 14001 Standard. ISO 14001 is a management framework for planning, developing, and implementing environmental strategies in an organization. The framework includes a policy, a planning process, an organizational structure, specific objectives and targets, specific implementation programs, communications and training programs,

and management review, monitoring, and corrective action, which includes environmental audit. The standard is applicable to any organization regardless of size or business type (www.iso.org).

Lean Manufacturing Practices. The lean manufacturing concept focuses on eliminating waste and enhancing the value of a company's products to its customers. This concept can be applied to all kinds of manufacturing industries and all types of companies, including process industry, high-volume (mass production), and job shop industry.

Lean Service Practices. Lean service practices can be applied to service industries to eliminate waste and enhance value. This requires eliminating non-value-added activities, increasing value-added activities, and streamlining service processes to reduce hold (wait) time and number of handoffs.

Statistical Process Control. Statistical process control (SPC) techniques reduce variation in products and services resulting from deviation from specifications, standards, or targets. Both variable and attribute control charts along with regression analysis and scatter diagrams are used to control the process variations. For example, the control chart distinguishes between natural (common) and unnatural (special) variations. Regression analysis points out the relationships between variables using the scatter diagrams.

Six Sigma Quality. Coined by Motorola Inc. and implemented by many world-class organizations including General Electric (GE) Company, Six Sigma is a highly disciplined process that helps organizations focus on developing and delivering near-perfect products and services.[16] It is a vision of quality, a striving for perfection (www.ge.com).

The phrase "six sigma" is a statistical term that measures how far a given process deviates from perfection. The central idea behind the approach is that if one can measure how many "defects" are found in a process, one can systematically figure out how to eliminate them and get as close to "zero defects" as possible. Defects are sources of customer irritation. Defects are costly to both customers and to manufacturers or service providers. Eliminating defects provides cost improvements. To achieve Six Sigma quality, a process must produce no more than 3.4 defects per million opportunities. An "opportunity" is defined as a chance for nonconformance, which in turn is defined as not meeting required specifications. This means organizations need to be nearly flawless in executing their key processes.

GE uses three approaches and models in implementing its Six Sigma quality initiative:

1. Design for Six Sigma (DFSS). DFSS is a systematic methodology utilizing tools, training, and measurements to enable GE to design products and processes that meet its customer expectations and can be produced at Six Sigma quality levels.
2. Define, Measure, Analyze, Improve, and Control (DMAIC). DMAIC is a process for continued improvement. It is a systematic scientific, and fact-based approach. The closed-loop process eliminates nonproductive steps and activities, often focuses on new measurements, and applies technology for improvement.
3. Critical to Quality (CTQ). CTQ is an element of a process or practice that has a direct impact on the perceived quality of the process or practice.

Just in Time Methods. The just in time (JIT) method is a philosophy of doing business differently to achieve cost, production, and service efficiencies, and to reduce

waste, delays, and problems. JIT can be applied to production, purchasing, inventory, transportation, training, and quality.

Quick Response System. The quick response (QR) system links manufacturers, wholesalers, and retailers in a logistics network by synchronizing product flows with information flows. The goal of the QR system is to achieve greater accuracy of sales demand forecasts and to improve in-stock percentage availability. The QR system, which is for retailers and wholesalers what the JIT method is for manufacturers, reduces inventory investment by scheduling the delivery of parts or raw materials close to production lines. Critical success factors for the effective functioning of the QR system include low cycle times, high service levels, high inventory turns, and high fill rates for product orders.

Mistake-Proofing Concept. Both manufacturing and service operations must be designed with mistake-proofing ("idiotproofing") in mind. The approach uses automatic devices or methods to avoid simple human-made or machine-made errors. It focuses on prediction and detection of errors and defects. The concept is relatively easy and inexpensive to implement. Japanese companies follow this concept very closely (*Poka-yoke*).

Focus Points: Five Ss. Manufacturing management should focus on five "Ss" to keep the factory and its facilities clean looking and efficient in operation. These focus points include Sort, Set in order, Shine, Standardize, and Sustain. Japanese companies follow these five Ss to the letter.

American Production and Inventory Control Society. The American Production and Inventory Control Society (APICS), which is the association for operations management, is a professional organization and the voice of the operations management profession. It establishes professional certifications (CPIM and CSCP), professional standards, and a code of ethics for operations managers to follow. CPIM is Certified in Production and Inventory Management, and CSCP is Certified Supply Chain Professional (www.apics.org).

Institute for Supply Management. The Institute for Supply Management (ISM) is a professional organization and the voice of the supply management profession. It establishes professional certifications (CPM., APP., and CPSM), professional standards, and a code of ethics for supply managers to follow. CPM. is Certified Purchasing Manager, APP is Accredited Purchasing Practitioner, and CPSM is Certified Professional in Supply Management (www.ism.ws).

American Society for Quality. The American Society for Quality (ASQ) is a professional organization and the voice of the quality profession. It establishes professional certifications (e.g., CQE, CQM, and CQA), professional standards, and a code of ethics for quality professionals to follow. CQE is Certified Quality Engineer, CQM is Certified Quality Manager, and CQA is Certified Quality Auditor (www.asq.org).

Generally Accepted Manufacturing Practices. Just as there are generally accepted accounting principles (GAAP) in the accounting profession, there are generally accepted manufacturing practices in production. There are four operations pillars of excellence, including the bill of materials, the route/process sheet, inventory record accuracy, and demonstrated capacity. The first two pillars are linked to material planning, while the last two pillars are linked to capacity planning.[17]

One of the basic concepts of manufacturing is manufacturing lead time, which consists of operation time and interoperation time, with operation time comprising process time, ingredients-mix time, part-fabricating time, part-fastening time, subassembly time, and assembly time, and with interoperation time representing queue time, preparation time, postoperation time, wait time, and transportation time. The goal is to maximize the operation time (i.e., value-added activities) and minimize the interoperation time (i.e., non-value-added activities).

Industry Standards. Each industry has its own standards. For example, the automobile industry, food industry, oil industry, chemical industry, mining industry, pharmaceutical industry, steel industry, insurance industry, and healthcare industry each operates within its own standard operating procedures (SOP) and process and engineering specifications, and each has to comply with its particular rules and regulations These industry standards must be followed to ensure quality of products and services. For example, food industries must comply with United States Department of Agriculture (USDA) standards, pharmaceutical industries must comply with U.S. Food and Drug Administration (FDA) standards, and contractors working with the U.S. Department of Defense (DoD) must comply with the DoD's cost accounting standards when estimating costs during contract bidding. These standards are established by the cost accounting standards board (CASB) of the DoD.

Additional Resources

Blanchard, David. *Supply Chain Management Best Practices*. Hoboken, NJ: John Wiley & Sons, 2007.

Bragg, Steven M. *Inventory Best Practices*. Hoboken, NJ: John Wiley & Sons, 2004.

Correll, James., and Kevin Herbert. *Gaining Control: Managing Capacity and Priorities*, third edition. Hoboken, NJ: John Wiley & Sons, 2006.

Fogli, Lawrence, ed. *Customer Service Delivery: Research and Best Practices*. Hoboken, NJ: John Wiley & Sons, 2006.

Hugos, Michael. *Essentials of Supply Chain Management*, second edition. Hoboken, NJ: John Wiley & Sons, 2006.

Landvater, Darryl. *World-Class Production and Inventory Management*, second edition. Hoboken, NJ: John Wiley & Sons, 1997.

Schonberger, Richard. *Best Practices in Lean Six Sigma Process Improvement*. Hoboken, NJ: John Wiley & Sons, 2007.

Wild, Tony. *Best Practices in Inventory Management*. Hoboken, NJ: John Wiley & Sons, 1997.

Zylstra, Kirk. *Lean Distribution: Applying Lean Manufacturing to Distribution Logistics, and Supply Chain*. Hoboken, NJ: John Wiley & Sons, 2005.

Notes

1. This section is reprinted with permission. Dr. David M. Anderson, *Design for Manufacturability and Concurrent Engineering: How to Design for Low Cost, Design in High Quality, Design for Lean Manufacture, and Design Quickly for Fast Production* (Cambria, CA: CIM Press, 2006).
2. *Id*. This section is reprinted with permission.
3. *Id*. This section is reprinted with permission.
4. *Id*. This section is reprinted with permission.

5. This section is reprinted with permission. David M. Anderson, *Build-to-Order and Mass Customization: The Ultimate Supply Chain Management and Lean Manufacturing Strategy for Low-Cost On-Demand Production without Forecasts or Inventory* (Cambria, CA: CIM Press, 2004).
6. *Id*. This section is reprinted with permission.
7. *Id*. This section is reprinted with permission.
8. *Id*. This section is reprinted with permission.
9. *Id*. This section is reprinted with permission.
10. U.S. General Accounting Office, *Inventory Management: Greater Use of Best Practices Could Reduce DOD's Logistics Costs* (GAO/T-NSIAD-97-214), Washington, DC: July 1997.
11. GAO, *Best Management Practices: Reengineering the Air Force's Logistics System Can Yield Substantial Savings* (GAO/NSIAD-96-5), Washington, DC: February 1996.
12. GAO, *Defense Transportation: Commercial Practices Offer Improvement Opportunities* (GAO/NSIAD-94-26), Washington, DC: Nov. 1993. (U.S. General Accounting Office).
13. GAO, *Partnerships: Customer-Supplier Relationships Can Be Improved through Partnering* (GAO/NSIAD-94-173), Washington, DC: July 1994.
14. GAO, *Customer Service: Human Capital Management at Selected Public and Private Call Centers* (GAO/GGD-00-161), Washington, DC: Aug. 2000. , (U.S. General Accounting Office).
15. GAO, *Best Practices: Taking a Strategic Approach Could Improve DOD's Acquisition of Services* (GAO-02-230), Washington, DC: January 2002.
16. General Electric (GE) Co., "Six Sigma." Excerpted from the GE Web site http://www.ge.com/en/company/companyinfo/quality/quality.htm.
17. Steven A. Melnyk and R. T. Christensen, *Back to Basics: Your Guide to Manufacturing Excellence* (Boca Raton, FL: CRC Press, 2000).

CHAPTER 6

MARKETING- AND SALES-MANAGEMENT BEST PRACTICES

6.1 OVERVIEW

The evolution of marketing moves from production era to sales era to marketing era to relationship era, with the latter taking as its focus managing the supply chain, keeping existing customers, and acquiring new customers. According to the American Marketing Association (AMA), marketing is ultimately an exchange process centered on planning and executing the conception, pricing, promotion, and distribution of ideas, goods, and services to create exchanges that satisfy the goals of individuals and organizations.[1]

Marketing is directed at market segments (i.e., homogeneous groups of customers) that are defined by their product usage wants and needs. As a business strategy, market segmentation allows the company to focus its marketing efforts on narrowly defined markets. Many organizations lack the resources to efficiently and effectively appeal to every segment in a market; therefore, they often choose to focus on specific segments called *target markets*.

The *marketing mix*, composed of product, pricing, distribution (place), and promotion decisions, is tailored to meet the needs and wants of specific target markets and to carve out a position in the marketplace. *Product positioning* refers to how customers perceive a product's position in the marketplace relative to the competition. Ultimately, marketing strategy directs the product positioning of the firm and directs and develops a mix of other marketing activities, processes, and practices that are specifically tailored to effectively and profitably serve the needs of a target market.

6.2 ROLES AND RESPONSIBILITIES OF THE CHIEF MARKETING OFFICER

The Chief Marketing Officer (CMO) is a key person in the C-level executive suite and is in charge of both the marketing and sales functions, with the following roles and responsibilities:

- Integrating marketing and sales activities for maximum synergy, efficiency, and effectiveness
- Lowering marketing and sales costs in order to lower selling prices, increase sales volume, and increase profits
- Linking marketing and sales costs to cash flows and net profits since marketing and sales costs are part of administrative costs, which are subtracted from the operating profits to result in net profits

- Speeding up product and service deliveries to achieve customers' total satisfaction (i.e., faster time-to-market of products and services)
- Innovating new marketing and sales techniques and processes by leveraging technology to improve quality and reduce costs
- Eliminating non-value-added activities in marketing and sales to trim waste and reduce costs
- Focusing more on value-added activities in marketing and sales to provide a solid value to customers and to the organization
- Identifying key drivers of cost, quality, risks, expenses, revenues, profits, business growth, market segments, customer loyalty, competition, and performance. Focus on the root causes of these drivers and understand why these drivers go up and down.
- Seamlessly integrating the back-end systems with the front-end systems for (1) maximum data consistency, completeness, and accuracy, (2) better service and satisfaction of internal and external customers, and (3) stronger connection of disparate and disconnected business processes
- Building standardized, transparent, and repeatable marketing and sales processes to provide the stable, consistent, and quality products and services that customers expect
- Understanding that increases in sales velocity increases inventory velocity, which in turn increases production or service velocity, finance velocity, human capital velocity, and systems velocity. The goal is to synchronize these velocities in a cohesive manner.
- Implementing the goal congruence concept by linking individual employee goals with those of the department/division and the organization. Remove or reduce the competing or conflicting goals.
- Implementing crosscutting best practices across business units, divisions, departments, and functions through busting silos and building bridges
- Linking employee rewards, bonuses, and promotions to employees' true performance and tangible results
- Building solid working relationships with the C-level executives in operations, finance, human resources, and other functions through formal and informal approaches at the workplace
- Fostering ethical values and cultural sensitivity in light of workforce diversity
- Encouraging employees to continuously acquire and improve their knowledge, skills, and abilities (KSAs) through targeted training courses, management development programs, and professional certifications
- Establishing a solid and sustainable Chain of Knowledge linked through the entire management hierarchy to ensure core knowledge competencies for all levels of employees in the organization
- Inviting marketing, sales, distributor, and competitor audits; customer perception audits; special management reviews; and self-assessments periodically and proactively to ensure continuous improvement in marketing and sales of products and services

- Encouraging employees at all levels of the organization to think differently and radically (i.e., out-of-the-box thinking) at all times, which can lead to new perspectives providing best-of-breed solutions.
- Participate in the succession-planning process for key positions.
- Adhering to the code of ethics established by the American Marketing Association for marketers and salespeople (www.marketingpower.com).
- Analyzing outside-in views (i.e., views of stakeholders about company management) and inside-out views (i.e., views of company management about stakeholders) to identify disconnections between these views and to integrate them in a coherent manner.

6.3 WORLD-CLASS MARKETING AND SALES MANAGEMENT

(a) MARKETING AND SALES STRATEGY. World-class marketing and sales organizations have a clear marketing and sales strategy. They strive to satisfy customers with the products and services that customers need and want, meet or beat the competition, and increase revenues, cash flows, and profits for the company. They also integrate marketing and sales functions for maximum synergy, efficiency, and effectiveness.

Critical Success Factors for a World-Class Marketing and Sales Function

Critical success factors for a world-class marketing and sales function include new product development, brand management, customer relations (acquisition, retention, and satisfaction), creation of permanent value to customers and to the organization, efficient logistics operations, listening to stakeholder voices, leadership, organizational culture, customer service, organizational structure, technology, process, and people.

Marketing and sales strategy involves deploying major financial and human capital resources to develop a superior, distinctive, and difficult to imitate competitive advantage that the company can claim as its own, one based on superior product design and technology, a superior distribution system, superior cost structure, and superior brand reputation. The marketing and sales strategy should contain such elements as target markets, product positioning, product/service features and functions, pricing, distribution channels, promotion programs (i.e., marketing mix), and above all customer service.

Specifically, marketing and sales strategy should focus on the following questions:

- Which products and services to create, make, and sell
- Which markets or market segments to serve (e.g., B2C, B2B, and B2G)
- What prices to charge customers
- Which advertising channels to use
- Which distribution channels to use
- What promotion programs to offer
- How much market share to gain
- How to increase revenues, cash flows, and profits
- How to beat or meet the competition
- How to deliver a permanent value to customers through quality products and services

Here, markets include current, new, and adjacent markets, while the customers include current and potential customers. Marketing management should perform Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis on the company's capabilities and characteristics, customer needs and profiles, and competitors' capabilities and characteristics. They should also scan both the internal and external environments.

Marketing management must develop the tools of *marketing communications*, which include personal selling, advertising, public relations, sales promotion, sponsorship and event marketing, and point-of-purchase communications.

A *marketing channel* (also known as a distribution channel or as channel distribution) is the network of organizations that create time, place, and possession utilities for consumers and business users. The goals are to use shorter channel structures, exercise control over the channel members, optimize the length of the channel, use the right channel structure, and use the right type of intermediaries in the channel structure.

Marketing and sales management should focus on the return on sales (ROS) metric and not so much on the return on investment (ROI) metric, the reason being that ROI is a good metric for overall company performance indicator but not such a good metric for the marketing and sales function. Also, note that ROI considers revenues, costs, investments, and profits in its calculation. But marketing and sales management may not have full control over all the costs that go into the ROI calculation. Therefore, marketing and sales management should pay more attention to incremental revenues, incremental costs, incremental cash flows generated from incremental sales, and incremental profits (i.e., contribution margin) from the additional sales, and not so much on raw sales or revenues. Let the senior management pay more attention on the ROI metric and let the marketing and sales management concentrate on improving the ROS metric. However, if marketing and sales management has full control over all the elements that go into the ROI calculation, then ROI should be measured.

(b) LISTENING TO STAKEHOLDER VOICES. Marketing and sales management, as a seller of products and services and revenue generator for the company, should pay close attention in understanding and listening to the following "voices" to achieve organizational goals and to improve overall performance. When these "voices" are heard together, they bring attention to new perspectives and creative conflicts, forcing new thinking that leads to new solutions (i.e., best-of-breed solutions). Listening to the collective voice of many stakeholders at once will have a greater impact than listening to one voice at a time in isolation, because the former requires a balanced approach after considering all party's concerns.

For each content of each voice, a T-Column analysis should be prepared, with "what happens if I listen to this voice" in the left column (benefits) and "what happens if I don't listen to this voice" in the right column (costs and risks). A comparative analysis of each content in each column will point to new problems requiring new solutions.

- Voice of the customer (external customers such as suppliers, vendors, contractors, consultants, key customers, regulators, investors, creditors, the stock market, and media/press, and internal customers such as the board of directors, corporate management, and employees in other functional departments, such as engineering, research and development, manufacturing, finance, human resources, and IT)

- Voice of the process (process flows, process variations, process delays and waste, and process inefficiencies)
- Voice of quality (TQM principles and practices, mistake-proofing, continuous improvement, cost of poor quality, quality assurance, quality control, quality audit, quality council, and quality circles)
- Voice of standards (consumer-credit granting, extension, and reporting standards, packaging and labeling standards, advertising standards, product warranty and recall standards, telemarketing standards, mergers and acquisition standards, ethical standards; and industry/organization standards)
- Voice of partners (advertising agencies; supply chain members; marketing channel members; wholesalers and retailers; licensees and franchisees; product resellers, dealers, and distributors; joint venture and venture capital partners; electronic commerce vendors; and outsourcing vendors)
- Voice of regulators (federal, state, and local laws and regulations)
- Voice of competitors (press releases, Web site pressrooms, industry magazines, daily business newspapers, advertising magazines, industry trade shows, product demonstrations and promotions, direct mail, e-mail campaigns, copyright/trademark/ patent news, business intelligence news, banner advertising, billboard and street advertising, product sponsorships, and online events and chat rooms)

(c) MARKETING AND SALES CYCLE-TIME MEASURES. Cycle time reduction in marketing and sales deals with speeding the time-to-market cycle for new products and services and reducing the order-to-cash cycle time, which produces benefits such as increased cash flows and profits, improved utilization of human and machine resources, decreased costs, and improved customer service. To attain these benefits, organizations must:

- Eliminate or decrease non-value-added activities (e.g., nonselling time for salespeople; customer hassle factors; impersonal selling methods; quotation rework time; customer call hold time; unnecessary handoffs, stop points, chokepoints, pain points, or fault points in the cycle; product recalls; defective product returns that cannot be salvaged; and delays at the interdepartmental and interdivisional boundaries and at the intradepartmental work stations).
- Enhance or increase value-added activities (e.g., customer viewpoints; customer touch points; sales points in terms of selling time with face-to-face meetings with customers; up-selling and cross-selling activities; quote time; marketing proof points; marketing and sales project hold points; product and service price points; bid-to-win ratio, sales close rates, customer rebate points; internal/external customer access points to marketing and sales systems; advertising creative points; customer order-processing time; customer order ship time; customer and competitor focus points; salvageable product returns to recapture value through reverse logistics; and marketing and sales decision points and control points).

This requires having the right products with the right prices available at the right place and at the right time so that delays and waste in marketing and sales operations are decreased.

Some examples of marketing and sales cycle time measures include:

- Percentage decrease in contract cycle time from initiation to completion
- Elapsed time between customer initial order and customer final order. The goal is to reduce the customer frustration and to streamline the internal work order processes.
- Percentage decrease in bid-to-win cycle time
- Percentage decrease in lead-to-quote cycle time
- Percentage decrease in quote-to-order cycle time
- Percentage decrease in order-to-cash cycle time
- Percentage decrease in quote-to-cash cycle time

These cycle times can be decreased with the use of automated workflow systems that handle various activities within the cycle, such as checking customer credit report files, converting sales leads/quotes to real orders, releasing customer orders to production, scheduling product shipments, preparing customer invoices, and collecting receivables from customers.

(d) MARKETING AND SALES METRICS. Marketing's role is to acquire new customers and to retain and support existing customers. Sales' role is to support the new and existing customers. Both the marketing and sales functions must be integrated so that the inside-out perspective (i.e., views of company management) can be balanced with the outside-in perspective (i.e., views of customers and competitors). Marketing and sales management must leverage major marketing and sales drivers (e.g., customers and competitors) by connecting their outcomes to key performance indicators (KPIs) or metrics.

Some examples of KPIs and metrics for marketing and sales include:

- Percentage increase in new-customer acquisition rates
- Percentage increase in current-customer retention rates
- Percentage decrease in current-customer defection rates
- Percentage increase in product line sales and profits
- Percentage increase in market share by product line or category
- Percentage increase in sales per salesperson, per region, or per territory
- Percentage increase in same-store sales for retailers
- Percentage increase in sales per square foot of selling space for retailers
- Percentage increase in revenue (yield management) for capital-intensive services, such as airlines, railroads, hotels, rental car agencies, shipping, and vacation-oriented industries
- Percentage increase in sales close rates
- Number of roadblocks to customer removed (e.g., hassle factors, choke points, pain points, and stop points)
- Percentage increase in overall sales or revenues

(e) MARKETING AND SALES CONTRACT MANAGEMENT. Marketing and sales management handles various sales contracts for its customers, with greater amounts of money involved. Sales contracts increase revenues, which affects the top line of the income statement.

Marketing and sales management, in conjunction with procurement management, also handles supply contracts with vendors and other third parties in the supply chain. Supply contracts increase expenses, which affects the bottom line of the income statement. Both sales and supply contracts require a systematic approach to reduce the overall contract cycle time, which runs from the initiation to the execution. Because the contract amounts are large, the contract time frames are long, and the contracting parties are several, violation of any contract terms and conditions can lead to legal, financial, and compliance risks.

Organizations should do the following to reduce potential risks in the contract management process:

- Involve the corporate legal department in establishing formal contract management policies, processes, procedures, and standards. This should cover items such as contract language; terms and conditions; clauses and provisions; and fees, penalties, and incentives.
- Ensure that no contract is mailed or signed until the legal department reviews and approves it.
- Hold the contract data in a centralized database for data consistency, completeness, accuracy, and quality.
- Automate repeatable tasks and eliminate redundant tasks in the contract management process to gain efficiency.
- Integrate the disparate and disconnected work processes involved in contract management.
- Provide legal training to business managers in contract management, explaining the risks involved in contract negotiations, contract adoption, and noncompliance with the contract.

(f) MARKET RESEARCH PROCESS

(i) Market Segmentation. One of the major uses of market research is to segment markets. Market segmentation is a powerful and well-developed marketing tool. A properly segmented market can improve marketing, distribution (logistics), and manufacturing efficiency, and generate additional profits and/or market share. Market segmentation research, especially baseline segmentation research, must be carefully planned and executed. Having a mis-segmented market is often worse than making the mass-market assumption. Foreign firms often enter a domestic market by segmenting the market, uncovering an underserved niche market, and then concentrating their marketing and financial resources on that niche market.

Broadly speaking, there are two methods for segmenting a market: a priori method and post hoc method. The priori segmentation method breaks out customer groups by a generally accepted classification procedure related to variations in customer purchases or in usage of the product category. Examples of the priori method include standard industrial classification (SIC) groups, geographic regions or sales territories, and basic demographic groups. The post hoc segmentation method is empirically derived based on the results of a research study undertaken for the specific purpose of segmenting a market. Aggregating buyers who respond similarly to a set of baseline questions forms the segments defined by such a study. Examples of the post hoc method include product

attribute preferences, product purchase patterns, product usage patterns, brand preferences and loyalty, price sensitivity, and customer values and benefits.

Recent developments in market segmentation methods include multidimensional segmentation, artificial neural networks, latent class models (mixture models), fuzzy and overlapping clustering, and occasion-based segmentation.

Organizations should not use the market segment research under the following circumstances:

- The product category is a pure commodity without significant differentiation in product attributes or product/service bundles.
- The market is so small that marketing to a portion of it is not profitable.
- A relatively few heavy users make up such a very large portion of the sales volume that they are the only relevant target set.
- A single brand is the dominant brand in the market, and therefore, all users are the relevant target set.[2]

(ii) Survey Research. Organizations rely on survey research to learn much-needed business intelligence. Survey results can help understand customer preferences about a particular product, gauge employee satisfaction, identify market opportunities, and much more. Areas that can benefit from survey research include customer acquisition, customer retention, customer/employee complaint tracking, customer/employee profiles, and customer/employee satisfaction measurements.

Survey research can be divided into seven steps, and problems at any step can lead to incorrect results.

Step 1: Survey planning and design
Step 2: Data collection
Step 3: Data access
Step 4: Data preparation and management
Step 5: Data analysis
Step 6: Reporting
Step 7: Deployment

Survey research is much more than simply asking someone a few questions. In order to obtain reliable results from the survey research, one must be able to plan the survey research project, collect data, access and manage the data easily, and report relevant results. The final step is to share the survey results with the decision makers who can act upon them.[3]

(g) MEASURING ADVERTISING EFFECTIVENESS Advertising, like markets, can be segmented. In this case the categories are television (TV) spot commercials, print ads, radio ads, outdoor (billboards) ads, company Web site banner ads, e-mail, and direct mail. It is safe to say that there is no general consensus, on the part of advertisers or advertising researchers, as to the best way to test advertising or measure its effectiveness.

Most advertising testing is done for television spot commercials because they are the most expensive form of advertising to produce. Print ads are also frequently tested, though not as often. More rarely, radio ads, outdoor (billboards) ads, and even Web site

banner ads will be tested too. Direct mail is tested, but by small-batch mailings where the evaluation is based on direct response measures. The same can be done with Web site banner ads that have a click-through response feature.

In order to test an ad, one has to create a stimulus to expose to respondents. The validity and accuracy of their responses is only as good as the stimulus. Clearly the most valid stimulus is the advertising in its final, finished form. For simple print ads, this is not much of a problem. For expensive TV spot commercials, however, waiting to test the ad until after it has been produced largely defeats the purpose of doing ad testing in the first place.

In order, from roughest to most finished form, the following are the recommended types of stimuli one might want to use for testing the TV spot commercial: Storyboards (hand-drawn ideas), Roughs (prototypes), and Finished ads (what consumers see). It is rare that ad testing is done with the finished ads first, due to the heavy costs involved.[4]

(h) CUSTOMER ACQUISITION, RETENTION, AND LOYALTY Leading organizations invest huge amounts of money in acquiring to new customers and retaining them, yet customer defection is normal, which is puzzling to marketing and sales management. Acquiring and retaining customers is associated with cash flows—acquiring new customers is tied to short-term cash flows, and retaining customers is tied to long-term cash flows. Marketing experts say that if customers are not coming to the company, the company should go to customers.

A possible solution to the customer puzzle is to develop a one-to-one business relationship with customers by using a customer-centric approach instead of a product-centric approach. Another solution is to understand what makes a customer a loyal customer. These two solutions are based on the business theme that building long-term, loyal relationships with customers is the key to profitability and growth.

(i) Customer Relationship Management System. Marketing departments are acquiring or developing a customer relationship management (CRM) computer application system to survive in the customer-centric environment and to establish a one-to-one business relationship with customers. Some define CRM as a call center solution. Some view it as sales force automation, others as direct mail, marketing automation, or simply a Web page. Many companies see it as a front-end application only, interacting at the point of contact or point of purchase, or providing customer support. Others believe the secret to CRM success is in tackling back-end activities, such as data mining, data warehousing, data distribution, and data sharing. A properly designed and implemented CRM system encompasses all of these and much more. It is better to view the CRM system as a bridge system, not as a front-end system or back-end system.

Organizations must do the following to derive benefits from the CRM system:

- Understand that customers come first, products and services come next.
- Understand the customer cycle as “get, keep, grow” or “acquire, support, retain.”
- Understand that customers “pull” the company’s products or services of their choice.
- Understand that marketers “push” company’s products or services on to customers.

- Understand that pull and push concepts must be linked together to create interactive, learning relationships between the company and its customers. This linkage, in turn, results in increasing customer satisfaction and loyalty, share of customer, ROS, and ROI.
- Establish a strong linkage between the CRM system and financial performance such as ROS and ROI.

Organizations must avoid the following if they want to acquire and retain customers:

- Developing a product-centric approach in an effort to gain market share or share of customer
- Developing disparate and disconnected database systems to capture vital customer data at various processes such as shipping, billing, sales, and customer-service access points
- Developing products and services first, looking for customers next[5]

(ii) Customer Loyalty. A loyal customer:

- Makes regular repeat purchases
- Purchases across product and service lines
- Refers other customers
- Demonstrates immunity to the pull of the competition
- Tolerates an occasional lapse in the company's support without defecting, owing to the goodwill established through regular, consistent service and provision of value

There is a common denominator that runs through all these behaviors and helps explain why loyalty and profitability are so inextricably linked: each behavior, either directly or indirectly, contributes to sales and profitability. The financial rewards of loyalty run deep.

The best approach to building loyal customers is to ensure that all marketing and sales plans and programs are built around the tried-and-true principles of loyalty. Consider these 12 principles of loyalty:

Principle 1: Build the organization's staff loyalty by reducing employee turnover to establish strong customer relationships and familiarity.

Principle 2: Practice the 80/20 rule (i.e., Pareto principle) by knowing that 80% of revenues come from 20% of customers.

Principle 3: Know the customer loyalty stages: suspect, prospect, first-time customer, repeat customer, client, and advocate.

Principle 4: Serve first, sell second, striving to earn the customer's business with service that is pleasant, productive, and personalized.

Principle 5: Aggressively seek out customer complaints by watching especially for negative behaviors such as unpaid invoices, lack of basic courtesy to the frontline service representatives, and bad publicity through negative word of mouth.

Principle 6: Get and stay responsive to increase the customer's perception of good service.

Principle 7: Know the customer's definition of value by conducting customer loyalty research to understand loyalty drivers.

Principle 8: Win back lost customers by segmenting the defected customers and by developing action plans to recapture those high-value customers who defected.

Principle 9: Use multiple channels to serve the same customers well by internally coordinating sales and service across multiple channels at all customer access points.

Principle 10: Give frontline employees the skills to perform by converging call centers that bring together multichannel access points (e.g., phone, facsimile, e-mail, and Web site). Provide tools such as online knowledge base systems, help agents, workload balancing, and training. Track employee performance.

Principle 11: Collaborate with channel partners by establishing solid supply-chain relationships.

Principle 12: Store the customer data in a centralized database by bringing data from disparate and disconnected databases established for shipping, billing, sales, and customer service. The centralized data can be useful for data-mining purposes.[6]

WHO ARE MY LOYAL CUSTOMERS?

- Most organizations believe in the business theme of ''customers are always right'' while others do not believe in it.
- Some organizations segment their customers into two groups: high yielding and high risk and low yielding and low risk. They pay more attention to high yielding customers and less attention to low yielding customers.
- Are low yielding customers not loyal, not profitable, and not right?
- It seems that there is a tradeoff here between risk and return.

6.4 PRODUCT MARKETING BEST PRACTICES

(a) OVERVIEW. Products are the major focus of every product-oriented organization. In general, products can be classified as consumer, business, or government, depending on who the buyer is (i.e., B2C, B2B, and B2G, respectively) and for what purpose the product is being bought. The goal is to provide the right mix of products at the right time to the right customers at the right place.

(b) NEW-PRODUCT DEVELOPMENT. New products are the lifeblood of many organizations. The goal of the research and development (R&D) function is to create and develop the right products in the right way and deliver at the right time to the right customers at the right place. This is a difficult goal to accomplish, as it requires the cooperation and coordination of R&D, engineering, manufacturing, logistics, marketing, and sales management to improve existing products and create new products. A cross-functional team—at a minimum representing the R&D, engineering, manufacturing, finance, marketing, and sales functions—is needed to analyze customer needs,

competition, and production issues, and to develop strategies, policies, and procedures to deliver a value-based product to customers.

Organizations should do the following to ensure success in new-product development efforts:

- Invest in long-term new products that are sustainable and that facilitate business growth in terms of increased revenues and profits.
- Develop new products to satisfy customers' unmet needs and problems by talking to them (i.e., voice of the customer, VOC).
- Establish a customer advisory board (CAB) to connect the VOC to the company's products and services.
- Conduct a customer perception audit that includes both happy and unhappy customers to improve product/service management, marketing, and sales efforts. The goal is to obtain honest feedback from customers so a link can be made between the audit results and the VOC.
- Develop a competitively advantaged product to demonstrate superior performance in terms of percentage of sales from new products, success rates, and meeting sales and profit objectives.
- Establish a formal product development process consisting of well-defined stages (phases) and each stage's associated tasks and activities. The goal is to reduce the new-product development cycle time.
- Establish a new-product manager, a new-product executive, and a new-product steering committee to create the right environment and to foster top management support. Periodic status reports are needed to monitor progress, establish priorities, and review performance targets.
- Prior to the commercialization and launch stage of new products, marketing management must make decisions about branding, packaging, and labeling to reinforce a product's competitive position in the minds of consumers.
- Develop specific strategies for managing new products as they move through their life cycle stages, such as introduction, growth, maturity, and decline.
- Link R&D, marketing, and sales activities to cash flows and profits and not so much to revenues and sales volume.
- Develop and monitor the following metrics for new-product development:
    - Number of times a new-product test marketing target date was met
    - Number of times a new-product revenue or sales target was met
    - Number of times a new-product cost target was met
    - Number of times a new-product quality target was met
    - Number of times new-product features, functions, and performance targets were met
    - Number of times a new-product time-to-market target date was met

(c) BRAND MANAGEMENT. The scope of brand management is changing from the traditional view that brand building is a marketing function to the new view that it is spread throughout an organization's several functions (e.g., call centers, distribution channels, billing, and customer service). All the touch points that a customer goes through with a company's products, services, and functions must work together regarding the message, care, quality, and service that a customer receives. Any disconnects between these diverse functions can make the customer unhappy and less likely to return.

What is needed is a holistic, whole-company approach to brand building that considers the collective perceptions of key stakeholders (e.g., customers, suppliers, investors, employees, distributors, and channel intermediaries). The traditional approach has focused on the marketing function at the expense of a company's other functions. When branding is done correctly, it creates a powerful and coherent identity that customers come to rely on and that the company can leverage to its competitive advantage.

Organizations must do the following to build a strong branding image:

- Craft the brand identity first by senior management. This may take the form of describing the customer value proposition and by taking an outside-in approach (i.e., views of a customer about a company).
- Analyze all the touch points where a customer comes in contact with the company's products, services, or functions. The contact can be either direct or indirect. The touch points revolve around topics, issues, products, and services.
- Remove all unnecessary handoffs and delays at the touch points.
- Obtain continuous feedback from customers so the brand continues to evolve and to anticipate customers' needs.[7]

(d) PRICING STRATEGIES AND METHODS. Price is a monetary value charged by an organization for the sales of its products and services to customers. Pricing strategies include setting a base price for a product or service and making adjustments to the base price over time.

Two basic costing methods are commonly used: cost-based pricing and demand-based pricing. Managers' use cost as a dominant consideration in pricing decisions and the cost-based pricing includes standard markup and target return pricing approaches. The demand-based pricing determines the relationship between price and sales (demand) using an economic analysis, such as break-even analysis, marginal revenue, and marginal cost concepts.

Organizations must do the following in setting prices for their products and services:

- Understand that the cost-based pricing method is the natural and simple way for companies to set base prices but that sometimes it is the wrong way to do so because production and other inefficiencies result in additional costs, which are added to the cost base. This method ignores the customer side of the equation in pricing and does not make sense to customers.
- Consider the demand-based pricing method, as customers find it natural and understandable.
- Understand that marketers may offer different prices to different buyers or different market segments, based on the company's objectives and in response to competitive price moves. Be aware of the U.S. federal laws and regulations such as the Robinson-Patman Act and the Clayton Act, which place constraints on manufacturers' ability to charge business customers different prices.
- Realize that temporary price reductions may work well in the short term but not in the long term due to quick customer switch-over, which is not sustainable.
- Realize that offering rewards and incentives to entice customers to buy company products and services may not create long-term loyal customers.

- Recognize that price is not the only factor customers consider when making purchase decisions; benefits, value, and convenience are very important considerations.

Organizations must not do the following in setting prices for their products and services:

- Price flexing, price shading, discounts, allowances, promotions, coupons, and rebates, unless and until they have been reviewed and approved by the corporate legal department. They present legal and financial risks that must be examined.

6.5 SERVICE-MARKETING BEST PRACTICES

(a) TRADITIONAL SERVICES. The global economy, especially the U.S. economy, is becoming more service-oriented. Some manufacturing organizations are strictly product-oriented whereas some service organizations are purely service-oriented. On the other hand, there are some manufacturing and service organizations that are both product- and service-oriented. The major issue in service marketing is controlling costs, especially service people costs (i.e., wages and salaries, employee benefits, and employee travel-related costs). The challenging goal is to reduce the overall service costs while improving the service quality and customer response.

Organizations should do the following to reduce service costs and to improve service quality and customer response:

- Establish a self-service strategy at the call center or at the contact center using the Internet, voice response systems, and other tools to increase customer retention rates and customer satisfaction rates, and to reduce the total cost of customer support. Major benefits include improvements in the first-call closure or resolution rate.
- Implement field-service-technician scheduling and routing technologies to meet promised response times and service level agreement (SLA) requirements, and to increase service profitability. The goal is to dispatch the right technician to the right place at the right time with the right part(s) available.
- Design presales and postsales service operations as a strategic profit center, not as a tactical cost center, so that operations managers are responsible for both revenues and costs. The resulting benefits include increased customer value and improved financial performance and service quality.
- Reduce the necessity to dispatch service technicians by implementing knowledge-based tools and self-diagnostic systems to resolve customer issues and problems earlier, faster, and better.
- Strive to make the customer experience with the company easier, pleasant, and profitable to both parties.
- Implement kiosk stations where needed to provide self-help or self-service for customers in order to reduce operating costs (i.e., people costs) resulting from automation efforts.
- Improve part fill rates for better service by reducing part stockouts.
- Improve first-time problem fix rates by increasing the service technicians' productivity rates and skill sets through training and supervision, combined with incentives or punishments.

- Automate repeatable tasks and eliminate redundant tasks in the entire service chain.
- Align information flow with process flow for better results in the service chain.
- Integrate disparate and disconnected work processes in the service chain.
- Understand that customer "touch points" are important to demonstrate how a company interacts with its customers from the beginning to the end of their experience cycle with the company.
- Analyze all the tasks or activities before and after the "touch points" to remove roadblocks and stop points in the cycle.
- Enhance the value of "touch points" for maximum customer retention and satisfaction.
- Customer defection rates are a good metric to watch for and improve. Uncomfortable or unpleasant touch points, stop points, hassle factors, and pain points can lead to customer defection.
- Implement data-mining tools to analyze customer behavior, attitude, and purchasing habits to improve service to customers. These results may explain the reasons for customer defection rates and may help in building strategies and plans to win back the lost customers.
- Reduce the order-processing time, order assembly time, and order delivery time. The goal is to reduce the average order cycle time and to reduce the order cycle time variability.
- Increase accuracy in filling customer orders.
- Reduce the billing-processing time and errors.
- Increase claims processing time and response time to customers.
- Understand that output of the logistics system is customer service. There is a tradeoff between higher costs and higher service levels.
- Remove all customer hassle factors in the service chain.
- Minimize service gaps, standards gaps, delivery gaps, communications gaps, and knowledge gaps in the overall service chain.

(b) INTERNET-BASED MARKETING. The terms "Internet marketing," "Web-based marketing," and "interactive marketing" refer to use of the Internet and related technologies to achieve marketing goals and objectives. There are two ways to view Internet marketing. The first is to look at Internet-based marketing as a way to provide added value to stakeholders such as customers, suppliers, investors, and the media. The second perspective focuses on using the Internet to develop marketing strategies and tactics outside of a company's Web site. The goal of these programs often is to drive traffic to the company Web site, but the execution is through external means such as banner advertising, sponsorships, and e-mail campaigns. Often these tactics are part of an overall branding strategy.

Many traditional elements of marketing easily translate into Internet marketing, such as price, product, place, and promotion. For example, consider the following with respect to "promotion" tactics:

Traditional Marketing	Internet Marketing
Broadcast advertising	Banner advertising
Direct mail	E-mail
Press releases	Web site pressroom

Promotions	Online events
Networking	Chat rooms/Listserv
Word of mouth	Viral marketing

Like traditional marketing, successful online and Internet marketing requires persistence and commitment to a long-term strategy. Unfortunately, even with innovative technology, Internet marketing cannot be done with the click of a mouse. If the goal of Internet marketing is building stronger relationships between the customer and the brand, one should not neglect the power of a Web-based plan.

Companies are realizing that Web-based techniques and strategies must be approached like any traditional marketing activity. Fundamental questions must still be answered:

- Who are our customers?
- What is the competition doing?
- What are the channel dynamics?
- Which marketing-mix strategies are most effective?
- Are our business models realistic?
- How and when we will make a return on investment?[8]

6.6 SALES-MANAGEMENT BEST PRACTICES

World-class sales management focuses on two major things: lead management cycle and managing the sales process, because the former feeds the latter.

(a) LEAD MANAGEMENT CYCLE. Lead management is the process of rapidly and effectively creating, nurturing, distributing, and analyzing leads. The ultimate goal is to increase the likelihood that a lead will convert to a qualified sale opportunity and then a new, satisfied customer.

To implement a lead management strategy, marketing and sales functions must work closely together. The key focus here is on the quality of leads, not quantity of leads. Marketing and sales management should focus on the conversion rates of leads to sales (i.e., percentage of leads resulted in closed sales), not so much on the number of raw leads generated.

For best results, a lead management system must bring together the right people, processes, and information at various stages in the lead management cycle. Successful implementers should:

- Identify hot leads and automatically route them to direct-sales or channel partners.
- Actively engage the remaining leads (i.e., not-so hot leads) and nurture them through the pipeline to eventual sale.
- Track all leads to closure and evaluate the ROS and ROI of marketing campaigns.
- Integrate the external channels, including value added resellers (VARs), other resellers, and strategic partners.
- Integrate off-line qualification resources such as call centers.

Organizations should do the following to manage the lead management cycle:

- Plan and generate leads.
- Qualify leads.

- Distribute leads.
- Nurture leads.
- Measure and evaluate leads.[9]

(b) MANAGING THE SALES PROCESS. The sales process consists of eight basic steps or stages: (1) prospecting, (2) preapproach and planning, (3) approaching the client, (4) identifying the client's needs, (5) presenting the product to the client, (6) handling buyer objections, (7) gaining commitment from the buyer, and (8) following up and keeping promises.[10]

Salespeople use either the traditional selling method or the professional selling method, where the latter method is better. Each selling method is described next:

In the traditional selling method, little time is spent on the early stages of the sales process (i.e., stages 3 and 4) and no time is spent on stages 1 and 2. Consequently, the prospective buyer is not usually convinced that he really needs the product, so gaining commitment from the buyer is difficult, tedious, and time-consuming.

In the professional selling method, a great deal of time is spent in the early stages of the sales process (i.e., stages 1, 2, 3, and 4), so that commitment is gained as a very natural or logical, next step. Essentially, customers are convinced that the product will solve their problems, or meet their need, because early in the sales process care has been taken to establish that need and link it to the benefits of the product.

Organizations should do the following to fulfill the defined roles and responsibilities of the marketing and sales management:

- Understand that marketing management finds the sales leads and that sales management converts the discovered leads into real sales and supports existing and new customers alike. Automate the lead management process as much as possible to increase efficiency and effectiveness.
- Understand that sales leads are the "touch points" between marketing and sales functions.
- Understand that sales management focuses on short-term results while marketing management focuses on long-term results. Both functions must coexist in harmony and consistency.
- Salespeople should increase the face-to-face time with their customers, and spend not so much time on phone calls, e-mails, voice mails, facsimiles, and Web sites. The key is to increase the number of "touch points" between the salesperson and the customer as they establish a solid business relationship.
- Salespeople should increase the selling time and decrease the nonselling time with the customers because the former is a value-added activity whereas the latter is a non-value-added activity.
- Sales management should remove "pain points" and "hassle factors" that customers experience when dealing with a company and focus on increasing both up-selling and cross-selling activities with customers.
- Building a one-to-one business relationship with the customer is an example of a "guided-selling" process.
- Marketing should develop product usage scenarios, and sales staff should receive training on product usage.
- Marketing and sales must work together to develop sales campaigns for pushing a product.

- Marketing should develop "proof points" to convince a potential customer and give them to sales staff. This includes providing customer success stories, press releases, customer testimonials, product demonstrations, and focused presentations.
- Implement sales force automation technologies to increase the overall effectiveness of salespeople by reducing the sales cycle time, by completing all sales calls on time, and by speeding the resolution of customer inquiries. This requires that customer data be available to the entire sales staff in a real-time mode.

6.7 APPLICABLE LAWS, REGULATIONS, STANDARDS, AND PRINCIPLES

Organizations have a legal and ethical obligation to comply with the various federal, state, and local laws, regulations, circulars and bulletins, directives and executive orders, government orders, and ordinances pertinent to a specific business area. Noncompliance with these laws and regulations can lead to fines, civil and/or criminal penalties, probation, and jail punishments (prison time), thus creating reputation (image) risk. Compliance with industry and/or organization standards, including professional standards, can increase the quality of products and services, which, in turn, can enhance an organization's reputation and image in the marketplace. Adherence to generally accepted business principles and practices could have a similar effect as complying with standards.

A brief roundup of information about major laws, regulations, and standards is provided here as a reminder for checklist purpose. Note that these laws and regulations are subject to change as new ones are added and existing ones are amended or repealed. The reader is advised to obtain the original laws, regulations, and standards from the official sources for a better understanding of the provisions, requirements, and conditions of the laws, regulations, and standards (www.regulations.gov). Although some of the following laws, regulations, and standards directly affect public sector organizations (i.e., government agencies), private-sector organizations can read, learn, and apply them to improve their business operations on a proactive basis.

U.S. organizations should comply with the following laws, regulations, standards, and principles pertinent to marketing and sales management:

Federal Consumer Credit Protection Act. In 1968, in response to concerns about abuses in consumer credit transactions, including misleading credit disclosures, unfair marketing practices, and oppressive collection methods, the U.S. Congress passed the Federal Consumer Credit Protection Act, which requires creditors to disclose finance charges (including interest and other charges) and credit extension charges, and sets limits on garnishment proceedings.

Equal Credit Opportunity Act. The Equal Credit Opportunity Act, enacted by the U.S. Congress in 1974, prohibits all businesses that regularly extend credit from discriminating against any credit applicant on the basis of gender, marital status, race, color, religion, national origin, or age.

Fair Packaging and Labeling Act. The Fair Packaging and Labeling Act of 1967 requires certain information be listed on all labels and packages, including product identification, manufacturer or distributor mailing address, and the quantity of contents.

Foreign Corrupt Practices Act. In 1977, the U.S. Congress enacted the Foreign Corrupt Practices Act (FCPA) and amended it in 1988. The FCPA prohibits all U.S. domestic concerns from bribing foreign governmental or political officials to obtain business or licenses in foreign countries.

Sherman Antitrust Act. The Sherman Antitrust Act of 1890 prohibits actions that are "in constraint of trade" or actions that attempt to monopolize a market or create a monopoly. Legal actions under this act typically involve price fixing or other forms of collusion among sellers. However, the law also prohibits reciprocity or reciprocal purchase agreements.

Clayton Antitrust Act. The Clayton Antitrust Act of 1914 makes price discrimination illegal and prohibits sellers from exclusive arrangements with purchasers and/or product distributors. The Clayton Act strengthens the Sherman Act by restricting such practices as price discrimination, exclusive dealing, tying contracts, and interlocking boards of directors where the practices' effect may be to substantially lessen competition or tend to create a monopoly.

Celler-Kefauver Antimerger Act. The Celler-Kefauver Antimerger Act of 1950 amended the Clayton Act to include major asset purchases that decrease competition in an industry.

Miller-Tydings Resale Price Maintenance Act. The Miller-Tydings Resale Price Maintenance Act of 1937 exempts the interstate fair trade contracts from compliance with antitrust requirements.

Robinson-Patman Act. The Robinson-Patman Act of 1936 further addresses the issue of price discrimination established in the Clayton Act. It prohibits sellers from offering a discriminatory price where the effect of discrimination may limit competition or create a monopoly. There is also a provision that prohibits purchasers from inducing a discriminatory price. While a seller may legally lower price as a concession during negotiations, the purchaser should not mislead or trick the seller, which would result in a price that is discriminatory to other buyers in the market.

Federal Trade Commission Act. The Federal Trade Commission Act of 1914 authorizes the Federal Trade Commission (FTC) to interpret trade legislation, including the provisions of the Sherman Antitrust Act that deal with restraint of trade. The Act also addresses unfair competition and unfair or deceptive trade practices.

Wheeler-Lea Act. The Wheeler-Lea Act of 1938 amended the FTC Act to further outlaw unfair practices and give the FTC jurisdiction over false and misleading advertising.

Consumer Product Safety Act. The U.S. Consumer Product Safety Commission was created by the Consumer Product Safety Act of 1972 as an independent agency responsible for protecting the public from unreasonable risks of injury and death associated with consumer products. The Commission specifies safety standards for consumer products. The Act has jurisdiction over many consumer products used in and around the home, in schools, and in recreation. The Act requires U.S. manufacturers of consumer products to report information about settled or adjudicated lawsuits and product recalls.

Magnuson-Moss Warranty Act. The Magnuson-Mass Warranty Act of 1975 governs consumer product warranties. The Act requires manufacturers and sellers of consumer products to provide consumers with detailed information about warranty coverage. In addition, it affects both the rights of consumers and the obligations of warrantors under written warranties.

Fair Credit Reporting Act. The Fair Credit Reporting Act (FCRA) was passed to establish safeguards for the reporting of information on consumers and to ensure

that the information being reported was confidential, accurate, relevant, and properly utilized.

Gramm-Leach-Bliley Act. The Gramm-Leach-Bliley Act (GLBA), in conjunction with the FCRA, regulates the manner in which consumer credit information can be shared by financial institutions with affiliates and third parties. Sharing of this information with nonaffiliates is subject to the notice and opt-out provisions of the GLBA.

Health Insurance Portability and Accountability Act. The Health Insurance Portability and Accountability Act (HIPAA) requires an individual's written authorization before a disclosure of his protected health information is made available for marketing purposes. The same is required for use of health information.

CAN-SPAM Act. The U.S. Congress passed the CAN-SPAM Act in 2003 to regulate the amount of unsolicited commercial e-mails. The Act, which applies to marketers using e-mail as a marketing medium, prohibits false or misleading subject lines and requires that "from" lines identify the message "initiator."

National Do-Not-Call Registry. In 2004, the Federal Trade Commission (FTC), the Federal Communications Commission (FCC), and state Attorneys General established the National Do-Not-Call Registry. Telemarketers using telephone solicitations must comply with the intent of this law to reduce legal risks.

Marketing Promotions, Trademarks, Copyrights, and Advertising. Marketers must respect the promotion laws (dealing with sweepstakes, games of chance, and skill contests), trademark laws, copyright laws, and advertising laws (dealing with free offers, discount offers, television ads, radio and print ads, solicitation letters, facsimiles, telemarketing, e-mail, direct mail, T-shirts, viral marketing campaigns, and Web sites). Viral marketing campaigns deal with the following types of messages: (1) forward-to-a-friend, (2) incentivized viral, (3) stealth, and (4) buzz or word-of-mouth. Various federal, state, and local laws and regulations govern these areas. Both FTC and FCC are actively enforcing the federal laws and regulations.

Voice of the Customer. "Voice of the customer" (VOC) means organizations should listen to and understand the external customers' needs, wants, and expectations (i.e., customers' voice), and provide products and services that truly meet such needs, wants, and expectations. The same thing applies to internal customers' needs (i.e., departments or functions within an organization).

Voice of the Process. "Voice of the process" means understanding and evaluating the nature of process flows, process variations, and process characteristics and capabilities for both products and services. The goal is to reduce process variations in order to make the process stable and predictable and to reduce cycle time.

New work processes must be designed to reduce the cycle time by eliminating stop points, chokepoints, pain points, or fault points in a process that enjoys the support and availability of resources such as tools, technology, people, equipment, and information. Existing work processes must be (1) streamlined by reviewing the upstream and downstream work steps, (2) simplified by removing unnecessary handoffs, stop points, chokepoints, pain points, or fault points, (3) standardized based on "lessons learned," (4) institutionalized by being rolled out to the entire organization.

American Marketing Association. The American Marketing Association (AMA) is a professional organization and the voice of marketers and salespeople. It establishes

professional certification (Professional Certified Marketer, PCM), professional standards, and a code of ethics for marketers and salespeople to follow. (www.ama.org).

Additional Resources

LeSueur, Jeff. *Marketing Automation: Practical Steps to More Effective Direct Marketing*. Hoboken, NJ: John Wiley & Sons, 2007.

Peppers, Don, and Martha Rogers. *Managing Customer Relationships: A Strategic Framework*. Hoboken, NJ: John Wiley & Sons, 2004.

Young, Roy A., Allen M. Weiss, and David W. Stewart. *Marketing Champions: Practical Strategies for Improving Marketing's Power, Influence, and Business Impact*. Hoboken, NJ: John Wiley & Sons, 2006.

Notes

1. *CBM Exam Preparation Guide*, vol. 1, 589–592. Original material was taken into the *CBM Guide* from *Marketing: Best Practices*, Hoffman et al, Thomson Learning, Second edition., 2003, South-Western, a division of Thomson Learning.
2. Portions of this section have been adapted with permission from MarketingPower.com. For more information about market segmentation, refer to "Principles of Market Segmentation" by William D. Neal, *Best Practices in Marketing*, American Marketing Association (AMA), http://www.marketingpower.com.
3. Portions of this section have been adapted with permission from MarketingPower.com. For more information about survey research, refer to "Seven Stages of Effective Survey Research" by Dan Meir, *Best Practices in Marketing*, American Marketing Association (AMA), http://www.marketingpower.com. Copyright 2002 by MarketingPower.com Inc.
4. Portions of this section have been adapted with permission from MarketingPower.com. For more information about measuring advertising effectiveness, refer to "Principles of Measuring Advertising Effectiveness" by David Olson, *Best Practices in Marketing*, American Marketing Association (AMA), http://www.marketingpower.com. Copyright 2001 by MarketingPower.com Inc.
5. Portions of this section have been adapted with permission from MarketingPower.com. For more information about CRM system, refer to "CRM Overview" by Christopher Helm, *Best Practices in Marketing*, American Marketing Association (AMA), http://www.marketing power.com. Copyright 2002 by MarketingPower.com Inc.
6. Portions of this section have been adapted with permission from MarketingPower.com. For more information about customer loyalty, refer to "Twelve Laws of Loyalty" by Jill Griffin, *Best Practices in Marketing*, American Marketing Association (AMA), http://www.marketing power.com. Copyright 2004 by MarketingPower.com Inc.
7. Portions of this section have been adapted with permission from MarketingPower.com. For more information about brand management, refer to "Branding Overview" by Michael Dunn, *Best Practices in Marketing*, American Marketing Association (AMA), http://www.marketing power.com. Copyright 2001 by MarketingPower.com Inc.
8. Portions of this section have been adapted with permission from MarketingPower.com. For more information about Internet-based marketing, refer to "Internet Marketing Overview" by Toby Bloomberg, *Best Practices in Marketing*, American Marketing Association (AMA), http://www. marketingpower.com. Copyright 2001 by MarketingPower.com Inc.
9. Portions of this section have been adapted with permission from MarketingPower.com. For more information about lead management, refer to "Best Practices in Lead Management" by Alexandra Best, *Best Practices in Marketing*, American Marketing Association (AMA), http://www.marketingpower.com. Copyright 2003 by MarketingPower.com Inc.
10. *CBM Exam Preparation Guide*, vol. 1, 775. Original material was taken into the *CBM Guide* from *Marketing: Best Practices*, Hoffman et al, Thomson Learning, Second Edition, 2003, South-Western, a division of Thomson Learning.

CHAPTER 7

QUALITY-MANAGEMENT BEST PRACTICES

7.1 OVERVIEW

Achieving high levels of quality has become an increasingly important element in competitive success. Many organizations have found that they could not accomplish world-class quality by using traditional approaches to managing product and service quality. To enhance their competitive position, leading organizations have reappraised their traditional view of quality and have adopted what is known as the total quality management (TQM) model in running their businesses. Exhibit 7.1 presents a comparison of the traditional way of managing with the TQM way of managing.[1]

For many years the traditional way to achieve quality was through systematic final inspection. This approach is referred to as "inspecting in quality," which is based on detection and correction. Intense competition has led many companies to adopt TQM practices that are prevention based. This approach is often referred to as "building in quality."

7.2 WHAT IS TOTAL QUALITY MANAGEMENT?

TQM is a relatively new approach to improving business or government operations. It seeks to improve product/service quality and increase customer satisfaction by restructuring traditional management practices. TQM is an endless journey, a striving for perfection in products and services.

(a) BASIC FEATURES OF QUALITY. The best way to describe the basic features of quality is to relate them to the United States' Malcolm Baldrige National Quality Award program. The Baldrige performance excellence criteria are a framework that any organization can use to improve overall performance. Seven categories make up the award criteria.[2]

1. **Leadership.** Examines how senior executives guide the organization and how the organization addresses its responsibilities to the public and practices good citizenship
2. **Strategic Planning.** Examines how the organization sets strategic directions and how it determines key action plans
3. **Customer and Market Focus.** Examines how the organization determines requirements and expectations of customers and markets; builds relationships with customers; and acquires, satisfies, and retains customers

Traditional Way of Managing	TQM Way of Managing
The organization structure is hierarchical and has rigid lines of authority and responsibility	The organization structure becomes flatter, more flexible, and less hierarchical
Focus is on maintaining the status quo (no change)	Focus shifts to continuous improvement in systems and processes
Workers perceive supervisors as bosses or cops	Workers perceive supervisors as coaches and facilitators. The manager is seen as a leader
Supervisor/subordinate relationships are characterized by separateness, fear, and control	Supervisor/subordinate relationships shift to interdependency, trust, and mutual commitment
The focus of employee efforts is on individual effort; workers view themselves as competitors	The focus of employee efforts shifts to team effort; workers see themselves as teammates
Management determines what quality is and whether it is being provided	The organization asks customers to define quality, and it develops measures to determine if customers' requirements are met
Management perceives employees and training as costs	Management perceives employees as an asset and training as an investment
Primary basis for decisions is ''gut feeling'' or instinct	Primary basis for decisions shifts to facts and systems
Quality is not seen as providing a competitive edge	Quality is seen as providing a competitive edge

Exhibit 7.1 A Comparison of the Traditional Way of Managing with the TQM Way of Managing

4. **Measurement, Analysis, and Knowledge Management.** Examines the management, effective use, analysis, and improvement of data and information to support key organization processes and the organization's performance management system
5. **Human Resource Focus.** Examines how the organization enables its workforce to develop its full potential and how the workforce is aligned with the organization's objectives
6. **Process Management.** Examines aspects of how key production/delivery and support processes are designed, managed, and improved
7. **Business Results.** Examines the organization's performance and improvement in its key business areas: customer satisfaction, financial and marketplace performance, human resources, supplier and partner performance, operational performance, and governance and social responsibility. The category also examines how the organization performs relative to competitors.

(b) BASIC CONCEPTS OF QUALITY. The basic concepts of quality include quality assurance; quality control; quality audit; quality circles; quality councils; plan, do, check, and act (PDCA) cycle; and mistake-proofing. These concepts are part of quality infrastructure in meeting customer quality requirements. In addition, the work processes used to produce products and services must be designed to prevent problems and errors from occurring in the first place. Each concept is briefly discussed next.

Quality assurance focuses on the front end of processes, beginning with inputs, rather than the traditional controlling mode of inspecting and checking products at the end of operations, after errors are made. Processes are designed both to prevent errors and to detect and correct them as they occur throughout the process. As part of the emphasis on prevention and early detection, employees are trained to analyze incoming supplies. Suppliers are asked to assure, assess, and improve their processes and products or services. The organization establishes a partnership with suppliers and customers to assure continuous improvement in the quality of the end products and services.

Quality control is an evaluation to indicate needed corrective action, the act of guiding, or the state of a process in which the variability is attributable to a constant system of chance causes. Quality control includes the operational techniques and activities used to fulfill requirements for quality. Often, quality assurance and quality control are used interchangeably, referring to the actions performed to ensure the quality of a product, service, or process.

Quality Assurance vs. Quality Control

- Quality assurance focuses on front end of processes.
- Quality control focuses on middle and back end of processes.
- Quality assurance is a management issue.
- Quality control is a technical issue.

Quality audit is a systematic, independent examination and review to determine whether quality activities and related results comply with planned arrangements, and whether these arrangements are implemented effectively and are suitable to achieve the objectives.

Quality circles refer to a team of employees (6 to 12) voluntarily getting together periodically to discuss quality-related problems and issues and to devise strategies and plans to take corrective actions. Participative management places a premium on teamwork as the way to solve problems and initiate process improvements, especially issues with cross-functional implications. The focus is on teamwork and processes rather than on individual efforts and tasks. Quality circles should be introduced in an evolutionary manner so that employees feel that they can tap their creative potential.

Establishment of a *quality council* is a prerequisite of implementing a TQM program in the organization. The quality council is similar to an executive steering committee. By establishing a quality council, senior management provides an identity, structure, and legitimacy to the quality improvement effort. It is the first concrete indication that senior management has recognized the need to improve and has begun to change the way the organization conducts its business. The direction that this change will take becomes clear when the Quality Council publishes its vision, guiding principles, and mission statement. Management needs to support and promote the TQM program, not just sponsor it. Labor union representatives can become members of the quality council and act as coteachers of quality classes.

The *plan, do, check, act (PDCA) cycle* was first known as the Shewhart cycle and later known as the Deming cycle. It is a core management tool for problem solving

and quality improvement. The PDCA cycle can be used for planning and implementing quality improvements. The "plan" calls for developing an implementation plan for initial effort followed by organization-wide effort. The "do" part carries out the plan on a small scale using a pilot organization, and later on a large scale. The "check" phase evaluates lessons learned by pilot organization. The "act" phase uses lessons learned to improve the implementation. It supports both old and new quality tools.

Stratification can be used to break down a problem to discover its root causes and can establish appropriate corrective actions, called countermeasures. Stratification is important to the proper functioning of the Deming PDCA cycle. Failure to perform meaningful stratification can result in the establishment of inappropriate countermeasures, which can then result in process or product deterioration in quality.

The purpose of *mistake-proofing* concept is to prevent, detect, and correct inadvertent human or machine errors occurring in products and services. Automatic devices or methods can be used to avoid simple human or machine error in a production process. Mistake-proofing a service process requires identifying when and where failures generally occur. Once a failure is identified, the source must be found. The final step is to prevent the mistake from occurring through source inspection, self-inspection, or sequential checks.

7.3 BENEFITS OF TQM PRACTICES

Quality experts in private industry and government feel that there are four key measurable areas of an organization's operations that could demonstrate the impact of TQM practices on corporate performance. These benefit areas include:[3]

1. **Better Employee Relations.** One of the most important features in implementing a successful TQM system is attaining a highly involved and motivated workforce. Leading companies are using several key indicators to measure the extent to which their focus on quality leads to improvement in employee job satisfaction, attitudes, and behavior. These key indicators include employee satisfaction, employee attendance, employee turnover, safety and health, and number of suggestions made to improve quality and/or lower costs.
2. **Improved Operational Performance.** Organizations' operational performance indicators measure the quality and cost of their products and services. Leading companies are using their measures to assess the impact of quality management on their operations. These measures include reliability, timeliness of delivery, order-processing time, production errors, product lead-time, inventory turnover, quality costs, and cost savings.
3. **Greater Customer Satisfaction.** Many leading companies have changed their traditional view that quality involves merely meeting technical specifications. They now recognize that the customer defines quality and that companies must focus on meeting customer needs and expectations. Customer satisfaction is defined in terms of new customer referrals, fewer customer complaints, and high customer retention.
4. **Increased Financial Performance.** The impact on a company's "bottom line" or operating results was measured by several ratios. One important measure used is market share. Companies that build market share on the basis of improved product/service quality and value believe it is the route to increased profitability. Other

measures include productivity and profitability expressed as sales per employee and sales per a comparable retail store; return on assets; and return on sales.

7.4 TQM EFFORTS TO IMPROVE CORPORATE PERFORMANCE

World-class quality organizations have six interrelated common features consistently appeared in the companies' TQM efforts contributing to improved performance. These features involve the following best practices:

- Corporate attention focuses on meeting customer quality requirements.
- Management leads the way in disseminating TQM values throughout the organization.
- Employees are asked and empowered to continuously improve all key business processes.
- Management nurtures a flexible and responsive corporate culture with information sharing, fewer formal and informal barriers, a spirit of innovation, and high employee morale and job satisfaction.
- Management systems support fact-based and informed decision-making.
- Partnerships with suppliers improves product or service quality.

7.5 IMPORTANT FEATURES OF TQM

TQM is useful for small and large companies alike in order to improve their competitive position in both the domestic and world marketplace. Adopting TQM as a method for conducting company business will have a positive impact on key areas of corporate performance. Important features of TQM that are common to many world-class quality organizations include:

- Customer satisfaction is critical in order to remain competitive in the marketplace. Ultimately, customer satisfaction, both internal and external, drives quality efforts. Organizations, therefore, need to determine what customers want and must have processes in place to meet those customer needs.
- Top executives must provide active leadership to establish quality as a fundamental value to be incorporated into the company's management philosophy.
- Quality concepts need to be clearly articulated and thoroughly integrated throughout all activities of the company.
- Top executives need to establish a corporate culture that involves all employees in contributing to quality improvements.
- Companies need to focus on employee involvement, teamwork, and training at all levels. The focus should strengthen employee commitment to continuous quality improvement.
- To succeed, TQM systems must be based on a continuous and systematic approach of gathering, evaluating, and acting on facts and data.
- Suppliers should be made full partners in the quality management process. A close working relationship between suppliers and producers could be mutually beneficial

7.6 HUMAN RESOURCES MANAGEMENT'S ROLE IN QUALITY

Quality award-winning organizations have embraced the following four human resource management strategies to involve their employees more effectively in the effort to improve quality and better meet customer needs. These four strategies include:[4]

1. Implementing a comprehensive program to train employees in quality management concepts, problem-solving techniques, decision-making techniques, and interpersonal skills they will need to meet the organization's strategic plan for the future
2. Increasing communication within the organization through multidirectional communication systems, such as top-down, bottom-up, horizontal, and diagonal communication formats
3. Promoting, supporting, and rewarding teamwork and team culture through self-managed teams, problem-solving teams, cross-functional teams, or virtual teams
4. Empowering employees by involving them in efforts to satisfy customer needs and share in managing work processes through employee suggestion programs, management by walking around, and brainstorming sessions

7.7 PRODUCT-QUALITY BEST PRACTICES

Quality is easier to define when manufacturing tangible products, due to conformance to specifications. A defect means a product has failed to meet those specifications, with specifications coming from product designers and customers. A defect in a product does not require immediate attention until it is noticed; there is a delayed effect resulting in product recalls. In other words, the product-quality situation is either black or white.

- Monitor product-quality costs to reduce overall cost of manufacturing a product. Costs related to quality are usually separated into at least three areas: prevention costs, appraisal costs, and failure costs. Exhibit 7.2 presents relative value of investment in components of cost of quality. It is important to understand the cost relationships, in that money invested in prevention and appraisal activities can substantially reduce failure costs. In addition to reducing expenses, the reduction in external failure costs results in fewer customer complaints, which, in turn, increases customer satisfaction. A dollar invested in a prevention program saves money many times in failure costs.
    - **Prevention costs**. These costs are associated with all the activities that focus on preventing defects. Collectively, they are the cost of conformance to quality standards. Some major cost categories included in this cost classification are: operator inspection costs, supplier ratings, supplier reviews, purchase-order technical data reviews, training, supplier certification, design reviews, pilot projects, prototype test, vendor surveys, quality design, and quality department review costs.
    - **Appraisal costs**. These costs are associated with measuring, evaluating, or auditing products to assure conformance with quality standards and performance requirements. Some major cost categories included in this cost classification are purchasing appraisal costs, qualifications of supplier product,

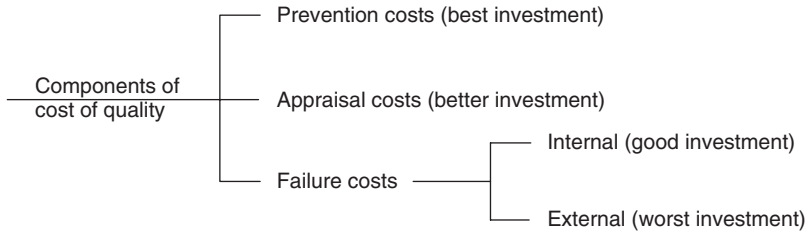

Exhibit 7.2 Components of Cost of Quality

equipment calibration, receiving and shipping inspection costs, tests, and product-quality audits.

- **Failure costs**. These costs are associated with evaluating and either correcting or replacing defective products, components, or materials that do not meet quality standards. Failure costs can be either internal failure costs that occur prior to the completion or shipment of a product or the rendering of a service, or external failure costs that occur after a product has been shipped or a service has been rendered. Examples of internal failure costs include product/part repair, redesign, reinspection, rework, retesting, sorting, and scrap. Examples of external failure costs include product warranty charges, returns, and recalls; liability suits; and field-service-staff training costs.

- Implement quality-management tools, problem-solving tools, and decision-making tools to improve product quality.
- Implement Six Sigma quality approaches to reduce defects in products.
- Measure return on quality (ROQ) to justify investments in improving quality of products.
- Develop and monitor quality metrics to help manage overall product quality. Some examples of metrics include the following:
  - The total cost of quality (COQ) as percentage of revenue by year
  - The cost of conformance as percentage of total cost of quality
  - The cost of nonconformance as percentage of total cost of quality
  - Total number of defects as a percentage of good production
  - Total number of product recalls this year compared to last year
  - Total cost of product recalls as a percentage of revenue or operating cost by year
  - Total number of customer complaints this year compared to last year
- Eliminate non-value-added activities (e.g., rework and inspections) and focus on value-added activities in manufacturing a product.
- Conduct product-quality audits and environmental audits periodically and unexpectedly to improve quality of products and to reduce pollution respectively.
- Invite key customers and suppliers into internal product design, development, and quality meetings to understand their concerns, inputs, and needs.

- Implement "design for product quality" approaches such as (1) selecting parts with the criteria of cost, functionality, and quality, (2) designing processes that are statistically "in control," (3) keeping the design and processing steps simple, and (4) preventing defects with mistake-proofing techniques.
- Measure product quality in terms of length of useful life (e.g., six years or 60,000 miles), amount of a desirable input (e.g., 90% gas and 10% ethanol), and amount of a desirable output (e.g., 40 miles per gallon of gas).
- Invite labor union representatives to work as full partners alongside company management to implement quality-management systems. Benefits of formal partnership include increased trust and cooperation between management and labor unions.

7.8 SERVICE-QUALITY BEST PRACTICES

Quality is difficult to define when providing intangible services due to specifications coming from multiple sources, such as one company and thousands of individual customers. Misalignment between company specifications and customer specifications leads to customer dissatisfaction and defection. An error in service requires immediate attention, correction, and feedback. In other words, the service-quality situation is neither black nor white.

- Monitor service-quality costs to reduce the overall cost of providing a service. Some examples include cost of service guarantees, cost of refunds, customer service cost, and cost of lost customers.
- Implement quality management tools, problem-solving tools, and decision-making tools, to improve service quality. Complement these tools with customer satisfaction and perception surveys, focus groups, customer complaint analysis, employee research, similar industry studies, and transaction analysis.
- Implement Six Sigma quality approaches to reduce errors in delivering services.
- Measure return on quality (ROQ) to justify investments in improving quality of services.
- Develop and monitor quality metrics to help manage overall service quality. Some examples of metrics include the following:
    - The total cost of customer service as a percentage of revenue by year
    - The total cost of lost customers as a percentage of revenue by year
    - The total cost of lost customers as a percentage of customer service cost
    - The total cost of customer service as a percentage of operating cost by year
    - The total cost of service guarantees as a percentage of revenue by year
    - The total cost of refunds as a percentage of revenue by year
    - The combined cost of customer service, lost customers, service guarantees, and refunds as a percentage of operating cost by year
    - Total number of customer complaints this year compared to last year
- Eliminate non-value-added activities (e.g., reviews and rework) and focus on value-added activities in providing a service.
- Conduct service-quality audits periodically and unexpectedly to improve quality of services.

- Conduct random surveys of customers to obtain their feedback on service they receive, using a number of techniques such as toll-free telephone numbers and online Web site questionnaires.
- Implement "design for service quality" approaches such as (1) selecting the right employees with the right skills, (2) providing targeted training, (3) giving quick feedback to employees as things happen, instead of waiting for a year, (4) keeping work-processing steps simple, and (5) preventing errors with mistake-proofing techniques.
- Measure service quality in terms of employee reliability, responsiveness, and assurance toward service, and empathy toward customers.
- Invite labor union representatives to work as full partners alongside company management to implement quality-management systems. Benefits of formal partnership include increased trust and cooperation between management and labor unions.

7.9 QUALITY-IMPROVEMENT, PROBLEM-SOLVING, AND DECISION-MAKING TOOLS

Quality tools and techniques can be used to analyze processes, prioritize problems, report the results, and to evaluate the results of a corrective action plan. In the beginning, seven original quality control tools were introduced, and later seven quality management tools came into effect. The seven quality management tools are modern, while the seven quality control tools are traditional. The seven problem-solving tools and the seven decision-making tools are also important in solving quality-related issues and problems.

(a) SEVEN QUALITY CONTROL TOOLS. The seven original quality-control tools are check sheets, histograms, scatter diagrams, Pareto diagrams, flowcharts, cause-and-effect diagrams, and control charts. Each tool is discussed briefly below.

(i) Check sheets. Check sheets are used for collecting data in a logical and systematic manner. The data collected can be used in constructing a quality-control chart, Pareto diagram, or histogram. The most important use of the check sheet is that it enables the user to gather and organize data in a format that permits efficient and easy analysis of data.

Process improvement is facilitated by the determination of what data or information is needed to reduce the difference between customer needs and process performance. Some examples of data that can be collected include: process variables, including size, length, weight, and diameter; number of defects generated by each cause; product characteristics; costs; vendors; inspection procedures; customer profiles; employees' attitudes; and defect location. The idea is that once this data is collected and analyzed, the cause can be found and a plan to eliminate the problem can be implemented.

(ii) Histograms. A histogram is a frequency distribution diagram in which the frequencies of occurrences of the different variables being plotted are represented by bars. The purpose is to determine the shape of the graph relative to the normal distribution (or other distributions). It is often confused with a bar graph, in which the frequency of a variable is indicated by the height of the bars. In a histogram, the area of the bar indicates

the frequency. Histograms can only be used with variable data, which require measurements on a continuous scale. Only one characteristic can be shown per histogram, and at least 30 observations representing homogeneous conditions are needed.

A histogram is a frequency distribution, in which the area of each bar is always proportional to the actual percentage of the total falling in a given range. If the bars are of equal length, then the histogram is equivalent to a bar graph, in which the relative size of the bars depends only on their heights. A histogram can be compared to the normal distribution (or other distribution). For example, if the graph is off centered or skewed, this may indicate that a process requires adjustment. Histograms are essentially used for the same applications as bar graphs, except that the horizontal scale in a histogram must be numerical, usually representing a continuous random variable.

A bar graph is a frequency distribution diagram in which each bar represents a characteristic or attribute, and the height of the bar represents the frequency of that characteristic. The horizontal axis may represent a continuous numerical scale (e.g., hours), or a discrete nonnumerical scale (e.g., phases of a project). Generally, numerical-scale bar graphs in which the bars have equal widths are more useful for comparison purposes; numerical-scale bar charts with unequal intervals can be misleading because the characteristics with the largest bars (in terms of area) do not necessarily have the highest frequency. Bar graphs are used to compare the frequencies of different attributes (e.g., number or percentage of problem reports by phase).

(iii) Scatter diagrams. A scatter diagram is a plot of the values of one variable against those of another variable to determine the relationship between them. These diagrams are used during analysis to understand the cause-and-effect relationship between two variables. Scatter diagrams are also called correlation diagrams.

If the data points fall approximately in a straight line, this indicates that there is a linear relationship, which is positive or negative, depending on whether the slope of the line is positive or negative. Further analysis using the method of least squares can be performed. If the data points form a curve, then there is a nonlinear relationship. If there is no apparent pattern, this may indicate no relationship. However, another sample should be taken before making such a conclusion.

Method of least squares can be used in conjunction with scatter diagrams to obtain a more precise relationship between variables. It is used to determine the equation of the regression line (i.e., the line that "best fits" the data point). With this equation, one can approximate values of one variable when given values of the other.

(iv) Pareto diagrams. A Pareto diagram is a special use of the bar graph in which the bars are arranged in descending order of magnitude. The purpose of Pareto analysis, using Pareto diagrams, is to identify the major problems in a product or process, or more generally, to identify the most significant causes for a given effect.

This allows a developer to prioritize problems and decide which problem area to work on first.

Pareto analysis is based on the 20/80 rule, which states that approximately 20% of the causes (the "vital few") account for 80% of the effects (problems). The "vital few" can be determined by drawing a cumulative percent line and noting which bars are to the left of the point marking 80% of the total count. The vital few are usually indicated by significantly higher bars and/or a relatively steep slope of the cumulative percent line.

Pareto diagrams (charts) can be helpful in determining whether efforts toward process improvement are producing results. These diagrams are useful when the process is stable; they will not be effective if used on a chaotic process because the process is not ready for improvement. The process must first be stabilized through the use of control charts. *Root cause analysis is performed using the Pareto diagrams*.

Pareto diagrams can be drawn showing before and after improvements, demonstrating the effect of the improvements through the use of Pareto diagrams. The diagrams are a powerful tool when used in this way because they can mobilize support for further process improvement and reinforce the continuation of current efforts. Pareto diagrams are based on the 80/20 rule, which holds that 20% of sources account for 80% of problems, and are usually drawn as pie charts, histograms, or vertical bar charts.

(v) Flowcharts. A flowcharting tool can be used to document every phase of a company's operation—for example, in a manufacturing company, from order taking to shipping. It is an effective way to break down a process or pinpoint a problem. Flowcharting can be done at both the summary level and the detailed level, serving different user needs.

Flowcharting is a first step toward the documentation of a process required for ISO 9000 and other quality awards. In this way, problems can be traced quickly to the right source and corrected properly. Also, the flowcharts can be used as a training tool or a reference document on the job.

A process map is similar to a flowchart. Mapping is the activity of developing a detailed flowchart of a work process showing its inputs, tasks, and activities in sequence. A process map provides a broader perspective than typical flowcharts.

(vi) Cause-and-effect diagrams. A cause-and-effect (C&E) diagram is used when a series of events or steps in a process creates a problem and it is not clear which event or step is the major cause of the problem. Each process or subprocess is examined for possible causes; after the causes associated with the different steps in the process are discovered, significant root causes of the problem are selected, verified, and corrected. C&E diagrams are also called fishbone or Ishikawa diagrams (after the diagrams' inventor).

The C&E diagram should be used as a framework for collecting efforts. If a process is stable, it will help organize efforts to improve the process. If a process is chaotic, the C&E diagram will help uncover areas that can help stabilize the process.

(vii) Control charts. A control chart assesses a process variation. The control chart displays sequential process measurements relative to the overall process average and control limits. The upper and lower control limits establish the boundaries of normal variation for the process being measured. Variation within control limits is attributable to random or chance causes, while variation beyond control limits indicates a process change due to causes other than chance—a condition that may require investigation. The upper control limit and lower control limit give the boundaries within which observed fluctuations are typical and acceptable. They are usually set, respectively, at three standard deviations above and below the mean of all observations.

A run chart is a simplified control chart, in which the upper and lower control limits are omitted. The purpose of the run chart is more to determine trends in a process, rather than its variation. Run charts can be used effectively to monitor a process—for

example, to detect sudden changes and to assess the effects of corrective actions. Run charts provide the input for establishing control charts after a process has matured or stabilized in time. Limitations of this technique are that it analyzes only one characteristic over time and does not indicate if a single data point is an outlier.

(b) SEVEN QUALITY MANAGEMENT TOOLS. The original quality control tools were adequate for data collection and analysis, but the new seven quality management tools allow better identification, planning, and coordination in quality-problem solving. While the original seven quality control tools are used for quantitative data analysis, the new seven quality management tools are used for qualitative data analysis. These new tools are affinity diagrams (the KJ method), tree diagrams, process-decision program charts, matrix diagrams, interrelationship digraphs, prioritization matrices, and activity network diagrams (arrow diagrams). Each tool is discussed briefly below.

(i) Affinity diagrams. The affinity diagram is a data reduction tool, in that it organizes a large number of qualitative inputs into a smaller number of major categories. These diagrams are useful in analyzing defect data and other quality problems, and are used in conjunction with cause-and-effect diagrams or interrelationship digraphs.

(ii) Tree diagrams. A tree diagram can be used to show the relationships of a production process by breaking it down from few larger steps into many smaller steps. The greater the detail of steps, the better simplified they are. Quality improvement actions can start from the right-most of the tree to the left-most.

(iii) Process-decision program charts. The process-decision program chart (PDPC) is a preventive control tool in that it prevents problems from occurring in the first place, although it also mitigates the impact of the problems if they do occur. From this aspect, it is a contingency planning tool. The objective of the tool is to determine the impact of the "failures" or problems on project schedule.

(iv) Matrix diagrams. A matrix diagram is developed to analyze the correlations between two groups of ideas with the use of a decision table. This diagram allows one to systematically analyze correlations. Quality function deployment (QFD) is an extension of the matrix diagram. The American Supplier Institute defines QFD as: "A system for translating consumer/customer requirements into appropriate company requirements at each stage, from research and product development, to engineering and manufacturing, to marketing/sales and distribution."

QFD is a structured method and uses a series of charts called "quality tables" to provide the discipline and communication required to focus on answering three action-oriented questions: what, how, and how much. QFD can be used both for products and services.

(v) Interrelationship digraphs. The interrelationship digraph is used to organize disparate ideas. Arrows are drawn between related ideas. An idea that has arrows leaving it but none entering is a "root idea." More attention is then given to the root ideas for system improvement. The digraph is often used in conjunction with affinity diagrams.

(vi) Prioritization matrices. Prioritization matrices are used to help decision makers determine the order of importance of the activities being considered in a decision. Key issues and choices are identified for further improvement. These matrices combine the use of a tree diagram and a matrix diagram.

(vii) Activity network diagram. Activity network diagrams (arrow diagrams) are project management tools to determine which activities must be performed, when they must be performed, and in what sequence. These diagrams are similar to program evaluation and review technique (PERT) and critical path method (CPM), the popular tools in project management. Unlike PERT and CPM, activity network diagrams are simple to construct and require less training to use.

(c) SEVEN PROBLEM-SOLVING TOOLS. Seven major tools are available for the problem solver to arrive at robust solutions. They are brainstorming, synectics, nominal group technique, the force-field approach, systems analysis, TRIZ, and investigative questions. Differences exist among the problem-solving tools, and often they do not work equally well in different situations. In any given situation, one or two tools might have a greater probability of leading to the desired outcomes.

(i) Brainstorming. The purpose of the brainstorming technique is to generate a great number of ideas; that is, its purpose is idea generation. The key is to let the members of the group feel free to express whatever ideas come to mind without fear of judgment or criticism. Uninhibited flow of ideas is permitted; negative thinking is not permitted. Recording all ideas and deferring judgment until the later phases of the analysis is the hallmark of brainstorming. The brainstorming technique is most effective when the presence of an expert is not necessary, the high level of creativity is seen as a bonus rather than an irritant, and a large quantity of ideas is needed.

(ii) Synectics. Synectics is a technique for creating an environment that encourages creative approaches to problem solving. It is a highly structured approach for an individual who needs a group to help solve a problem. It involves the use of nontraditional activities, such as excursions and fantasies, and analogies. Synectics is good for idea generation and team building.

(iii) Nominal group technique. The nominal group technique (NGT) is an idea-generating, consensus-building tool. *No real group exists—it is there in name only*. A strength of this process is that a problem can be brought into focus in a short period of time. The approach is very structured and is an excellent technique to use when the group members are drawn from various levels of the organizational hierarchy or when they are in conflict with one another. The technique gives everyone an opportunity to express ideas without being interrupted by others in the group.

The unique NGT process combines a silent time for idea generation with the social reinforcement of an interacting-group setting. This structured process forces equality of participation among members in generating and sharing information about the issue. The NGT group may consist of five to eight participants.

(iv) Force-field analysis. Force-field analysis involves the identification of a problem, the factors or forces contributing to making it a problem, and steps for generating solutions. Two main sets of forces are identified: (1) inhibiting forces—those that resist the resolution of the problem; and (2) facilitating forces—those that push the problem toward resolution. Once the forces acting on a problem are identified, actions can be taken to decrease the major resisting forces, increase the major facilitating forces, or both. This process, then, is basically an analysis of the forces acting to keep the problem a problem.

(v) Systems analysis. Systems analysis breaks down a large problem into many smaller problems. It is an excellent technique if the desired outcome of the problem-solving session is a detailed understanding of a problem. The technique offers a structure for analyzing a problem and various alternative solutions. However, it does not structure the roles of the participants. The major strength of this process is that it offers a method of reviewing the total context of a problem. The phrase "systems analysis" does not mean analysis of computer-based information systems. The scope is broader than that—manual systems, automated, or both.

This method requires the problem solver to look beyond the unit of the problem to the environment for various possible solutions. It focuses on three attributes: (1) open systems, (2) multiple reasons and causes, and (3) the entire picture.

(vi) TRIZ. TRIZ is a Russian language acronym loosely translated into English and designates a theory of solving inventive problems. It supports the idea that unsolved problems are the result of contradicting goals (constraints) and nonproductive thinking. It suggests breaking out of the nonproductive-thinking mold by reframing the contradicting and competing goals in such a way that the contradictions disappear.

(vii) Investigative Questions. The approach is to ask six investigative (journalism) questions—who, what, when, where, why, and how—to better understand the root causes of issues and problems.

(d) SEVEN DECISION-MAKING TOOLS. Seven major tools are available for the decision maker to reach sound decisions. They are decision tables, discriminant analysis, decision trees, payoff tables, success-failure analysis, risk analysis, and reality checks. As with the problem-solving tools, any one or two of the decision-making tools may have a greater probability of leading to the desired outcome in a given situation.

(i) Decision tables. A decision table documents rules used to select one or more actions based on one or more conditions. These conditions and their corresponding actions can be presented either in a matrix or tabular form.

(ii) Discriminant analysis. Discriminant analysis is a qualitative, subjective tool to differentiate between effective and ineffective procedures or actions.

(iii) Decision trees. A decision tree is a graphical representation of possible decisions, events, or states of nature resulting from each decision with its associated probabilities and outcomes. The decision problem displays the sequential nature of the decision-making situation.

(iv) Payoff tables. A payoff table is a tabular representation of the payoffs for a decision problem. It shows losses and gains for each outcome of the decision alternative.

(v) Success-failure analysis. Success-failure analysis is a qualitative approach to brainstorm conditions for both success and failure. A T-column can be used with the headings "What will guarantee success" and "What will guarantee failure."

(vi) Risk analysis. Risk analysis is the analysis of possible risks to be encountered and possible means of handling them. A T-column can be used with the headings "Anticipated risks" and "Actions to overcome risks."

(vii) Reality checks. The reality check decision is tested in the pseudo-real-world conditions. A T-column is used with headings "Our expectations" and "Our concerns" to facilitate the analysis.

7.10 APPLICABLE LAWS, REGULATIONS, STANDARDS, AND PRINCIPLES

Organizations have a legal and ethical obligation to comply with the various federal, state, and local laws, regulations, circulars and bulletins, directives and executive orders, government orders, and ordinances pertinent to a specific business area. Noncompliance with these laws and regulations can lead to fines, civil and/or criminal penalties, probation, and jail punishments (prison time), thus creating reputation (image) risk. Compliance with industry and/or organization standards, including professional standards, can increase the quality of products and services, which, in turn, can enhance an organization's reputation and image in the marketplace. Adherence to generally accepted business principles and practices could have a similar effect as complying with standards.

A brief roundup of information about major laws, regulations, and standards is provided here as a reminder for checklist purposes. Note that these laws and regulations are subject to change as new ones are added and existing ones are amended or repealed. The reader is advised to obtain the original laws, regulations, and standards from the official sources for a better understanding of the provisions, requirements, and conditions of the laws, regulations, and standards (www.regulations.gov). Although some of the following laws, regulations, and standards directly affect the public sector organizations (i.e., government agencies), private-sector organizations can read, learn, and apply them to improve their business operations on a proactive basis.

U.S. organizations should comply with the following laws, regulations, standards, and principles pertinent to quality management:

Consumer Product Safety Act. The U.S. Consumer Product Safety Commission was created by the Consumer Product Safety Act of 1972 as an independent agency responsible for protecting the public from unreasonable risks of injury and death associated with consumer products. The Commission specifies safety standards for consumer products. The Act has jurisdiction over many consumer products used in and around the home, in schools, and in recreation. The Act requires U.S. manufacturers of consumer products to report information about settled or adjudicated lawsuits and product recalls.

Magnuson-Moss Warranty Act. The Magnuson-Mass Warranty Act of 1975 governs consumer product warranties. The Act requires manufacturers and sellers of consumer

products to provide consumers with detailed information about warranty coverage. In addition, it affects both the rights of consumers and the obligations of warrantors under written warranties.

Malcolm Baldrige National Quality Improvement Act. The Malcolm Baldrige National Quality Improvement Act was passed in 1987 to issue the Malcolm Baldrige National Quality Award to U.S businesses—manufacturing and service, small and large—and to education, nonprofit organizations, and health care organizations that apply and are judged to be outstanding in seven areas or categories: leadership; strategic planning; customer and market focus; measurement, analysis, and knowledge management; human resource focus; process management; and business results. The award is not given for specific products or services (baldrige.nist.gov).

The seven criteria are used by thousands of organizations for all kinds for self-assessment and training, and as a tool to develop performance and business processes. For many organizations, using the criteria results in better employee relations, higher productivity, greater customer satisfaction, competitive edge, increased market share, and improved profitability.

Cost of Quality. The cost of quality (COQ) measurement identifies areas for process improvement. The focus of this measurement is to express quality in terms of quantitative and financial language—that is, costs, return on investment, cost of poor quality, cost of rework, and so on.

The COQ definition includes the following three items:

1. The cost of making a product conform to quality standards (i.e., quality goods)
2. The cost of not conforming to quality standards (e.g., waste and loss)
3. A combination of items 1 and 2

$$\text{COQ} = \text{the cost of conformance (A)} + \text{the cost of nonconformance (B)},$$

where (A) includes cost to prevent and detect a failure, and (B) includes cost to correct a failure.

ISO 9000 Series Standards. ISO 9000 consists of a series of generic standards with appropriate guidelines published by the International Organization for Standardization (called ISO) for vendor certification programs. ISO 9000 addresses quality-system processes, not product performance specifications. In other words, the ISO 9000 covers how products are made, but not necessarily how they work. ISO 9000 focuses on processes, not on products or people. It is based on the concept that one will fix the product by fixing the process. The ISO 9000 is a set of standards for judging the quality of suppliers. It assumes that suppliers have a sound quality system in place and it is being followed. ISO 9000 can be used as a baseline quality system to achieve TQM objectives (www.iso.org).

The standards are becoming an acceptable worldwide approach to vendor certification and international trade. The real push is from companies throughout the world who are requesting that their suppliers become certified. The ISO 9000 standards are equally applicable to manufacturing and service industries, and remove the nontariff barriers that arise from differences and inadequacies among national, local, or company standards. Major categories of nontariff barriers include quantitative import restrictions such as quotas, voluntary export restraints, and price controls.

There are two kinds of standards: (1) product standards dealing with technical specifications, and (2) quality standards dealing with management systems. Quality measures for ISO 9000 include leadership, human resource development and management, management of process quality, and customer focus and satisfaction.

ISO 14000 Standard. ISO 14000 is the international standard for environmental management. The scope of the standard includes all efforts to minimize waste and redesign manufacturing processes, products, and packaging to prevent pollution. More attention should be given to pollution prevention rather than correction. To achieve these goals, environmental protection, like quality and safety management, must be integrated into daily business operations (www.iso.org).

ISO 14001 Standard. ISO 14001 is a management framework for planning, developing, and implementing environmental strategies in an organization. The framework includes a policy, a planning process, an organizational structure, specific objectives and targets, specific implementation programs, communications and training programs, and management review, monitoring, and corrective action, which includes environmental audit. The standard is applicable to any organization regardless of size or business type (www.iso.org).

Six Sigma Quality.[5] Coined by Motorola Inc. and implemented by many world-class organizations including General Electric (GE) Co., Six Sigma is a highly disciplined process that helps organizations focus on developing and delivering near-perfect products and services. It is a vision of quality, a striving for perfection.

The phrase "six sigma" is a statistical term that measures how far a given process deviates from perfection. The central idea behind the approach is that if one can measure how many "defects" are found in a process, one can systematically figure out how to eliminate them and get as close to "zero defects" as possible. Defects are sources of customer irritation. Defects are costly to both customers and to manufacturers or service providers. Eliminating defects provides cost improvements. To achieve Six Sigma quality, a process must produce no more than 3.4 defects per million opportunities. An "opportunity" is defined as a chance for nonconformance, which in turn is defined as not meeting required specifications. This means organizations need to be nearly flawless in executing their key processes.

GE uses three approaches and models in implementing its Six Sigma quality initiative:

1. Design for Six Sigma (DFSS). DFSS is a systematic methodology utilizing tools, training, and measurements to enable GE to design products and processes that meet its customer expectations and can be produced at Six Sigma quality levels.
2. Define, Measure, Analyze, Improve, and Control (DMAIC). DMAIC is a process for continued improvement. It is a systematic scientific, and fact-based approach. The closed-loop process eliminates nonproductive steps and activities, often focuses on new measurements, and applies technology for improvement.
3. Critical to Quality (CTQ). CTQ is an element of a process or practice that has a direct impact on the perceived quality of the process or practice.

Voice of the Customer. "Voice of the customer" (VOC) means organizations should listen to and understand the external customers' needs, wants, and expectations

(i.e., customers' voice) and provide products and services that truly meet such needs, wants, and expectations. The same thing applies to internal customers' needs (i.e., departments or functions within an organization).

Quality Function Deployment. Quality function deployment (QFD) is a structured method in which customer requirements are translated into appropriate technical requirements for each stage of product development and manufacturing. Input for the QFD process comes from listening to the voice of the customer.

House of Quality. The house of quality (HOQ) is a diagram that clarifies the relationship between customer needs and product features. It helps correlate market or customer requirements and analysis of competitive products with higher-level technical and product characteristics. The diagram, which makes it possible to bring several factors into a single figure, is named for its house-shaped appearance but sometimes is referred to as QFD, a sign of the connection between the three approaches of VOC, QFD, and HOQ.

Taguchi Method. Genichi Taguchi of Japan emphasizes reducing variation in the production process and in the final product as the principal way of improving quality. He believes this can be done by designing products that perform in a consistent manner, even under conditions of varying or adverse use. He also believes that one can make this happen at the design stage by appropriate statistical experimental design methods.

Taguchi views quality engineering as composed of three elements: system design, parameter design, and tolerance design. He developed a quality-loss function to measure quality in monetary units that reflect both short-term and long-term losses.

Taguchi's approach to quality is relatively precise. Conventional quality-control activities center on final inspection sampling or on control charts and process control. This is called on-line quality control. Taguchi pushed the process upstream to focus on product and process design. This is called off-line quality control.

Mistake-Proofing Concept. Both manufacturing and service operations must be designed with the mistake-proofing concept ("idiotproofing") in mind. It uses automatic devices or methods to avoid simple human-made or machine-made errors. It focuses on prediction and detection of errors and defects. The concept is relatively easy and inexpensive to implement. Japanese companies follow this concept very closely (*Poka-yoke*).

American Society for Quality. The American Society for Quality (ASQ) is a professional organization and the voice of the quality profession. It establishes professional certifications (e.g., CQE, CQM, and CQA), professional standards, and a code of ethics for quality professionals to follow. CQE is Certified Quality Engineer, CQM is Certified Quality Manager, and CQA is Certified Quality Auditor (www.asq.org).

International Quality Standards. The Deming Prize was instituted in Japan and is awarded to all companies that meet its prescribed standard. The small number of awards given each year is an indication of the difficulty of achieving the standard.

The European Foundation for Quality Management (EFQM) Excellence Award, formerly known as the European Quality Award, was designed to increase awareness throughout the European Community, and among businesses in particular, of the growing importance of quality to member nations' competitiveness in the increasingly global market and to their standards of life.

The Canadian Awards for Business Excellence quality citeria are similar in structure to the U.S. Baldrige Award criteria, with some key differences.

The Australian Business Excellence Award has solid labor union support. As with Baldrige, this award emphasizes the holistic and interconnected nature of the management process.

Additional Resources

Schonberger, Richard. *Best Practices in Lean Six Sigma Process Improvement*. Hoboken, NJ: John Wiley & Sons, 2007.

Watson, Gregory H. *Strategic Benchmarking Reloaded with Six Sigma: Improving Your Company's Performance Using Global Best Practice*. Hoboken, NJ: John Wiley & Sons, 2007.

Notes

1. U.S. General Accounting Office, *Management Practices: U.S. Companies Improve Performance through Quality Efforts* (GAO/NSIAD-91-190), Washington, DC: May 1991.
2. The Malcolm Baldrige National Quality Improvement Act of 1987, Washington, DC: National Institute of Standards and Technology, U.S. Department of Commerce, Washington, DC; http://www.baldrige.nist.gov.
3. *See* note 1.
4. GAO, *Federal Quality Management: Strategies for Involving Employees* (GAO/GGD-95-79), Washington, DC: April 1995.
5. General Electric (GE) Co., Six Sigma. Excerpted from the GE Web site http://www.ge.com/en/company/companyinfo/quality/quality.htm

CHAPTER 8

PROCESS-MANAGEMENT BEST PRACTICES

8.1 OVERVIEW

The scope of process management includes processes in manufacturing and service operations. Processes are used to manufacture a product or to provide a service. Manufacturing processes transform raw materials (inputs) into finished goods (outputs), using labor, equipment, energy, and manufacturing facilities. Service processes, for example, transform insurance claims (inputs) into checks (outputs), using office staff, computers, and buildings. Both manufacturing and service processes exhibit variability, in that process outcomes are uncertain or unpredictable due to variations in performance levels of people and machines. Management's challenge is to control the process variability so that outputs or outcomes meet the defined product specifications or service performance criteria.

Manufacturing processes exhibit bottlenecks, machine breakdowns, waste, delays, defects, and excess inventories leading to increased costs and investments, decreased production throughput, and increased customer dissatisfaction. Similarly, service processes exhibit delays in terms of waiting for information from downstream or upstream functions; inefficiencies in terms of repeat or redundant activities and many handoffs; and worker fatigue leading to increased costs, decreased productivity, and increased customer dissatisfaction. Management's goal is to make both manufacturing and service processes lean, flexible, efficient, and predictable to meet customer needs and satisfaction.

8.2 BUSINESS PROCESSES

A *process* is a set of interrelated resources and activities that transform inputs into outputs. A *product* or *service* is the result of activities or processes. Two kinds of process models exist: the "as is" process model and the "to be" process model. The "as is" process model portrays how a business process is currently structured. During process improvement efforts, the "as is" model is used to establish a baseline for measuring subsequent business improvement actions and progress. The "to be" process model results from a business process redesign or reengineering action. It shows how the business process will function in the future after the improvement action is implemented.

"As is" process model $\longrightarrow$ "To be" process model = Change required

(Before Improvement) (After Improvement) (Level of change)

The difference between the "to be" process model and the "as is" process model indicates the amount and level of change required to achieve the desired improvement. This change needs to be managed with required resources allocated.

A *process owner* should be assigned for major business processes. This owner should be held accountable and responsible for the workings and improvement of one of the organization's defined-processes and its related subprocesses. The process owner may be someone currently associated with the existing process, but not necessarily. The process owner should be closely involved—if not actually leading—the reengineering team.

Organizations should implement the following best practices to improve business processes:

- Utilize business-process management tools to understand and evaluate a business process.
- Understand and listen to the "voice of the process" in order to improve business processes.
- Increase production throughput by (1) eliminating bottlenecks in a process, (2) reducing workloads on the bottleneck resource, (3) synchronizing process flows, (4) acquiring newer and faster equipment, (5) streamlining process flows, (6) rearranging the work cells, and (7) giving employees incentives to work faster and smarter.
- Increase service employees' productivity through proper training, motivation, and incentives, and through empowerment.
- Decrease product and process costs by eliminating non-value-added activities and repeat activities and reducing waste. Examples of non-value-added activities include rework time, reviews and inspections time, waiting time, and transport time.
- Decrease product and process costs by focusing on value-added activities such as process time, assembly time, and core production time.
- Decrease investment in inventory and inventory levels at all storage locations with just in time (JIT) methods and quick response (QR) systems.
- Reduce the work content of an activity on the critical path or move the work content to a non critical path.
- Design key performance indicators (KPI) and metrics to reduce process variability by (1) using statistical process control (SPC) tools and control charts, and (2) streamlining, simplifying, standardizing, and institutionalizing work processes.
- Implement Six Sigma approaches to reduce product and process variability and to increase their quality.
- Champion business operations improvements, such as business process reengineering (BPR), business process improvement (BPI), business process redesign, benchmarking, and total quality management (TQM) programs or initiatives.

8.3 BUSINESS PROCESS REENGINEERING

(a) SCOPE OF BUSINESS PROCESS REENGINEERING. Business process reengineering (BPR) is a management technique for achieving dramatic improvements in cost, quality, and customer service by making fundamental changes in the way an organization defines

its mission and performs its work. BPR is based on a thorough understanding of an organization's customers, their needs, and the environment in which it operates. BPR is focused on improving business processes that create and deliver value by satisfying the customer's needs. Generally, these processes cut across functional, geographic, and organizational units.

BPR is typically characterized by the following elements:

- Challenging the current organizational mindset to become one that is more receptive to customers and the environment, driven by top-management effort
- Identifying and analyzing core business processes
- Applying cost/service/quality measures to determine how effectively they are meeting customer needs
- Making systematic changes to the organization's structure, culture, roles, and responsibilities in order to support reengineered processes

The ultimate goals of BPR are to improve efficiency, reduce costs, and improve customer service. The concept of fundamental or radical change is an integral part of BPR. Rather than focusing on how to do things better, faster, or less expensively, BPR asks whether a given activity should be done at all. BPR efforts are often characterized by their broad, far-reaching, fundamental changes to the nature of the work itself. In many cases, BPR is used to take an organization that is fragmented and specialized by function and to reintegrate it into a new whole that is focused on the processes that result in value to the customer. A by-product of BPR is elimination of non-value-added activities.

(b) PROCESS REENGINEERING

WHAT IS REENGINEERING?

Reengineering is customer-focused and outcome-oriented.

Process-reengineering changes should not be constrained by the existing organizational structure, current thinking, or culture of the organization. Long-standing and ingrained ways of doing things may be radically changed. The changes made often include organizational, structural, and procedural changes geared toward achieving multiple results, such as improving service delivery, lowering costs, increasing quality, eliminating redundancies, and speeding up processes. BPR cannot be carried out in small and cautious steps.

A reengineering project is situational and specific to each process and to each organization. When a reengineering project leads to new information requirements, it may be necessary to acquire new information technology (IT) to support those requirements. It is important to bear in mind, however, that acquiring new IT does not constitute reengineering. IT is an enabler of process reengineering, not a substitute for it. Acquiring technology in the belief that its mere presence will somehow lead to process innovation is a root cause of bad investments in information systems. Exhibit 8.1 shows interconnections between organization mission and IT through work processes, decisions, and information needs.[1]

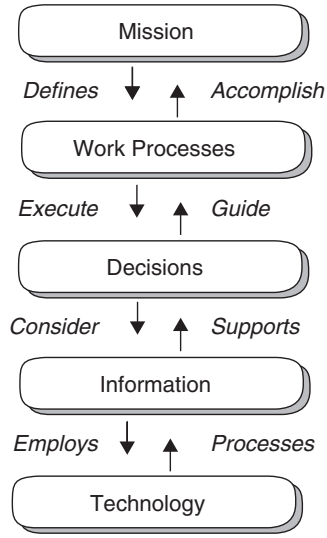

EXHIBIT 8.1 RELATIONSHIP OF MISSION AND WORK PROCESSES TO INFORMATION TECHNOLOGY

ROLE OF IT MANAGEMENT

IT management should champion process improvements, such as business process reengineering, business process improvement, and total quality management programs in their organizations.

IT is almost always an important enabler in BPR, but it is not the driver of the changes being implemented. The business's needs must drive the processes. After processes have been redefined, technology provides the necessary tools for support of the new processes. IT is often what allows organizations to "break the rules" and radically change their processes. Old rules such as the need for documents to move in a linear, sequential manner can be broken by applying the appropriate technology to enable the new nonlinear processes to work. BPR uses IT to enable employees to work in fundamentally different ways and to support changes in the way in which work is done.

The biggest challenge of BPR is the implementation. It requires a special set of leadership skills sustained over a long period of time in order to see the process through to successful implementation and reap the rewards of BPR.

(c) REENGINEERING PRINCIPLES. World-class organizations have developed five principles for reengineering organizations in order to increase customer satisfaction and decrease operating costs by eliminating non-value-added activities. To do so, many companies have radically changed their way of doing business. While these principles are not intended to be an all-inclusive list on how to effectively implement reengineering, they should form the basis of a framework for bringing about the radical change required to reengineer business processes in a large organization.[2]

Principle 1: Top management must be supportive of and engaged in reengineering efforts to remove barriers and drive success.

Principle 2: An organization's culture must be receptive to reengineering goals, objectives, and principles.

Principle 3: Major improvements and savings are realized by focusing on the business from a process rather than a functional perspective.

Principle 4: Processes should be selected for reengineering based on a clear notion of customer needs, anticipated benefits, and potential for success.

Principle 5: Process owners should manage reengineering projects with teams that are cross-functional, maintain a proper scope, focus on customer metrics, and enforce implementation timelines and discipline.

(d) BPR ASSESSMENT. BPR is one approach for redesigning the way work is done to better support an organization's mission and reduce costs. Reengineering starts with a high-level assessment of an organization's mission, strategic goals, and customer needs. Basic questions are asked, such as "Does our mission need to be redefined? Are our strategic goals aligned with our mission? Who are our customers?" An organization may find that it is operating on questionable assumptions, particularly in terms of the wants and needs of its customers. Only after the organization rethink *what* it should be doing, does it go on to decide *how* best to do it.[3]

BPR assessment issues are grouped into three major areas and parts, with a total of nine issues being addressed.

Part A: Assessing the organization's decision to pursue reengineering, focuses on strategic and general management issues that need to be resolved before an organization embarks on a reengineering project. Three issues, along with their key activities, are the following:

Issue 1: Has the organization reassessed its mission and strategic goals?

Key Activities for Issue 1 include:

- Reassessing the organization's mission and priorities
- Reassessing how well the organization's products, services, and delivery modes align with the needs of its customers and other stakeholders
- Identifying and assessing the impact of other change drivers, such as a changing mission, demographic shifts, budget cuts, and downsizing
- Defining and mapping the business processes that are key to meeting customer and other stakeholder needs

Issue 2: Has the organization identified performance problems and set improvement goals?

Key Activities for Issue 2 include:

- Measuring performance and identify problems in meeting mission goals and the needs of customers and other stakeholders
- Benchmarking against the goals and performance of leading organizations
- Establishing ambitious performance improvement goals that are mission-oriented and meaningful to customers and other stakeholders
- Selecting and prioritizeing processes to be improved

Issue 3: Should the organization engage in reengineering?

Key Activities for Issue 3 include:

Deciding whether any of the processes needing improvement should be reengineered
Assessing the organization's readiness to engage in a reengineering project
Developing and communicating a compelling business case for initiating a reengineering project
Integrating the reengineering project into the organization's overall strategy for improving mission performance
Developing and beginning implementation of a change management plan

Organizations should do the following for Part A:

- **Action 1.** Reassess mission and strategic goals. Well-defined missions and strategic goals form the foundation of the key business systems and processes, and thus help ensure the successful outcome of their operations. Day-to-day activities should support the organization's missions and move management closer to accomplishing its strategic goals.
- **Action 2.** Map each of its core processes at a high level. High-level process mapping typically results in a graphic representation depicting the inputs, outputs, constraints, responsibilities, and interdependencies of the core processes. This high-level map provides managers and staff with a common understanding of how the processes work and how they are connected.
- **Action 3.** Assess which processes are in greatest need of improvement in terms of cost, quality, and timeliness. By analyzing the gap between where processes are and where they need to be to achieve desired outcomes, organizations can target those processes that are in most need of improvement, set realistic improvement goals, and select an appropriate process improvement technique (e.g., benchmarking).

Part B: In assessing the new processes' development, pick up at the point where the organization has decided to begin a reengineering project. The assessment issues focus on the management of the reengineering team, the team's process redesign activities, and the business case it develops to support a decision to begin implementing the new design. Three issues, along with their key activities, are the following:

Issue 4: Is the reengineering project appropriately managed?

Key Activities for Issue 4 include:

Establishing an executive steering committee and project sponsor to support the reengineering project
Establishing an owner for the process to be reengineered
Forming a qualified, trained, well-led team to reengineer the target process and its supporting structures
Establishing a clear team charter that defines project goals, resources, constraints, and deliverables.
Selecting and following a reengineering methodology to guide the project

Issue 5: Has the project team analyzed the target process and developed feasible alternatives?

Key Activities for Issue 5 include:

Mapping and analyzing the target process in enough detail to identify the costs and causes of performance breakdowns
Designing alternative processes and testing their effectiveness through simulations and/or limited pilots
Assessing the impact of potential barriers to implementing the alternative processes
Developing a performance-based and risk-adjusted cost-benefit analysis of each alternative process

Issue 6: Has the project team completed a sound business case for implementing the new, target process?

Key Activities for Issue 6 include:

Selecting a feasible process alternative with a high return on investment
Developing a formal business case for implementing the new process that describes costs, benefits, and risks
Using the organization's capital-investment review process to evaluate the business case and decide whether to proceed with implementation

Organizations should do the following for Part B:

- **Action 1.** Decide whether they want to engage in reengineering for process improvement. After the reengineering project is selected and resources and responsibilities are assigned, the project team needs to develop a deeper understanding of the target process workflow, problem areas, and improvement opportunities. This is largely done through more detailed process modeling. The current process should be modeled in enough detail to (1) provide the organization with a common understanding of the process, (2) establish a performance baseline at the process activity level from which to measure improvements, (3) identify problem areas and non-value-added activities that need to be changed or eliminated, such as excessive handoffs, reviews, rework, and queuing and waiting time, and (4) understand exactly what will be changed and who will be affected during the shift from the current process to a new process. This last point is particularly important for successful implementation. Simulation-modeling tools and other analytical techniques include flowcharting, tree diagrams, fishbone diagrams, and process-mapping analysis.
- **Action 2.** Team members should include people who work within the process being reengineered and should represent several organizational levels. The team may also include outside suppliers, employee unions, consultants, and others who bring different skills and perspectives to the team and are able to think "out of the box." Because of the variety of skills needed at different phases of the reengineering project, the composition of the team may change over the course of the project, but a core of team members should participate throughout the entire reengineering process for continuity.

Based on what it learns in analyzing the existing process, the team begins its redesign effort—the creative part of reengineering. The team should use a cost-effective method for conducting its preliminary assessment of alternative processes. Such methods include prototyping, limited pilot testing, and modeling and/or computer simulation. As the project team completes its process redesign work, the business case will be enlarged and updated to present a full picture of the benefits, costs, and risks involved in moving to a new process.

- **Action 3.** The team should identify potential barriers to implementing alternative processes. The purpose of barrier identification is to find unusual or major obstacles that will need to be overcome in order to implement a new process. Political issues should be a key concern. Other concerns include entrenched workplace attitudes or values, an insufficient number of employees with the skills required for the redesigned roles, collective bargaining agreements, incompatible organizational or physical infrastructure, current laws and regulations, and funding constraints. The impact of these barriers and the costs of addressing them (such as staff training, hiring, and relocating) need to be factored into the cost/benefit analysis.

Barriers that arise from internal skepticism and resistance to change are to be expected and can often be overcome through the use of employee education, change management activities, and successful pilot testing of the new process.

The team should develop a performance-based cost/benefit analysis for each alternative to provide (1) the foundation for comparing the baseline benefits and costs with proposed alternative processes and (2) a basis for decision-makers to use in selecting a feasible alternative process that meets performance goals.

Given several possible process design alternatives, the reengineering team and the executive steering committee need to settle on one. The new design must be feasible to implement, given the various constraints and barriers that face the organization. There must also be a high return on investment in the project, in terms of improved performance and/or reduced costs.

Part C: Assessing project implementation and results deals with the problems involved in piloting and developing a new business process. Both the technical and nontechnical (human) issues surrounding implementation are touched on, along with the need to evaluate the performance and results of the new process. Three issues, along with their key activities, are the following:

Issue 7: Is the organization following a comprehensive implementation plan?

Key activities for Issue 7 include:

Establishing a transition team and developing a comprehensive plan to manage implementation

Managing training and workforce redeployment issues

Conducting pilot tests of the new process prior to full implementation

Issue 8: Are organization executives addressing change management issues?

Key Activities for Issue 8 include:

Preparing and following a change management strategy

Encouraging staff to accept new ideas and adopt the new process
Preparing staff, managers, and executives for changes in their roles and career expectations

Issue 9: Is the new process achieving the desired results?

Key Activities for Issue 9 include:

Measuring the performance of the new process
Determining if the new process is achieving the desired results
Using performance measurement as a feedback loop for continuously improving the new process

Organizations should do the following for Part C:

- **Action 1.** Implementation is the most difficult phase of the reengineering project. Ideas are turned into actions, and the organization's natural resistance to change must be overcome. An implementation plan should be developed that spells out the work that needs to be done, with time frames, milestones, decision points, and resource allocations. Training and workforce issues are important elements of an effective implementation plan. Pilot testing provides a method for redefining the process and building support for full implementation of the new process across the organization.

  The organization needs to establish a *transition team* to manage the implementation process. The team should include the project sponsor, the process owner, members of the reengineering team, key executives, managers, and staff from the areas directly affected by changeover from the old process to the new process.

  Training and redeploying the workforce is often a major challenge and generally requires substantial preparation time. When a process is redesigned and new information systems (IS) are introduced, many of the tasks that workers perform are radically changed or redistributed. Some positions may be eliminated or cut back, while others are created or modified. Workers may need to handle a broader range of responsibilities, rely less on direct supervision, and develop new skills.

  Pilot testing is an effective—and usually necessary—tool for moving the organization successfully to full implementation. Pilot testing allows the organization to (1) evaluate the soundness of the proposed process in actual practice, (2) identify and correct problems with the new design, and (3) refine performance measures. Also, successful pilot testing will help strengthen support for full-scale implementation from employees and outside stakeholders and will help secure the funding needed for a smooth rollout.

  The length and extent of pilot testing will vary depending on the complexity of the changes being driven by the new process. For example, a complex process that affects regional offices and plants across the nation may require a series of pilot tests. Organizations should be careful, however, not to test beyond the point of diminishing returns. No matter how much testing is done, only full implementation can reveal all of the potential problems with the new process.

- **Action 2.** The implementation of a new process is typically the most failure-prone phase of the reengineering project because of an organization's natural resistance to change. Frequently, the greatest challenges lie not in managing the technical or operational aspects of change, but in managing the human dimensions of change. Widely shared perceptions, based on assumptions deeply rooted in the organization's culture, can translate into a belief that reengineering is unnecessary, unworkable, or unfair.
- **Action 3.** Executives should begin building a change management plan from the very beginning of the project. The plan should be revised to (1) present the goals and objectives of the new process in concrete, "nuts and bolts" language and (2) link the new process to specific issues, questions, and challenges involved in implementation (e.g., worker roles, relationships, performance expectations, supervisory methods, and career path). The plan should include periodic checkpoints for assessing and responding to the opinions and attitudes of staff about the perceived consequences of the new process.

  Executives and managers often speak of resistance to change from employees or outside groups. But management itself can resist the full implications of changing a work process. As a result of reengineering, staff often have a broader range of responsibilities and are *empowered* to make decisions and take actions with less direct supervision than before. Executives and managers must establish new working relationships with employees, placing more emphasis on their role as facilitators, teachers, or coaches, and less on being directors and controllers. This transition can be difficult. Executives and managers who fail to change with their staff put the reengineering effort at great risk.
- **Action 4.** An organization has no way of knowing if the new process has produced the desired results unless it has meaningful *performance measures*. Good performance measures generally include a mix of outcomes, output, and efficiency measures. Outcome measures assess whether the process has actually achieved the intended results. Output measures examine the products and/or services produced by the process, such as the number of claims processed or units produced. Efficiency measures evaluate such things as the cost of the process and the time it takes to deliver the output of the process (a product or service) to the customer. Ongoing performance measurement provides the feedback that is so critical for actual improvement and future successes.

As part of its business case for implementing the new process, the organization should have established specific performance goals for the reengineered process. These goals should include a mixture of intermediate goals to be met at various stages during the implementation phase, as well as ultimate performance goals for the process after it has been fully implemented and institutionalized. The intermediate goals are particularly important because the organization should be able to start showing a return on investment in the early stages of implementation.

The gains achieved by the new process can erode unless the organization continually monitors its performance and makes further refinements. Managers should use performance information to continually improve work processes, identify performance gaps, and set additional improvement goals, as needed.

TEN CRITICAL SUCCESS FACTORS FOR BPR

1. Top-level management support is critical.
2. Long-term commitment is critical.
3. High-quality staffing is critical.
4. Business, not technology, is the driver.
5. Substantial customer input is needed.
6. Coordination between functions and departments of an organization is needed.
7. Appropriate use of technology is necessary.
8. Good upfront planning is critical.
9. Organization culture must be changed.
10. Control, measurement, evaluation, and feedback are necessary.

(e) INFORMATION TECHNOLOGY REENGINEERING. The scope of IT reengineering consists of software reengineering, forward engineering, reverse engineering, and process reengineering to improve the quality of computer systems. Data reengineering is used to improve the quality of data within a computer system.

(i) Software Reengineering. Software reengineering is defined as (1) the examination and alteration of a subject system to reconstitute it in a new form and (2) the subsequent implementation of the new form. Software reengineering consists of reverse engineering followed by some form of forward engineering or modification. Enhancements to meet new requirements that were not in the original system may subsequently be performed. Reverse engineering is the process of analyzing a subject system to identify the system's components and their interrelationships and to create representations of the system in another form or at a higher level of abstraction. It is the derivation of system design specifications based on the physical system description. This involves analyzing the code and all documentation, and recording relevant information from the human users and maintainers. Reverse engineering does not involve modifications to the system, only examination of the system. Also, it is not necessary to start reverse engineering at the lowest-level description (code); it may be started at a higher level such as design. When abstracting low-level information to higher-level descriptions, optimization mechanisms or environment dependencies necessary for the original environment are removed. Those mechanisms that are applicable for the target environment can be added during forward engineering.

Another area in which it is useful to consider the use of software reengineering is in migrating the functionality of an older system to a new computing environment. This is especially true in those areas where it is necessary to enhance the system to satisfy new requirements. By reverse engineering, information for the development of the application system in a new environment is collected. An analysis of current functionality in light of new system requirements may permit redesign of the system. The software can then be forward engineered to the target environment directly from the gathered information.

Software reengineering also enables the reuse of software components from existing systems. The knowledge gained from reverse engineering can be used to identify candidate systems composed of reusable components, which can then be used in other applications. Reverse engineering can also be used to identify functionally redundant parts in existing application systems.

(ii) Forward Engineering. Forward engineering is the traditional process of moving from high-level abstractions and logical, implementation-independent designs to the physical implementation of a system.

One reason to consider reengineering is the possible reduction of software maintenance costs. In many of today's systems, maintenance changes have been directly implemented in the code and have not been carried back to the design documentation of the systems. Lack of documentation and complexity of code force software maintainers to devote an extensive amount of time to trying to understand the functions of a system. Reengineering provides a means of reworking the documentation and code into a more maintainable format that allows software maintainers to quickly gain a better understanding of the application system.

It is not necessary to apply the entire reengineering process to achieve the benefit of reducing maintenance costs—accomplishing part of the process, such as design recovery and restructuring, can have a significant impact on maintenance costs. Design recovery, for example, can be performed in order to recover and record lost system information. This can reduce an organization's dependence on those individuals who understand the present software and shorten the time necessary for new individuals to learn the system.

(iii) Reverse Engineering. Reverse engineering can be used to gain a better understanding of the current system's complexity and functionality and to identify "trouble spots." Errors can be detected and corrected, and modifications can be made to improve system performance. The information gained during reverse engineering can be used to restructure the system, thus making the system more maintainable. Maintenance requests can then be accomplished more easily and quickly.

(iv) Process Reengineering. Process reengineering is a code-level procedure that analyzes control flow. A program is examined to create overview architecture with the purpose of transforming undesirable programming constructs into more efficient ones. Program restructuring can play a major role in process reengineering.

(v) Data Reengineering. Data reengineering examines and alters the data definitions, values, and the use of data. Data definitions and flows are tracked through the system. This process reveals hidden data models. Data names and definitions are examined and made consistent. Hard-coded parameters that are subject to change may be removed. This process is important because data problems are often deeply rooted within computer systems.

8.4 BUSINESS PROCESS IMPROVEMENT

(a) SCOPE OF BUSINESS PROCESS IMPROVEMENT. BPI should be continuous, not discreet, and it tends to be more of an incremental change that may affect only a single task or segment of the organization. The concept of fundamental or radical change is the basis of the major difference between BPR and BPI. Quite often BPI initiatives limit their focus to a single existing organizational unit. This in itself breaks one of the tenets of BPR, which is that BPR must focus on redesigning a fundamental business process instead of looking at existing departments or organizational units. While BPR seeks to

Element	BPR	BPI
Degree of change	Radical (e.g., 80%)	Incremental (e.g., 10–30%)
Scope	Entire process	Single area, function/unit
Time	Years	Months
Driver	Business	Technology
Focus	Redefine process	Automate/eliminate the function
Work structure	Unified	Fragmented
Orientation	Outcome	Function

Exhibit 8.2 Key Differences Between BPR and BPI

define what the processes should be, BPI focuses more on how to improve an existing process or service. BPI is also called **continuous process improvement**.

Links Between BPR, BPI, and IT

Techniques such as BPR and BPI are used to improve efficiency, reduce costs, and improve customer service. IT is an enabler of BPR and BPI, not a substitute for them.

Through BPI, organizations can achieve significant incremental improvements in service delivery and other business factors (e.g., increase in employees' productivity). The expected outcomes of BPI are not as dramatic as those associated with BPR initiatives, but because radical change is not the aim, there is much less trauma involved in the process. In many cases, incremental changes may be achieved in situations that lack the support necessary for more radical changes. Exhibit 8.2 shows the key differences between the two concepts of BPR and BPI.

(b) METHODOLOGY FOR BPI. A methodology for business operations improvements includes BPI, BPR, business process redesign, benchmarking, and TQM programs or initiatives. Championing business operations improvements require the following five elements to be in place.

1. **Invest money wisely.** Investing money strictly in IT often does not achieve the improvements needed. The reason is that if outdated, labor-intensive work processes are further automated, there is little overall improvement. Therefore, it is essential for organizations to apply process improvement techniques to work processes. These techniques are often referred to as BPR and BPI, and their major features are compared in Exhibit 8.3.

   There are certain similarities between BPI and BPR, as indicated in the above exhibit. Both techniques involve processes as the primary unit of analysis, and measurement of process performance is necessary for both to succeed. Both BPI and BPR can be used effectively to bring an organization into closer accord with its customers' needs. Both demand organizational and behavioral change in order to be successful, and, lastly, both require an investment of time before significant results can be expected.

   There are key differences, however, between BPI and BPR. While BPI tends to involve incremental changes, BPR focuses on radical, fundamental changes.

Features of Business Process Improvement	Features of Business Process Reengineering
Normal organizational and behavioral change	Significant organizational and behavioral change
Incremental changes	Radical changes
Investment of time required before results are seen	Substantial investment of time required before results are seen
Start with existing process and improve	Start with clean slate

Exhibit 8.3 Major Features of BPI and BPR

BPI programs usually start with the current state of a process and then seek improvements to that process. Business-reengineering programs urge participants to break loose from outmoded business processes (begin with a "clean slate") and the design principles underlying them, to create new ones.

BPI provides a method for aligning existing information systems with business goals. BPR is more appropriate when an organization needs radical changes to align its information management and IT programs with new business strategies. In addition, BPR is used to achieve substantial cost savings through the reengineering of processes and the application of new technology. BPI techniques can be applied to information management through TQM.

How Long is What?

- BPI can take less than a year to implement.
- BPR can take two to five years to implement.
- Business process redesign can take several months to two years to implement.

Ideally, work process analysis should drive decisions concerning information system applications and new technologies. Incorporation of work process analysis into the system-development life cycle and methodology can yield tremendous benefits to the organization even before new technology is applied. Before any systems development or enhancement of existing systems takes place, the sponsoring department should evaluate needed changes in business practices. Then the organization can consider the introduction of new methodologies and technologies for use in improving business processes based on current needs and resources.

2. **Implement change methodologies.** Organizations should apply methodologies such as BPR or BPI to evaluate targets for change and areas that could benefit from application of information technology.
3. **Implement business process redesign efforts.** Process redesign focuses on improving an entire business process—or a major subprocess—where performance measurement and benchmarking indicate the opportunity or need for significant performance gains. Because it often requires additional resources or a redistribution of existing resources, redesign requires more senior management

attention than BPI. Redesign often affects several parts of an organization: reporting relationships, policies and procedures, and employee skill needs.

Role of Business Process Champions

Process champions improve business operations and processes by (1) investing money wisely, (2) implementing change methodologies, (3) implementing business-process redesign efforts, (4) implementing benchmarking techniques, and (5) implementing a TQM program.

4. **Implement benchmarking techniques.** In benchmarking with others, an organization (1) determines how leading organizations perform a specific process, (2) compares their methods to its own, and (3) uses the information to improve upon or completely change its process. Benchmarking is typically an internal process, performed by personnel within an organization who already have a thorough knowledge of the process under review.
5. **Implement a TQM program.** TQM is a management approach that emphasizes improving product or service quality while decreasing production or service costs by increasing the efficiency of work processes. Major strategies to implement TQM include (1) implementing a comprehensive program to train employees in quality management concepts, problem-solving techniques, decision-making tools, and other skills they will need to meet the organization's strategic plan for the future, (2) increasing communication within the organization, (3) promoting, supporting, and rewarding teamwork, and (4) empowering employees by involving them in efforts to satisfy customer needs and share in managing work processes.

8.5 BUSINESS-PROCESS MANAGEMENT TOOLS

Many analytical tools exist to understand and evaluate a business process. These tools include Pareto diagrams, root cause analysis, flowcharting, tree diagrams, process-mapping analysis, cause-and-effect (fishbone) diagrams, stratification, check sheets, value analysis and value engineering, run charts, histograms, scatter diagrams, control charts, and statistical process control (SPC).

(a) PARETO DIAGRAMS. Pareto diagrams allow management to focus its efforts on the problems that have the greatest potential for improvement by showing relative frequency and/or size in a descending bar graph. These diagrams or charts can be helpful in determining whether efforts toward process improvement are producing results. These diagrams are useful when the process is stable; they will not be effective if used on a chaotic process because the process is not ready for improvement. The process must first be stabilized through the use of control charts. Root cause analysis can be performed using the Pareto diagrams.

Pareto diagrams can be drawn showing before and after improvements, demonstrating the effect of the improvements through the use of Pareto diagrams. The diagrams are a powerful tool when used in this way because they can mobilize support for further process improvement and reinforce the continuation of current efforts. Pareto diagrams

are based on the 80/20 rule, which holds that 80% of problems are caused by 20% of sources. The diagram is usually drawn as pie charts, histograms, or vertical-bar charts. Pareto diagram focuses on "vital few" instead of "trivial many." When arranged from greatest to least, the Pareto chart graphically indicates which problems should be handled first.

(b) ROOT CAUSE ANALYSIS. Root cause analysis is a study of the original reason for nonconformance with a process. When the root cause is removed or corrected, the nonconformance can be eliminated. It is a technique used to identify the conditions that initiate the occurrence of an undesired activity or state. Six investigative questions—who, what, when, where, why, and how—can be used to better understand the root causes of issues and problems.

(c) FLOWCHARTING. A flowcharting tool can be used to document every phase of a company's operation—for example, in a manufacturing company, from order taking to shipping. It is an effective way to break down a process or pinpoint a problem. Flowcharting can be done at both the summary level or the detailed level serving different user needs.

Flowcharting is a first step toward the documentation of a process required for ISO 9000 and other quality awards. In this way, problems can be traced quickly to the right source and corrected properly. Also, the flowcharts can be used as a training tool or a reference document on the job.

(d) TREE DIAGRAMS. A tree diagram graphically shows any broad goal divided into different levels of detailed actions. It encourages team members to expand their thinking when creating solutions. Tree diagrams show the complete range of tasks and subtasks needed to achieve an objective. Tasks are displayed from summary (left) to detail (right), a range that can be rolled forward (disaggregation) and backward (aggregation). Both problems and solutions can be identified using the tree diagram.

(e) PROCESS-MAPPING ANALYSIS. Process mapping is an illustrated description of how things get done, which enables team participants to visualize an entire process and identifies areas of strengths and weaknesses. It helps reduce cycle time and defects. Process-mapping analysis is similar to a flowchart showing a work process in detail. Activities and subactivities are linked and mapped to process objectives. It also helps establish measurement metrics for key processes.

(f) CAUSE-AND-EFFECT DIAGRAMS. A cause-and-effect (C&E) diagram is used when a series of events or steps in a process creates a problem and it is not clear which event or step is the major cause of the problem. Each process or subprocess is examined for possible causes; after the causes associated with the different steps in the process are discovered, significant root causes of the problem are selected, verified, and corrected. C&E diagrams are also called fishbone or Ishikawa diagrams (after the diagrams' inventor).

The C&E diagrams should be used as a framework for collecting efforts. If a process is stable, it will help organize efforts to improve the process. If a process is chaotic, the C&E diagrams will help uncover areas that can help stabilize the process.

(g) STRATIFICATION. Stratification is a procedure used to describe the systematic subdivision of population or process data to obtain a detailed understanding of the structure of the population or process. It is not to be confused with a stratified sampling method. Stratification can be used to break down a problem to discover its root causes and can establish appropriate corrective actions, called countermeasures. Stratification is important to the proper functioning of Deming's plan, do, check, act (PDCA) cycle. *Failure to perform meaningful stratification can result in the establishment of inappropriate countermeasures, which can then result in process or product deterioration in quality of process or product*.

STRATIFICATION VERSUS PARETO DIAGRAM VERSUS C&E DIAGRAM

- Stratification can be used when performing root cause analysis with Pareto diagrams. A problem can be broken down into subcomponents, and each subcomponent can be further broken down into its subcomponents, and so on. Then attention should be paid to one or more of the root causes of a process or product problem, from which countermeasures can be established to resolve the problem.
- Stratification can also be used when performing root cause analysis with C&E diagrams. A C&E diagram can be used to stratify one bar at a time from a Pareto diagram in order to get an in-depth understanding of the corresponding cause (bar) before any other cause (bar) is studied.

(h) CHECK SHEETS. Check sheets are used for collecting data in a logical and systematic manner. The data collected can be used in constructing a quality control chart, Pareto diagram, or histogram. The most important use of the check sheet is that it enables the user to gather and organize data in a format that permits efficient and easy analysis of data.

Process improvement is facilitated by the determination of the data or information that is needed to reduce the difference between customer needs and process performance. Some examples of data that can be collected include: process variables, including size, length, weight, and diameter; number of defects generated by each cause; product characteristics; costs; vendors; inspection procedures; customer profiles; employees' attitudes; and defect location. The idea is that once data are collected and analyzed, the cause can be found and a plan to eliminate the problem can be implemented.

(i) VALUE ANALYSIS AND VALUE ENGINEERING. Value analysis is the organized and systematic study of every element of cost in a part, material, or service to make certain it fulfills its function at the lowest possible cost. The terms "value analysis" and "value engineering" are used synonymously. Since value analysis is a team effort, freedom of suggestions from all affected parties is necessary for successful work. Value analysis is similar to imagineering, although the latter focuses on describing a perfectly functioning process.

Value analysis is related to product or service characteristics such as quality, performance, marketability, maintainability, and reliability. There is a tradeoff involved among these characteristics.

Quality must be maintained or enhanced; otherwise any cost savings will be negligible as sales and reputation decline. The effort requires a continuous reappraisal

of the material, product, and process selected, because applications, competition, and customer expectations do change.

In value analysis, the goal is equal or improved accomplishment of the function at a lower cost. In some cases, cost may have to be increased to achieve better *performance* or to reduce maintenance costs and thereby improve product marketability. Value analysis recognizes that *marketability* must be maintained or improved. This requires that products should have sales appeal in terms of greater esteem value, lower repair and maintenance costs, and efficient and effective functioning.

Maintainability is an important feature affecting a customer's total cost of a product or service. If a value analysis study results in increased maintenance costs for the customer, any savings realized would sooner or later be negated by decreased sales and loss of goodwill. It is equally important that the required reliability of a product be preserved or improved by the value-analysis recommendations. *Reliability* must be studied in terms of its relation to lost sales, loss of customer goodwill, and lost profits.

(j) RUN CHARTS. A run chart shows performance measures monitored over time to display variability in process output (e.g., weight and volume) across time periods. Trend and seasonality factors can be observed.

(k) HISTOGRAMS. A histogram is a bar chart showing the frequency distribution of observed performance characteristics such as weights, volume, response time, cost, and customer experiences with the ordering process.

(l) SCATTER DIAGRAMS. A scatter diagram shows the strength of two variables of interest in a process under study. This diagram displays whether the two variables are positively correlated or negatively correlated with each other.

(m) CONTROL CHARTS. A control chart monitors variance in a process over time and alerts management to unexpected variance, which may cause defects. A control chart is like a run chart and contains an upper control limit or lower control limit. If the observed data falls within the upper and lower control limits, we conclude that variability is normal and the process is in control. If the observed data falls outside of upper and lower control limits, we conclude that the process is out of control, requiring analysis of assignable causes.

(n) STATISTICAL PROCESS CONTROL. Statistical process control (SPC) is the application of statistical methods to analyze data and to study and monitor process capability and performance. *Control* is the state of stability, normal variation, and predictability. SPC is a process of regulating and guiding operations and processes using quantitative data. *Variance* is a change in a process or business practice that may alter its expected outcome.

8.6 APPLICABLE STANDARDS AND PRINCIPLES

Compliance with industry standards, organization standards, and regional/national/international standards, including professional standards, can increase the quality of products and services, which, in turn, can enhance an organization's reputation and image in the marketplace. Adherence to generally accepted business principles and practices could have a similar effect to complying with standards.

U.S. organizations should comply with the following standards and principles pertinent to process management:

Six Sigma Quality. Coined by Motorola Inc. and implemented by many world-class organizations including General Electric (GE) Co., Six Sigma is a highly disciplined process that helps organizations focus on developing and delivering near-perfect products and services.[4] It is a vision of quality, a striving for perfection.

The phrase "six sigma" is a statistical term that measures how far a given process deviates from perfection. The central idea behind the approach is that if one can measure how many "defects" are found in a process, one can systematically figure out how to eliminate them and get as close to "zero defects" as possible. Defects are sources of customer irritation. Defects are costly to both customers and to manufacturers or service providers. Eliminating defects provides cost improvements. To achieve Six Sigma quality, a process must produce no more than 3.4 defects per million opportunities. An "opportunity" is defined as a chance for nonconformance, which in turn is defined as not meeting the required specifications. This means organizations need to be nearly flawless in executing their key processes.

GE uses three approaches and models in implementing its Six Sigma quality initiative:

1. Design for Six Sigma (DFSS). DFSS is a systematic methodology utilizing tools, training, and measurements to enable GE to design products and processes that meet its customer expectations and can be produced at Six Sigma quality levels.
2. Define, Measure, Analyze, Improve, and Control (DMAIC). DMAIC is a process for continued improvement. It is a systematic scientific, and fact based approach. The closed-loop process eliminates nonproductive steps and activities, often focuses on new measurements, and applies technology for improvement.
3. Critical to Quality (CTQ). CTQ is an element of a process or practice that has a direct impact on the perceived quality of the process or practice.

Theory of Constraints. Eliyahu M. Goldratt devised the theory of constraints, which deals with tools and techniques used for identifying and eliminating the constraints (bottlenecks) in a manufacturing process, steps that increase production throughput and productivity.

Voice of the Customer. "Voice of the customer" (VOC) means organizations should listen to and understand the external customers' needs, wants, and expectations (i.e., customers' voice) and provide products and services that truly meet such needs, wants, and expectations. The same thing applies to internal customers' needs (i.e., departments or functions within an organization).

Quality Function Deployment. Quality function deployment (QFD) is a structured method in which customer requirements are translated into appropriate technical requirements for each stage of product development and manufacturing. Input for the QFD process comes from listening to the voice of the customer.

House of Quality. The house of quality (HOQ) is a diagram that clarifies the relationship between customer needs and product features. It helps correlate market or customer requirements and analysis of competitive products with higher-level technical and

product characteristics. The diagram, which makes it possible to bring several factors into a single figure, is named for its house-shaped appearance but sometimes is referred to as QFD, a sign of the connection between the three approaches of VOC, QFD, and HOQ.

Just in Time Methods. The just in time (JIT) method is a philosophy of doing business differently to achieve cost, production, and service efficiencies, and to reduce waste, delays, and problems. JIT can be applied to production, purchasing, inventory, transportation, training, and quality.

Quick Response System. The quick response (QR) system links manufacturers, wholesalers, and retailers in a logistics network by synchronizing product flows with information flows. The goal of the QR system is to achieve greater accuracy of sales demand forecasts and to improve in-stock percentage availability. The QR system, which is for retailers and wholesalers what the JIT method is for manufacturers, reduces inventory investment by scheduling the delivery of parts or raw materials close to production lines. Critical success factors for the effective functioning of the QR system include low cycle times, high service levels, high inventory turns, and high fill rates for product orders.

Mistake-Proofing Concept. Both manufacturing and service operations must be designed with mistake-proofing ("idiotproofing") in mind. The approach uses automatic devices or methods to avoid simple human-made or machine-made errors. It focuses on prediction and detection of errors and defects. The concept is relatively easy and inexpensive to implement. Japanese companies follow this concept very closely (*Poka-yoke*).

Voice of the Process. "Voice of the process" means understanding and evaluating the nature of process flows, process variations, and process characteristics and capabilities for both products and services. The goal is to reduce process variations in order to make the process stable and predictable and to reduce cycle time.

New work processes must be designed to reduce the cycle time by eliminating stop points, chokepoints, pain points, or fault points in a process that enjoys the support and availability of resources such as tools, technology, people, equipment, and information. Existing work processes must be (1) streamlined by reviewing the upstream and downstream work steps, (2) simplified by removing unnecessary handoffs, stop points, chokepoints, pain points, or fault points, (3) standardized based on "lessons learned," and (4) institutionalized by being rolled out to the entire organization.

Additional Resources

Braganza, Ashley. *Radical Process Change: A Best Practice Blueprint*. Hoboken, NJ: John Wiley & Sons, 2001.

Graham, Ben B. *Detail Process Charting: Speaking the Language of Process*. Hoboken, NJ: John Wiley & Sons, 2004.

Halvey, John K. and Barbara Murphy Melby. *Business Process Outsourcing,* second edition. Hoboken, NJ: John Wiley & Sons, 2007.

Schonberger, Richard. *Best Practices in Lean Six Sigma Process Improvement*. Hoboken, NJ: John Wiley & Sons, 2007.

Watson, Gregory H. *Strategic Benchmarking Reloaded with Six Sigma: Improving Your Company's Performance Using Global Best Practice*. Hoboken, NJ: John Wiley & Sons, 2007.

Notes

1. U.S. General Accounting Office, *Business Process Reengineering Assessment Guide*, Version 3 (GAO/AIMD-10.1.15), Washington, DC: April 1997.
2. GAO, *Reengineering Organizations: Results of a GAO Symposium* (GAO/NSIAD-95-34), Washington, DC: Dec. 1994.
3. *See* note 1.
4. General Electric (GE) Corporation, Six Sigma. Exerpted from the GE Web site http://www.ge.com/en/company/companyinfo/quality/quality.htm.

CHAPTER 9

HUMAN-RESOURCES MANAGEMENT BEST PRACTICES

9.1 OVERVIEW

Both the private- and public sector organizations employ a diverse and knowledge-based workforce comprised of individuals with a broad spectrum of technical and functional skills and institutional memory. They are the organization's human capital, its greatest asset.[1]

To attain the highest level of performance and accountability, organizations depend on three enablers: people, process, and technology. The most important of these is people, because an organization's people define its character and its capacity to perform.

9.2 ROLES AND RESPONSIBILITIES OF THE CHIEF PEOPLE OFFICER

The Chief People (Human Resources) Officer or its equivalent is a key person in the C-level executive suite and has the following roles and responsibilities:

- Linking human resource (HR) strategy to business strategy
- Supporting all employees of the organization from hiring to firing
- Developing human talent acquisition and retention strategies that are sustainable over longer periods of time
- Developing an HR manual describing policies, procedures, and standards expected of employees
- Establishing and encouraging self-service systems so employees can select health care benefits and life insurance coverage, can schedule paid time off and vacations, can participate in attitude and satisfaction surveys, and can enroll in training and development courses
- Conducting employee exit interviews to understand the reasons for leaving the organization. Incorporate the "lessons learned" from the exit interviews into the employee hiring-to-rehiring cycle
- Integrating HR administrative tasks with HR strategic tasks for maximum efficiency and effectiveness
- Developing a "one system of record" to capture employee information in one place by integrating the back-end systems with the front-end systems through automation such as business application systems (e.g., payroll and personnel systems) and Web-based systems (e.g., resume requests, interview requests, job offers made, and job offers accepted). Some benefits of integrated systems include

(1) maximum data consistency, completeness, and accuracy, (2) better internal customer service and satisfaction, and (3) stronger connection of disparate and disconnected business processes.

- Linking HR costs to cash flows and gross profits, and lower total HR costs to increase profits
- Increasing faster HR service deliveries to internal customers to achieve their total satisfaction
- Innovating new HR service techniques and processes by leveraging technology to improve quality and to reduce costs
- Eliminating non-value-added activities such as HR administrative and clerical tasks to reduce inefficiencies and to lower costs
- Focusing more on value-added activities such as HR strategic tasks to provide a solid value to the internal customers and to the organization
- Identifying key drivers of cost, quality, risks, expenses, revenues, profits, business growth, competition, and performance. Focus on the root causes of these drivers and understand why these drivers go up and down.
- Building standardized, transparent, and repeatable HR service processes to provide the stable, consistent, and quality services that internal customers expect
- Understanding that increases in sales velocity increase inventory velocity, which, in turn, increases production or service velocity, finance velocity, human capital velocity, and systems velocity. The goal is to synchronize these velocities in a cohesive manner.
- Implementing the goal congruence concept by linking individual employee goals with those of the department/division and the organization. He must remove or reduce the competing or conflicting goals.
- Implementing crosscutting best practices across business units, divisions, departments, and functions through busting silos and building bridges
- Linking employee rewards, bonuses, and promotions to employees' true performance and tangible results, and empower employees
- Building solid working relationships with C-level executives in marketing, finance, operations, IT, and other functions through formal and informal approaches at the workplace
- Fostering ethical values and cultural sensitivity in light of workforce diversity, and provide cross-cultural orientation and preparation
- Encouraging employees to continuously acquire and improve their knowledge, skills, and abilities (KSAs) through targeted training courses, management development programs, and professional certifications
- Establishing a solid and sustainable chain of knowledge linked through the entire management hierarchy to ensure adequate core knowledge competencies for all levels of employees in the organization
- Inviting human resource audits, special management reviews such as benefits auditing, and self-assessments periodically and proactively to ensure continuous improvement in human resource function
- Encouraging employees at all levels of the organization to think differently and radically (i.e., out-of-the-box thinking) at all times, which can lead to new perspectives providing best-of-breed solutions

- Participating in the succession-planning process for key positions
- Adhering to professional and ethical standards established by the relevant professional bodies
- Analyzing outside-in views (i.e., views of stakeholders about company management) and inside-out views (i.e., views of company management about stakeholders) to identify disconnections between these views and to integrate them in a coherent manner

9.3 WORLD-CLASS HUMAN RESOURCES MANAGEMENT

(a) HUMAN RESOURCES STRATEGY. Two principles are central to the human capital (human resources) idea. First, people are assets whose value can be enhanced through investment. As with any investment, the goal is to maximize value while managing risk. As the value of people increases, so does the performance capacity of the organization and, therefore, its value to clients/customers and other stakeholders. Second, an organization's human capital policies must be aligned so as to support the organization's shared vision—the mission, vision for the future, core values, goals, and strategies by which the organization has defined its direction and its expectations for itself and its people. All human capital policies and practices should be assessed by the standard of how well they help the organization pursue its shared vision.[2]

CRITICAL SUCCESS FACTORS FOR A WORLD-CLASS HUMAN RESOURCES FUNCTION

Critical success factors for a world-class human resources function include: acquisition and retention of human capital; policies, procedures, and standards; employee diversity management; employee training and development; employee empowerment; listening to stakeholder voices; leadership; organizational culture; customer service; organizational structure; technology; process; and people.

At most organizations, the lion's share of operating costs is devoted to the workforce. For this reason, employees traditionally have been viewed through the budgetary lens, and therefore they have often been seen as costs to be cut rather than as assets to be appreciated. However, high-performance organizations in both the private- and public sectors recognize that an organization's people largely determine its capacity to perform. Therefore, the value of the organization is dependent on the value of its people.

Enhancing the value of employees is a win-win goal for employers and employees alike. The more an organization recognizes the intrinsic value of each employee, the more it recognizes that this value can be enhanced with nurturing and investment, the more it recognizes that employees vary in their talents and motivations—and that a variety of incentive strategies and working arrangements can be created to enhance each employee's contributions to organizational performance—the more likely the organization will be to appreciate the diversity of employee needs and circumstances and to act in ways that will make sense in both business and human terms.

(b) LISTENING TO STAKEHOLDER VOICES. Human resources management, as a provider and overseer of employees for the company, should pay close attention in understanding and listening to the following "voices" to achieve organizational goals

and to improve overall performance. When these "voices" are heard together, they bring attention to new perspectives and creative conflicts, forcing new thinking that leads to new solutions (i.e., best-of-breed solutions). Listening to the collective voice of many stakeholders at once will have a greater impact than listening to one voice at a time in isolation, because the former requires a balanced approach after considering all party's concerns.

For each content of each voice, a T-Column analysis should be prepared with "what happens if I listen to this voice" in the left column (benefits) and "what happens if I don't listen to this voice" in the right column (costs and risks). A comparative analysis of each content in each column will point to new problems requiring new solutions.

- Voice of the customer (external customers such as suppliers, vendors, contractors, consultants, key customers, regulators, investors, creditors, the stock market, labor unions, and media/press, and internal customers such as the board of directors, corporate management, and employees in other functional departments, such as marketing, manufacturing, finance, and IT)
- Voice of the process (process flows, process variations, process delays and waste, and process inefficiencies)
- Voice of employees (employee suggestion program, employee complaints and grievances, employee attitude surveys, and employee exit interviews)
- Voice of quality (TQM principles and practices, mistake-proofing, continuous improvement, cost of poor quality, work teams and focus groups, quality assurance, quality control, quality audit, quality council, and quality circles)
- Voice of standards (standards in hiring, training, benefits, and education; internal/external benchmarks; ethical standards; and industry/organization standards)
- Voice of partners (insurance companies; electronic commerce vendors; training consultants, contractors, and institutions; private/public universities; corporate universities; job search firms; outplacement firms; and outsourcing vendors
- Voice of regulators (federal, state, and local laws and regulations)
- Voice of competitors (press releases, Web site pressrooms, industry magazines, daily business newspapers, advertising magazines, industry trade shows, product demonstrations and promotions, direct mail, e-mail campaigns, copyright/trademark/patent news, business intelligence news, banner advertising, billboard and street advertising, product sponsorships, and online events and chat rooms)

(c) HUMAN-RESOURCES CYCLE TIME MEASURES. Cycle time reduction in HR deals with improving the employee hiring-to-rehiring cycle, with associated benefits such as increased performance and productivity, improved utilization of human and machine resources, decreased costs, and improved internal customer service. To attain these benefits, organizations must:

- Eliminate or decrease non-value-added activities (e.g., paper-driven tasks; unnecessary handoffs; rework steps; waiting time; and delays at the interdepartmental and interdivisional boundaries and at the intradepartmental work stations).
- Enhance or increase value-added activities (e.g., job application process time; job performance tests; new employee orientation time; employee performance appraisal time; employee counseling time; employee attitude surveys; employee

exit time; use of automated systems; negotiating points between labor unions and organization management; internal/external customer access points to HR systems; HR project hold points; and HR management decision points and control points).

This requires placing the right employees with the right skills in the right jobs throughout the organization so that delays and waste in HR operations are decreased.

HR cycle times can be decreased with the use of automated workforce management systems that handle various activities within the cycle, such as employee hiring, job assignment and scheduling, training and development, performance appraisals and feedback, career progression, and exit interviews.

Some examples of HR cycle time measures include:

- Time elapsed between job (position) analysis studies. Job analysis study is conducted for a specific job function, a group of jobs, or for an entire department, division, or company. The longer the time elapsed, the less current a job description becomes, thus leading to waste of human talent and poor job performance. There could be a mismatch between employee skills and job requirements thus not realizing the full potential of employees.
- Time elapsed between human capital–forecasting periods. Human capital forecasting is performed to ascertain the supply of and demand for employees. The longer the time elapsed, the less the match between demand for and supply of employees.
- Time elapsed between employee performance appraisal and performance feedback to employees. The longer the time elapsed, the greater the employee frustration and the greater the disconnect between employee performance and rewards (e.g., pay increase, bonus, and promotion).
- Time elapsed between a job opening and job filling. The longer the time elapsed, the greater the reflection of inefficient internal HR processes in recruiting and hiring.
- Time elapsed between employee succession plans. The longer the time elapsed, the less retention of talented employees and the less readiness on the part of the pool of qualified employees who can be moved into higher jobs as needed

(d) HUMAN RESOURCES METRICS. Some examples of HR metrics to improve employee performance and to increase productivity include:

- Yield ratios for each recruiting source (e.g., universities, newspapers, and job search firms). The yield ratio is the percentage of job applicants who successfully move from one stage of the recruitment and selection process to the next. These stages include resumes received, first interviews requested, final interviews requested, job offers made, and job offers accepted. The higher the yield ratio, the greater the reflection of HR management efforts and the better indication of the quality of a recruiting source.
- Percentage reduction in employee turnover rates by job title, job function, department, or division

- Percentage reduction in total employee costs (wages and benefits) as a percentage of revenues, sales, or profits
- Percentage increase in employee training and development cost as a percentage of revenues, sales, or profits

9.4 CONDUCTING A SELF-ASSESSMENT OF HUMAN CAPITAL PROGRAM

(a) BENEFITS. Self-assessment is the starting point for creating human capital organizations that focus on valuing employees and aligning their people policies to support organizational performance goals.[3]

Another advantage to doing a human capital self-assessment is that it will help organization leaders understand the strengths and limitations of their human capital data systems. Any self-assessment should be based—to the extent possible—on valid and reliable data regarding such matters as hiring, employee diversity, retention, promotions, succession cycles, and performance incentives. These data can help the organization produce a profile of its human capital, providing useful historical and prospective views. Doing a human capital self-assessment will give organization leaders an idea of the adequacy of the data being collected and of the gaps that may need to be filled.

(b) FRAMEWORK. A five-part framework is provided for conducting a self-assessment of human capital policies and practices: strategic planning, organizational alignment, leadership, human talent, and performance culture.

(i) Part 1: Strategic Planning: Establish the Organization's Mission, Vision for the Future, Core Values, Goals, and Strategies. High-performance organizations begin by defining what they want to accomplish and what kind of organization they want to be. They define a shared vision—a mission, a vision for the future, core values, goals, and strategies—and communicate that shared vision clearly, constantly, and consistently. The organization's shared vision provides the standard for assessing the appropriateness and effectiveness of everything the organization does. The organization should develop strategies to enhance the value of its employees and focus their efforts on the organization's shared vision. The effect should be in the best collective interests of employer and employee alike: the organization's capacity to achieve its shared vision will increase, while its employees will benefit from the incentives—tangible and intangible—of working for a high-performance organization.

Organizations should do the following:

- Develop and communicate a shared vision.
- Create a coherent human capital strategy containing policies, programs, and practices.
- Integrate the human capital strategy with the organization's overall strategic planning.
- Develop a HR information system to provide relevant and reliable data for fact-based decision-making on human capital.

(ii) Part 2: Organizational Alignment: Integrate Human Capital Strategies with the Organization's Core Business Practices. High-performance organizations choose the best strategies for integrating their organizational components, activities, core processes, and resources to support mission accomplishment. This requires workforce planning that is explicitly linked to the organization's shared vision. It also requires that the "personnel" or "human resources (HR)" function, as it traditionally has been called, be given an integral place in the top management team. Human capital professionals must have the knowledge and skills to provide effective mission support and to participate as partners with line managers and staff in developing and implementing human capital approaches. Further, line managers who may eventually be given greater decision-making authority in the human capital area must be sufficiently prepared and trained now to be accountable for their decisions.

Organizations should do the following:

- Link the workforce-planning efforts to the organization's strategic and program planning efforts.
- Identify current and future human capital needs, including the size of the workforce, its deployment across the organization, and the knowledge, skills, and abilities (KSAs) needed for the organization to pursue its shared vision.
- Ensure that the human capital function is appropriately staffed both in numbers and competencies.
- Maintain a ratio of human capital staff to line employees.
- Develop a skills inventory system identifying current and future skills needs and gaps, and including information on skills by demographic cohort. The skills inventory should support employee roles and core competencies.
- Collect data on distribution of employees by pay level, attrition rates, retirement rates, and projected eligibility for promotion pay level, and ratios of managers to employees.
- Conduct industry benchmarks in such areas as skills, education level, and demographic trends.

(iii) Part 3: Leadership: Foster a Committed Leadership Team and Provide Continuity Through Succession Planning. A committed senior leadership team is essential to fostering an organization's shared vision, aligning organizational components so that the organization can best pursue this vision, and building a commitment to the vision at all levels of the organization. To become a high-performance organization, an organization needs senior leaders who are drivers of continuous improvement and whose styles and substance are in accord with the way the organization sees its mission and its own character. To create a workforce that shares this vision and is aware of the contribution that each employee can and must make toward achieving it, the organization's senior leaders must work as a team to convey a clear and consistent portrayal of this vision throughout the organization through their words and deeds and the example they set. Since these goals can take years to achieve, the organization must have a succession-planning strategy that ensures a sustained commitment and continuity of leadership even as individual leaders arrive or depart.

Organizations should do the following:

- Define roles, responsibilities, attributes, and competencies of senior leaders, including performance expectations.
- Pursue an explicit strategy to build teamwork.
- Communicate the organization's shared vision in clear and consistent terms to all levels of the organization, and receive feedback from employees (i.e., new, current, and exiting employees) through focus groups and employee surveys.
- Ensure continuity of leadership through executive succession planning.
- Develop metrics on attrition rates, retirement eligibility, and retirement rates for executives.
- Develop an active executive development program, including mentoring and shadowing, with planned developmental opportunities, learning experiences, and feedback from executive candidates.

(iv) Part 4: Talent: Recruit, Hire, Develop, and Retain Employees with the Skills for Mission Accomplishment. A high-performance organization demands a dynamic, results-oriented workforce with the talents, multidisciplinary knowledge, and up-to-date skills needed to enhance the organization's value to its clients and customers, and to ensure that it is equipped to achieve its mission. Because mission requirements, client/customer demands, technologies, and other environmental influences (e.g., laws and regulations) change rapidly, a performance-based organization must continually monitor its talent needs. It must be alert to the changing characteristics of the labor market. It must identify the best strategies for filling its talent needs through recruiting and hiring and follow up with the appropriate investments to develop and retain the best possible workforce. Its compensation and benefits programs, workplace facilities, and work/family arrangements should be viewed from the perspective of how well they help the organization compete for and retain the best talent available and then get the best mission performance from that talent.

In addition, this talent must be continuously developed through education, training, and opportunities for continued growth. The organization must match the right people to the right jobs and, in the face of finite resources, be prepared to employ matrix management principles, maintaining flexibility to redeploy human capital and realigning organizational structures and work processes to maximize economy, efficiency, and effectiveness. Organizational structures and work arrangements must be fashioned to avoid stovepiping (or siloing) and draw upon the strengths of the various organizational components. Cross-functional teams—including just in time (JIT) teams and virtual teams, whose members may not work in the same physical location—can be used as a flexible means of focusing talent on specific tasks.

Organizations should do the following:

- Develop a recruiting and hiring strategy that is targeted to fill short- and long-term human capital needs and, specifically, to fill gaps identified through its workforce-planning efforts.
- Invest in education, training, and other developmental opportunities to help employees build the competencies needed to achieve the organization's shared vision.

- Ensure that the deployment of the organization's workforce is appropriate to mission accomplishment and keyed to efficient, effective, and economic operations.

(v) Part 5: Performance Culture: Enable and Motivate Performance while Ensuring Accountability and Fairness for All Employees. High-performance organizations foster a work environment in which people are enabled and motivated to contribute to continuous learning and improvement and mission accomplishment, an environment that fosters accountability and fairness for all employees. A high-performance organization's approach to its workforce is inclusive and draws on the strengths of employees at all levels and of all backgrounds. It maintains a workforce in which honest two-way communications and fairness are a hallmark, perceptions of unfairness are minimized, and workplace disputes are resolved by fair and efficient means.

High-performance organizations also have a holistic view of employees as key stakeholders, realizing that a variety of services, facilities, activities, and opportunities can be meaningful to employees and enhance their loyalty and commitment. A commitment to continuous learning and improvement can help an organization to not only respond to change, but to anticipate change, create new opportunities for itself, and pursue a shared vision that is ambitious and achievable.

Incentives are particularly important in steering the workforce; they must be results-oriented, client-based, customer-based, realistic, and subject to balanced measures that reveal the multiple dimensions of performance. Incentives should be part of a performance management system under which employees' performance expectations are aligned with the organization's mission, a system in which personal accountability for performance is reinforced by both rewards and consequences. Because organizations are increasingly technology-driven and knowledge-based, high-performing organizations ensure that their employees have the right information technology (IT) resources to do their work and to gather and share information.

Organizations should do the following:

- Design a performance management system to steer the workforce toward embodying and effectively pursuing the organization's shared vision.
  - Consider explicit performance-based rewards and consequences.
  - Provide ratings and feedback that meaningfully differentiate between performers and nonperformers.
  - Ensure that nonperformers are held accountable for their actions or nonactions.
  - Support managers and supervisors who give employees frank and constructive feedback on employee performance and who take performance-related actions where appropriate.
  - Seek feedback from managers/supervisors and employees on the meaningfulness and effectiveness of the performance management system and its return on investment.
- Make sure that any performance incentives operating at the organizational, team, or individual levels are meaningful to supporting the performance management system.
  - Link performance incentives to the performance management system to enable balanced measures that reveal the multiple dimensions of performance.

  - Seek feedback from managers/supervisors and employees on the equity, adequacy, and effectiveness of the performance incentive system.
  - Collect data on the organization's investments in bonuses, spot awards, and other tangible incentives over time to benchmark against high-performance organizations with similar missions and circumstances.
- Encourage and motivate employees to contribute to a continuous learning and improvement process.
  - Provide training and mentoring programs specifically aimed at promoting continuous learning and improvement.
  - Encourage employees to contribute their views on the shared vision and how to achieve it, including innovative ideas and process improvement through the use of employee suggestion system or other means.
  - Obtain feedback from employees on their perceptions of the organization.
  - Benchmark against high-performance organizations as part of a continuous scan of the environment.
- Develop managers and supervisors who help steer the workforce toward the pursuit of the organization's shared vision.
  - Train managers and supervisors in employee selections, promotions, and performance evaluations.
  - Provide specific training in the legal responsibilities of supervisors and in "people skills," such as employee motivation and conflict avoidance and resolution.
  - Obtain feedback from employees, including 360-degree appraisals, on the extent to which managers and supervisors show leadership in support of the organization's shared vision and in motivating and enabling all employees to pursue it.
- Tailor the organizational structures, job processes, workplace facilities, tools, work arrangements, and other resources and opportunities to help employees effectively, economically, and efficiently pursue their work.
  - Focus on organizational structures (flat vs. tall), core business processes, contracting decisions, resource allocations, and flexible working arrangements with the goal of improving mission accomplishment.
- Help employees with IT to perform their work better and to gather and share knowledge and information.
  - Obtain feedback from employees that they have the opportunity, incentives, support, and training to make the appropriate use of IT to do their work and to acquire and share knowledge.
  - Collect data on the organization's investments in IT over time and analyze return on these investments in terms of economy, efficiency, and service delivery; and do benchmark against organizations with similar missions, tasks, and service requirements.
- Maintain an environment characterized by inclusiveness and diversity of styles and personal backgrounds and that is responsive to the needs of diverse groups of employees.

  - Develop a written diversity policy or discussion of diversity in the organization's human capital plan or other documents.
  - Train staff and employees in team building and conflict avoidance and resolution methods.
  - Obtain employee feedback on the tolerance and encouragement of diverse styles and personal backgrounds in the workplace and on perceptions of unequal treatment.
  - Collect statistics on employee grievances and equal employment opportunity (EEO) complaints and findings over time.
- Maintain a workable relation between the organization's workforce and unions and its management to achieve the organization's shared vision.
  - Obtain feedback from employees on their commitment to the organization's shared vision and their views of management's efforts at communication and coordination.
  - Obtain feedback from union representatives with collective bargaining agreements, managers, and other employees on the extent to which they are in mutual agreement over the organization's shared vision and the means of achieving it.

9.5 MAJOR PRINCIPLES AND BEST PRACTICES OF HUMAN CAPITAL

The people that define organizations' character and capacity to perform—their human capital—are also the foundation for achieving high performance. The human capital idea centers on viewing people as assets whose value to an organization can be enhanced through investment. As with any investment, an organization's goal is to maximize the value of its people to increase organizational performance capacity, and thus the organization's value to clients, customers, and other stakeholders, while managing the related costs and risks. The following ten major principles and practices of human capital management demonstrate that leading organizations views human capital as the foundation for their ongoing success and viability. Giving top priority to implementing these principles and practices leads to a better, performance-based management system, with resulting success and higher performance.[4]

(a) TREAT HUMAN CAPITAL MANAGEMENT AS BEING FUNDAMENTAL TO STRATEGIC BUSINESS MANAGEMENT. Integrate human capital considerations when identifying the mission, strategic goals, and core values of the organization, as well as when designing and implementing operational policies, procedures, and practices.

Human capital issues are of strategic importance to overall business management because organizations are able to achieve high performance through recruiting, hiring, developing, and retaining employees who have the specific KSAs and behaviors needed to support missions and goals.

Organizations should do the following:

- Include language on the importance of human capital as part of corporate mission.
- Include human capital goals in strategic plans.
- Adopt core value and management models that incorporate human capital and strategic business management.

(b) INTEGRATE HUMAN-CAPITAL FUNCTIONAL STAFF INTO MANAGEMENT TEAMS. Include human capital (human resources) leaders as full members of the top management team rather than isolating them to provide after-the-fact support. Expand the strategic role of human capital staff beyond providing traditional personnel administrative services.

Human capital staff must assume greater responsibility beyond providing personnel administrative services. They should participate in management teams as full members and ensure that these teams proactively address human capital issues. By acting in this capacity, the human capital staff can directly contribute to the development of a pool of employees who are capable and motivated to accomplish the organizations' missions and goals.

Organizations should do the following:

- Involve human capital executives, managers, and staff as decision makers and internal consultants by having them (1) serve on senior-executive planning committees, (2) consult directly with line managers regarding specific human capital strategies, and/or (3) offer expert advice via centralized human capital offices or Intranet sites.

(c) LEVERAGE THE INTERNAL HUMAN CAPITAL FUNCTION WITH EXTERNAL EXPERTISE. Supplement internal human capital staff's knowledge and skills by seeking outside expertise from consultants, professional associations, and other organizations, as needed.

Organizations should do the following:

- Leverage the KSAs of their human capital staff by seeking outside expertise from consultants, professional associations, and other organizations.
- Outside experts should provide the following:
  - Provide cost-efficient and specialized expertise on an as-needed basis.
  - Introduce a fresh perspective to addressing the organizations' human capital challenges.
  - Allow the organization to benchmark their human capital policies and practices against those of other organizations.
  - Ensure confidentiality when obtaining employees' input on human capital issues through surveys, focus groups, and questionnaires.

(d) HIRE, DEVELOP, AND SUSTAIN LEADERS ACCORDING TO LEADERSHIP CHARACTERISTICS IDENTIFIED AS ESSENTIAL TO ACHIEVING SPECIFIC MISSIONS AND GOALS. Identify the leadership traits needed to achieve high performance of mission and goals, and build and sustain the organization's pool of leaders through recruitment, hiring, development, retention, and succession policies and practices targeted at producing leaders with the identified characteristics. These characteristics are specific to each organization to maintain its competitive advantage.

Organizations should do the following:

- Establish central training sites or corporate universities that provide training specifically targeted at assessing, developing, and maintaining those leadership characteristics among current and future leaders.

(e) COMMUNICATE A SHARED VISION THAT ALL EMPLOYEES, WORKING AS ONE TEAM, CAN STRIVE TO ACCOMPLISH. Promote a common understanding of the mission, strategic goals, and core values that all employees, working as a team, are directed to achieve. Create a line of sight between individual contributions and the organization's performance and results.

Organizations should do the following:

- Communicate a consistent vision about the organizations' missions, goals, and core values to all employees. This shared or common understanding should help employees in knowing how their individual and combined efforts will contribute to the organization's overall results and successes.
- Use several communications formats to build organizational teamwork, including formats that encourage or enable a two-way communication between leaders and employees, and to create a line of sight between employees' efforts and their organizations' outcomes.

(f) HIRE, DEVELOP, AND RETAIN EMPLOYEES ACCORDING TO COMPETENCIES. Identify the competencies—KSAs and behaviors—needed to achieve high performance of mission and goals, and build and sustain the organization's talent pool through recruitment, hiring, development, and retention policies and practices targeted at building and sustaining those competencies.

Organizations should do the following:

- Implement human capital policies and practices designed to competitively hire, develop, and retain employees with the desired competencies within their industry and market locations.

(g) USE PERFORMANCE MANAGEMENT SYSTEMS, INCLUDING PAY AND OTHER MEANINGFUL INCENTIVES, TO LINK PERFORMANCE TO RESULTS. Provide incentives and hold employees accountable for contributing to the achievement of mission and goals. Reward those employees who meet or exceed clearly defined and transparent standards of high performance.

Organizations should do the following:

- Implement incentive policies and programs such as pay for performance, profit sharing, variable pay, and/or some combination of these approaches.
- Balance the pay and incentive programs to encourage both individual and team-based high performance.

Organizations should not do the following:

- Rely on cash incentives. The reasons are that (1) cash incentives promote internal competition at the expense of organizational teamwork, and (2) employees might view extra cash payments as entitlements rather than rewards for exceptional performance.

(h) SUPPORT AND REWARD TEAMS TO ACHIEVE HIGH PERFORMANCE. Foster a culture in which individuals interact and support and learn from each other as a means of contributing to the high performance of their peers, business units, and the organization as a whole. Bring together the right people equipped with the right competencies to achieve high performance as a result of, rather than in spite of, the organizational structure.

Organizations should do the following:

- Implement a variety of mechanisms to promote doing work as teams, including the use of cross-functional (or matrixed) teams to address strategic goals or customer-specific needs, and team-based incentives and reward programs.

(i) INTEGRATE EMPLOYEE INPUT INTO THE DESIGN AND IMPLEMENTATION OF HUMAN CAPITAL POLICIES AND PRACTICES. Incorporate the first-hand knowledge and insights of employees and employee groups to develop responsive human capital policies and practices. Empower employees by making them stakeholders in the development of solutions and new methods of promoting and achieving high performance of organizational missions and goals.

Organizations should do the following:

- Collect employees' input using employee satisfaction surveys, convening focus groups, and/or including employees on task forces.
- Draw on employees' front-line knowledge of work processes and customer needs to provide better customer service.
- Empower employees to contribute constructive ideas for improvement to the organizations' existing human capital policies and practices. Employee empowerment emphasizes the importance of giving employees the ability and the responsibility to take active steps to identify problems in the working environment that affect quality or customer service and to deal effectively with these problems. Participatory management style is required on the part of middle or senior management. This includes soliciting employee input on improving operations (e.g., through sponsoring employee suggestion programs, conducting brainstorming sessions with employees, and managing by walking around) and encouraging middle managers to discuss operational issues with their employees on a frequent basis.
- Facilitate self-managed teams. Teams are needed as a basic building block to empower employees. Problems are solved as a group. As both employees and managers gain confidence in employees' abilities to identify problems and develop solutions, management can increase employee empowerment by establishing natural work groups and self-managed teams. These longer-term, function-based teams are empowered to make (1) ongoing improvements to work processes without first seeking the approval of a supervisor, and (2) supervisory-level decisions on work planning and staff utilization.

(j) MEASURE THE EFFECTIVENESS OF HUMAN CAPITAL POLICIES AND PRACTICES. Evaluate and make fact-based decisions on whether human capital policies and practices support high performance of mission and goals. Identify the performance return on human capital investments.

Organizations should do the following:

- Measure the effectiveness of human capital policies and practices using a wide variety of approaches and indicators.
- Use fact-based measures by which to judge not only bottom-line results (profits) but also the success of specific human capital strategies and practices.
- Use measures to hold managers accountable for designing and implementing human capital strategies that support the organizations' missions and goals.
- Collect the following quantifiable data to develop and monitor human resource performance metrics:
    - Size and shape of the workforce, including, but not limited to: the distribution of employees by pay level, attrition rates, retirement rates and projected eligibility for promotion by employee pay level, and ratio of managers to employees
    - Attrition rates, retirement rates, and projected retirement eligibility of managers and executives
    - Skills inventory, including, but not limited to: current and potential gaps in skills, distribution of skills by demographic cohort, and level of education of the workforce
    - Data on the dispersal of performance appraisal ratings, such as the mean, mode, and standard deviation of scores
    - Average time required to fill job/position vacancies
    - Acceptance rates among job candidates to whom jobs/positions are offered
    - Data on the number, size, and costs of bonuses, incentives, and other awards
    - Data from employee satisfaction surveys and focus groups
    - Data from exit interviews
    - Statistics on employee grievances, equal employment opportunity (EEO) complaints, and findings over time
    - Number of cases handled and/or resolved via alternative dispute-resolution programs
    - The organization's total human capital cost in dollars and as a percentage of total operating budget
    - Percentage of operating budget spent on recruitment
    - Costs of promotions, grade increases, and within grade increases
    - Percentage of operating budget spent on employee training and development programs and the amount per employee
    - IT expenses related to human capital, such as computer and equipment costs, contractor support, software upgrades, and employee training in systems

9.6 APPLICABLE LAWS, REGULATIONS, STANDARDS, AND PRINCIPLES

Organizations have a legal and ethical obligation to comply with the various federal, state, and local laws, regulations, circulars and bulletins, directives and executive orders, government orders, and ordinances pertinent to a specific business area. Noncompliance with these laws and regulations can lead to fines, civil and/or criminal penalties, probation, and jail punishments (prison time), thus creating reputation (image) risk. Compliance with

industry and/or organization standards, including professional standards, can increase the quality of products and services, which, in turn, can enhance an organization's reputation and image in the marketplace.

A brief roundup of information about major laws, regulations, and standards is provided here as a reminder for checklist purpose. Note that these laws and regulations are subject to change as new ones are added and existing ones are amended or repealed. The reader is advised to obtain the original laws, regulations, and standards from the official sources for a better understanding of the provisions, requirements, and conditions of the laws, regulations, and standards (www.regulations.gov). Although some of the following laws, regulations, and standards directly affect public sector organizations (i.e., government agencies), private-sector organizations can read, learn, and apply them to improve their business operations on a proactive basis.

U.S. organizations should comply with the following laws, regulations, standards, and principles pertinent to human resources management:

Affirmative Action Plans. Executive Orders 11246, 11375, and 11478 address affirmative action plans requiring federal government contractors to develop and implement a formal written plan for an employer with at least 50 employees and over $50,000 government contracts. The U.S. Secretary of Labor was given the power to cancel the contract of a noncomplying contractor or blacklist a noncomplying employer from future government contracts.

Age Discrimination in Employment Act. The Age Discrimination in Employment Act (ADEA) of 1967, amended in 1978, 1986, and 1991, makes it illegal for an employer to discriminate in compensation, terms, conditions, or privileges of employment because of an individual's age. There is no mandatory retirement age. The Act applies to all individuals above the age of 40 working for employers having 20 or more workers. However, the Act does not apply if age is a job-related occupational qualification.

Americans with Disabilities Act. The Americans with Disabilities Act (ADA), enforced by the Equal Employment Opportunity Commission (EEOC), was passed in 1990 to stop discrimination against individuals with disabilities. The Act applies to all employers (i.e., private employers, employment agencies, labor unions, and state and local governments) with 15 or more employees. Major requirements of the ADA include the following:

1. Discrimination is prohibited against individuals with disabilities who can perform a job's essential functions.
2. A covered employer must have reasonable accommodation for persons with disabilities so that they can function as employees, unless undue hardship would be placed on the employer.
3. Preemployment medical examinations are prohibited except after an employment offer is made, conditional upon individuals passing a physical examination.
4. Federal contractors and subcontractors with contracts valued at more than $2,500 must take affirmative action to hire qualified disabled individuals.

Civil Rights Act of 1964, Title VII. The Civil Rights Act of 1964, enforced by the EEOC, was passed in part to bring about equality in all employment-related decisions.

The Act covers most employers in the United States, such as private employers, educational institutions, state and local governments, employment agencies, and labor unions.

Civil Rights Act of 1991. The Civil Rights Act of 1991 requires employers to show that an employment practice is job-related for the position and is consistent with business necessity. Major provisions of the Act include race norming, international employees, and government employee rights.

Civil Service Reform Act. The Civil Service Reform Act of 1978 covers federal government dealing with unions. The Act also identifies areas that are and are not subject to bargaining. For example, wages and benefits are not subject to bargaining. Instead they are set by congressional actions.

Consolidated Omnibus Budget Reconciliation Act. The Consolidated Omnibus Budget Reconciliation Act (COBRA) requires that most employers (except churches and the federal government) with 20 or more employees offer extended health-care coverage to (1) employees who voluntarily quit, (2) widowed or divorced spouses and dependent children of former or current employees, and (3) retirees and their spouses whose health-care coverage ends.

Davis-Bacon Act. The Davis-Bacon Act of 1931 affects compensation paid by firms engaged in federal construction projects valued in excess of $2,000 and requires that the prevailing wage rate be paid on all federal construction projects.

The Walsh-Healy Public Contracts Act and the McNamara-O'Hara Service Contract Act of 1965 also applies to government contractors, similarly to the Davis-Bacon Act. These two acts require firms with federal supply or service contracts exceeding $10,000 to pay a prevailing wage rate.

Drug-Free Workplace Act. The Drug-Free Workplace Act of 1988 requires government contractors to take steps to eliminate employee drug usage. Failure to do so can lead to contract termination. Use of tobacco and alcohol are not considered controlled substances, and off-the-job drug use is not included in the Act. State laws mainly govern private employers.

Electronic Communications Privacy Act. The Electronic Communications Privacy Act applies to employer monitoring of employees' communications such as electronic mail and voice mail. The Act requires that at least one party to the electronic communication must have provided consent, but that employers can use electronic monitoring (e.g., eavesdropping) of employee's communications as part of the ordinary course of business.

Employee Polygraph Protection Act. The Employee Polygraph Protection Act bars most employers from using polygraphs for preemployment screening. However, federal, state, and local government agencies and certain private companies (e.g., security and pharmaceutical) are exempt. The Act does allow employers to continue to use polygraphs as part of internal investigations of theft or losses. But the polygraph test should be taken voluntarily, and the employee can stop the test at any time.

Employee Retirement Income Security Act. The purpose of the Employee Retirement Income Security Act (ERISA) of 1974 is to regulate private pension plans in order to assure that employees who put money into them, or who depend on a pension for retirement funds actually, will receive the money when they retire.

Foreign Corrupt Practices Act. The Foreign Corrupt Practices Act (FCPA) of 1977 prohibits U.S. firms from engaging in bribery in foreign countries. A fine line exists between paying agent-fees and gifts, which are legal, and bribery, which is illegal.

Fair Labor Standards Act. The Fair Labor Standards Act (FLSA) was passed in 1938 to cover compensation for private- and public-sector employees. The Act establishes a minimum wage, discourages oppressive use of child labor, and encourages limits on the number of weekly hours employees can work through overtime provisions.

Equal Pay Act. The Equal Pay Act was passed in 1963 as a major amendment to the FLSA. The Act focuses on wage discrimination on the basis of sex and prohibits having different wage scales for men and women performing substantially the same jobs.

Family and Medical Leave Act. The Family and Medical Leave Act (FMLA) of 1993 covers all employers with 50 or more employees who live within 75 miles of the workplace. It includes federal, state, and private employers. Only employees who have worked at least 12 months and 1,250 hours in the previous year are eligible for leave under the Act. The Act requires that employers allow eligible employees to take a total of 12 weeks' leave during any 12-month period for one or more of the following situations: (1) birth, adoption, or foster-care placement of a child, (2) caring for a spouse, child, or parent with a serious health condition, or (3) a serious health condition on the part of the employee. The Act allows 12 weeks of family leave without pay and requires that employees taking family leave be allowed to return to their jobs. The FMLA applies to both men and women, while the Pregnancy Discrimination Act (PDA) applies to women only.

Health Insurance Portability and Accountability Act. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 allows employees to switch their health insurance plan from one employer to another to get the new health coverage, regardless of preexisting health conditions. The Act prohibits group insurance plans from dropping coverage for a sick employee and requires them to make individual coverage available to employees who leave group plans.

Immigration Reform and Control Act. The Immigration and Reform and Control Act (IRCA) of 1986 makes it illegal for an employer to discriminate in recruiting, hiring, or terminating based on an individual's national origin or citizenship. The Act penalizes employers who knowingly hire illegal aliens, and establishes minimum documentation requirements for all new employees.

Occupational Safety and Health Act. The Occupational Safety and Health Act (OSHA) of 1970 was passed to ensure safe and healthful working conditions for every working man or woman. Every employer engaged in commerce who has one or more employees is covered by the Act. Farmers having fewer than ten employees are exempt. Federal, state, and local government employees and coal-mining employees are covered under different provisions or statutes.

Older Workers Benefit Protection Act. The Older Workers Benefit Protection Act (OWBPA) of 1990 was passed to amend the ADEA of 1967 to ensure equal treatment for older workers who are in early-retirement (e.g., buyouts) or severance situations.

The OWBPA specifies that employees considering an early-retirement buyout enhancement must:

1. Receive copies of any waiver of their rights to sue for age discrimination
2. Be given sufficient time to consider the buyout offer, most frequently up to 45 days if they must sign a waiver of age discrimination rights
3. Be able to revoke their retirement agreement within seven days of signing the waiver

Pregnancy Discrimination Act. The Pregnancy Discrimination Act (PDA) of 1978 requires that any employer with 15 or more employees must treat maternity leave the same as other personal or medical leaves. The PDA is closely related to FMLA, although the former applies only to women and the latter applies to both men and women.

Privacy Act. The Privacy Act of 1974 was intended to protect the privacy of personal information and applies to both private- and public-sector organizations. The Act requires an organization to have a signed release from a person before it can give information about that person to someone else.

Retirement Equity Act. The Retirement Equity Act was passed in 1984 as an amendment to ERISA. The measure liberalized pension regulations affecting women and lowered the vesting age while guaranteeing access to benefits and prohibiting pension-related penalties due to absences from work such as maternity leave.

Sherman Antitrust Act. The Sherman Antitrust Act, with various provisions, prohibits employers from sharing wage data with each other or taking other steps to artificially hold down wages.

Social Security Act. The Social Security Act of 1935 was established to provide old age, survivors', disability, and retirement benefits to previously employed workers. Employers and employees share in the cost of social security through a tax on employees' wages or salaries.

Vietnam-Era Veterans' Readjustment Act. The Vietnam-Era Veterans' Readjustment Act of 1974 requires that affirmative action in hiring and advancing Vietnam-era veterans be undertaken by federal contractors and subcontractors having contracts of $10,000 or more.

Uniformed Services Employment and Reemployment Rights Act. The Uniformed Services Employment and Reemployment Rights Act of 1994 requires employees to notify their employers of military service obligations. Employees serving in the military must be provided leaves of absence and have reemployment rights valid for up to five years.

Wagner Act. The Wagner Act of 1935 (also known as the National Labor Relations Act) was passed to encourage collective bargaining power for unions and to provide job security for union members. The Act helped unions to grow and prohibits employers from undertaking unfair labor practices, and hence it is known as a pro-union measure.

Taft-Hartley Act. The Taft-Hartley Act of 1947 (also known as the Labor-Management Relations Act) was passed to provide a balance to the power of unions, so it was considered pro-management. The Act was designed to offset the pro-union Wagner Act by limiting unions' actions. Union practices such as coercion, discrimination against nonmembers, refusal to bargain, and excessive membership fees are forbidden.

Landrum-Griffin Act. The Landrum-Griffin Act of 1959 (also known as Labor-Management Reporting and Disclosure Act) was passed to protect the rights of individual union members against union corruption. The Act requires unions to have bylaws, financial reports, and a bill of rights, and it mandates that the Secretary of Labor will act as a watchdog of union conduct. The Act ensures that the federal government protects the democratic rights of union members.

National Labor Relations Board. Two major functions of the National Labor Relations Board (NLRB) are to conduct and certify labor-union representation elections and to prevent unfair labor practices. NLRB enforces the Wagner Act, Taft-Hartley Act, and Landrum-Griffin Act (collectively called the National Labor Code) because each Act was passed to focus on some aspect of the relationships between labor unions and company management.

Norris-Laguardia Act. The Norris-Laguardia Act of 1932 was passed to guarantee workers some rights to organize and to restrict the issuance of court injunction in labor disputes.

Railway Labor Act. The Railway Labor Act of 1926 was passed to give railroad employees the right to organize and bargain collectively through representation.

Worker Adjustment and Retraining Notification. The Worker Adjustment and Retraining Notification (WARN) Act requires employers to give 60 days' notice before a layoff or facility closing that involves more than 50 employees. Part-time and seasonal employees are not counted toward the 50-employee rule.

Workforce Investment Partnership Act. The Workforce Investment Act (WIA) of 1998 supports employers who hire new workers, particularly workers who are among the long-term unemployed or who have been receiving welfare benefits. The Act also targets adult education, disadvantaged youth, and family literacy. Employers hiring and training individuals who meet the WIA criteria receive tax credits.

Voice of the Customer. "Voice of the customer" (VOC) means organizations should listen to and understand the external customers' needs, wants, and expectations (i.e., customers' voice) and provide products and services that truly meet such needs, wants, and expectations. The same thing applies to internal customers' needs (i.e., departments or functions within an organization).

Voice of the Process. "Voice of the process" means understanding and evaluating the nature of process flows, process variations, and process characteristics and capabilities for both products and services. The goal is to reduce the process variations in order to make the process stable and predictable and to reduce cycle time.

New work processes must be designed to reduce the cycle time by eliminating stop points, chokepoints, pain points, or fault points in a process that enjoys the support and availability of resources such as tools, technology, people, equipment, and information. Existing work processes must be (1) streamlined by reviewing the upstream and downstream work steps, (2) simplified by removing unnecessary handoffs, stop points, chokepoints, pain points, or fault points, (3) standardized based on "lessons learned," and (4) institutionalized by being rolled out to the entire-organization.

Society for Human Resource Management. The Society for Human Resource Management (SHRM) is a professional organization and the voice of the human-resources management profession. It establishes professional certifications (PHR, SPHR, and

GPHR), professional standards, and a code of ethics for human resource managers to follow. PHR is Professional in Human Resources, SPHR is Senior Professional in Human Resources, and GPHR is Global Professional in Human Resources (www.shrm.org).

Additional Resources

Baron, James N., and David M. Kreps. *Strategic Human Resources: Frameworks for General Managers*. Hoboken, NJ: John Wiley & Sons, 1999.

DeCenzo, David A., and Stephen P. Robbins. *Fundamentals of Human Resource Management*, ninth edition. Hoboken, NJ: John Wiley & Sons, 2006.

Hussey, David. *Business Driven HRM: A Best Practice Blueprint*. Hoboken, NJ: John Wiley & Sons, 2002.

Hyter, Michael C., Judith L. Turnock, and James Kitts. *The Power of Inclusion: Unlock the Potential and Productivity of Your Workforce*. Hoboken, NJ: Wiley & Sons, 2006.

Notes

1. U.S. General Accounting Office, *Human Capital: A Self-Assessment Checklist for Agency Leaders* (GAO/GGD-99-179), Washington, DC: Sept. 1999.
2. *Id*.
3. *Id*.
4. GAO, *Human Capital: Key Principles from Nine Private Sector Organizations* (GAO/GGD-00-28), Washington, DC: Jan. 2000.

CHAPTER 10

ACCOUNTING, TREASURY, AND FINANCE-MANAGEMENT BEST PRACTICES

10.1 OVERVIEW

The focus of accounting, treasury, and finance functions (hereafter called finance function) historically has centered on oversight and control, concentrating on the function's fiduciary responsibilities and paying less attention to increasing the effectiveness of operating divisions. However, over the past decade, dramatic changes in the business environment have driven finance function to reevaluate this role. Increased competition resulting from an emerging global market has put pressure on finance function to find new ways to reduce administrative costs, add value, and provide a competitive advantage. At the same time, advances in information technology (IT) have made it possible for the finance function to shift from a paper-driven, labor intensive, clerical role to a more consultative role as adviser, strategist, analyst, and business partner.[1]

10.2 ROLES AND RESPONSIBILITIES OF CONTROLLER, TREASURER, AND CHIEF FINANCIAL OFFICER

(a) MAJOR ROLES AND RESPONSIBILITIES. The *Controller* or *the Chief Accounting Officer* is usually responsible for financial accounting (e.g., billing, accounts payable, and payroll), general accounting (e.g., general ledger), cost accounting (e.g., inventory accounting and product/service costing), operating and capital budgeting, financial statement preparation, taxes, and coordination with internal auditors and external auditors. The controller reports to the chief financial officer.

The *Treasurer* is usually responsible for working-capital management (e.g., credit management, collection of accounts receivable, cash disbursements, and short-term borrowing and investing), external financing with banks and other financial institutions (e.g., long-term borrowing, leasing, and investor relations), risk management (e.g., interest rate risk and foreign-exchange-rate risk), insurance, pension funds, and dividend disbursement to investors. The treasurer reports to the chief financial officer.

The *Chief Financial Officer (CFO),* as a member of senior management, is usually responsible for both the accounting and treasury functions, and more besides. Both the controller and the treasurer report to the CFO, and the CFO, in turn, reports to the Chief Executive Officer (CEO). The CFO plays an important role in a firm's strategic planning, capital budgeting and investment decision-making process, stockholder relations, safeguarding of assets, financial statement analysis, and financial reporting.

The CFO is a key person in the C-level executive suite and has the following specific roles and responsibilities:

- Being a team player, not a policeman. However, the custodial role of protecting the organization's assets is here to stay.
- Maximizing shareholder value through increasing revenues, decreasing costs, and increasing profits in a legitimate and ethical manner
- Integrating accounting, treasury, and finance activities for maximum efficiency and effectiveness
- Lowering total manufacturing costs, marketing costs, administrative and selling costs, and service costs in order to lower selling prices, increase sales volume, and increase profits
- Linking finance service costs to cash flows and gross profits
- Speeding up finance service deliveries to internal customers to achieve their total satisfaction
- Innovating new finance-service techniques and processes by leveraging technology to improve quality and reduce costs
- Eliminating non-value-added activities in finance services to trim waste and to lower costs
- Focusing more on value-added activities in finance services to provide a solid value to the customers and to the organization
- Identifying key drivers of cost, quality, risks, expenses, revenues, profits, business growth, competition, and performance; focusing on the root causes of these drivers and understand why these drivers go up and down.
- Seamlessly integrating the back-end systems with the front-end systems for (1) maximum data consistency, completeness, and accuracy, (2) better customer service and satisfaction, and (3) stronger connection of disparate and disconnected business processes
- Building standardized, transparent, and repeatable finance-service processes to provide the stable, consistent, and quality services that internal customers expect
- Understanding that increases in sales velocity increase inventory velocity, which, in turn, increases production or service velocity, finance velocity, human capital velocity, and systems velocity. The goal is to synchronize these velocities in a cohesive manner.
- Implementing the goal congruence concept by linking individual employee goals with those of the department/division and the organization. He must remove or reduce the competing or conflicting goals.
- Implementing crosscutting best practices across business units, divisions, departments, and functions through busting silos and building bridges
- Linking employee rewards, bonuses, and promotions to employees' true performance and tangible results, and empowering employees
- Building solid working relationships with C-level executives in marketing, manufacturing, IT, human resources, and other functions through formal and informal approaches at the workplace
- Fostering ethical values and cultural sensitivity in light of workforce diversity

- Encouraging employees to continuously acquire and improve their knowledge, skills, and abilities (KSAs) through targeted training courses, management development programs, and professional certifications
- Establishing a solid and sustainable chain of knowledge linked through the entire management hierarchy to ensure adequate core knowledge competencies for all levels of employees in the organization.
- Inviting finance audits, self-audits, special management reviews, and self-assessments periodically and proactively to ensure continuous improvement in finance quality, cost, and delivery
- Encouraging employees at all levels of the organization to think differently and radically (i.e., out-of-the-box thinking) at all times, which can lead to new perspectives providing best-of-breed solutions
- Participating in the succession-planning process for key positions
- Adhering to accounting, auditing, treasury, and finance professional and ethical standards established by the relevant professional bodies
- Analyzing outside-in views (i.e., views of stakeholders about company management) and inside-out views (i.e., views of company management about stakeholders) to identify disconnections between these views and to integrate them in a coherent manner

(b) MAJOR FINANCE FUNCTIONS. Below is a list of major activities and a brief description of those activities usually found in accounting, treasury, and finance functions. These activities are grouped into three categories: transaction processing, which consumes 70% to 80% of finance resources; control and compliance; and decision support.[2]

Transaction Processing

- **Accounts Payable.** Processing and paying vendor invoices for business expenditures incurred. Activity begins when an invoice is coded and approved for payment. In order to facilitate separation of duties, the category excludes activities involved in purchasing and receiving. It has two parts: (i) Invoice processing—match invoice, purchase order, and receiving report; resolve discrepancies; approve and code invoices for payment; maintain appropriate files. (ii) Payment processing—prepare checks, electronic payments, and wire transfers; initiate and process recurring payments; respond to vendor inquiries.
- **Benefits Plan Accounting.** Accounting, tracking, and reporting on employee benefit plans
- **Billing.** Revenue accounting and the documentation and issuance of bills (i.e., invoices) for products sold and services rendered
- **Cash Application.** Recording and tracking payments received from customers
- **Credit and Collection.** The extension of credit to customers and the collecting of slow payments and past-due receivables from customers
- **Fixed Asset Accounting.** Recording and controlling the physical records and financial activities related to long-term assets of the corporation

- **General Accounting.** Overseeing, coordinating, and controlling the accounting records and closing activities of the corporation. Duties include maintaining the general ledger, preparing the trial balance and other financial reports, and related activities.
- **Inventory Accounting.** The accounting for valuation of raw, intermediate, and finished materials, spare parts, supplies, or products received, transferred, retired, or sold
- **Payroll.** The payment of wages, salaries, and pension amounts in accordance with organizational policies. Activity begins at the point of entry into the payroll system. It does not include benefits administration but does includes time and attendance processing.
- **Travel and Entertainment Accounting.** Overseeing and processing expense reports and cash advances. It has three parts: (i) Cash advances—approve and disburse cash advances, resolve cash advance problems. (ii) Expense reports—verify that expense reports meet guidelines; approve expense reports; prepare payments; resolve travel expense problems; distribute travel and entertainment expenses. (iii) Travel and entertainment card administration—oversee issuance of cards and monitor use of the cards.

Control and Compliance

- **Financial Budgeting and Forecasting.** Establishing long-term and short-term financial plan, budgets, and forecasts. The focus is on developing detailed financial budgets and controlling actual expenses by comparing them to an historical budget.
- **External/Consolidated Reporting.** Reporting consolidated financial information as dictated by generally accepted accounting principles (GAAP), Securities and Exchange Commission (SEC) regulations, and statutory, subsidiary, and international reporting requirements.

Decision Support

- **Banking and Cash Management.** Handling cash flows and bank relations for noninvestment accounts
- **Cost Accounting.** Calculating product or service costs by using fixed, variable, and semivariable cost elements. Developing allocation schemes and analyzing cost variances
- **Financial Analysis and Management Reporting.** Analyzing financial and operational information to assess, interpret, and predict business performance to support management decisions. Evaluating capital investment decisions. Gathering, evaluating, and presenting financial, operating, and contractual information about proposed business transactions for internal management purposes
- **Tax Planning.** Examining tax issues for the corporation to optimize tax effectiveness of management decisions
- **Treasury and Trust Management.** Securing funds to meet the corporation's cash flow needs and investing any excess funds.

10.3 WORLD-CLASS FINANCE MANAGEMENT

(a) FINANCE STRATEGY. A world-class finance function can best be defined in terms of the business outcomes it produces, outcomes such as improved business analysis, innovative solutions to business problems, reduced operating costs, increased capability to perform ad hoc analysis, and improved overall business performance. Leading organizations define a shared vision—that is, a mission, a vision for the future, core values, goals, and strategies geared toward making the finance function a value-creating, customer-focused partner in business results.[3]

CRITICAL SUCCESS FACTORS FOR A WORLD-CLASS FINANCE FUNCTION

Critical success factors for a world-class finance function include value creation for investors and the organization; financial results; listening to stakeholder voices; leadership; organizational culture; customer service; organizational structure; technology; process; and people.

(b) LISTENING TO STAKEHOLDER VOICES. Finance management, as a cost and profit overseer for the company, should pay close attention in understanding and listening to the following "voices" to achieve organizational goals and to improve overall performance. When these "voices" are heard together, they bring attention to new perspectives and creative conflicts, forcing new thinking that leads to new solutions (i.e., best-of-breed solutions). Listening to the collective voice of many stakeholders at once will have a greater impact than listening to one voice at a time in isolation, because the former requires a balanced approach after considering all party's concerns.

For each content of each voice, a T-Column analysis should be prepared, with "what happens if I listen to this voice" in the left column (benefits) and "what happens if I don't listen to this voice" in the right column (costs and risks). A comparative analysis of each content in each column will point to new problems requiring new solutions.

- Voice of the customer (external customers such as suppliers, vendors, contractors, consultants, key customers, regulators, investors, creditors, the stock market, and media/press, and internal customers such as the board of directors, corporate management, and employees in other functional departments, such as manufacturing, marketing, human resources, and IT)
- Voice of the process (process flows, process variations, process delays and waste, and process inefficiencies)
- Voice of the investor (individual investors, institutional investors, and stock/capital markets)
- Voice of quality (TQM principles and practices, mistake-proofing, continuous improvement, cost of poor quality, quality assurance, quality control, quality audit, quality council, and quality circles)
- Voice of standards (GAAP, GAAS, FASB, GASB, SEC, AICPA, and IFAC technical standards; professional standards; ethical standards; industry/organization standards; and mergers and acquisition standards)
- Voice of partners (outsourcing vendors, electronic commerce vendors, and financial institutions)
- Voice of regulators (federal, state, and local laws and regulations)

- Voice of competitors (press releases, Web site pressrooms, industry magazines, daily business newspapers, advertising magazines, industry trade shows, product demonstrations and promotions, direct mail, e-mail campaigns, copyright/trademark/patent news, business intelligence news, banner advertising, billboard and street advertising, product sponsorships, and online events and chat rooms)

(c) FINANCE CYCLE-TIME MEASURES. Cycle time reduction in the finance function deals with reducing the order-to-cash cycle time and increasing purchase-to-payment cycle time (within the allowed limits), with associated benefits such as increased cash flows and profits, improved utilization of human and machine resources, decreased costs, and improved customer service. To attain these benefits, organizations must:

- Eliminate or decrease non-value-added activities (e.g., waste, fraud, and abuse of organization's resources and assets; paper-driven manual systems; correction of human-made errors and machine-made errors; invoice/billing rework time; unnecessary handoffs, stop points, chokepoints, pain points, or fault points in the cycle; and delays at interdepartmental and interdivisional boundaries and at intradepartmental work stations).
- Enhance or increase value-added activities (e.g., internal-customer contact points; external-customer touch points; self-audits and self-assessments; customer-order processing time; customer-order ship time; customer-cash collection time; internal/external customer access points to finance systems; finance project hold points; and finance-management decision points and control points).

This requires having the right resources available at the right place and at the right time so that delays and waste in finance operations are decreased.

Some examples of finance cycle-time measures include:

- Percentage decrease in order-to-cash cycle time
- Percentage decrease in quote-to-cash cycle time
- Percentage decrease in inventory cycle time in taking physical inventory
- Percentage decrease in cycle time for producing scheduled internal reports to internal management
- Decrease by number of days in accounting month-end book- closing cycle time (i.e., elapsed days from month-end to management review of financial statements)
- Elapsed time between an employee's expense report submission and receipt of the reimbursement check
- Elapsed time between invoice discrepancies discovered and corrected

(d) FINANCE METRICS. In addition to the generic sources indicated in Chapter 1 (Section 1.3) for selecting performance indicators, some specific sources for the finance metrics include the income statement, balance sheet, and cash flow statement.

Income Statement

- Percentage increase or decrease in gross sales or gross revenues, this year and compared to previous years

- Percentage increase or decrease in net sales or net revenues, this year and compared to previous years
- Percentage increase or decrease in net income, this year and compared to previous years
- Percentage increase or decrease in previous year's net income adjusted because of financial restatements made this year
- Percentage increase in total contribution margin amount, this year and compared to previous years
- Percentage increase or decrease in total product costs as a percentage of total sales or profits, this year and compared to previous years
- Percentage increase or decrease in total service costs as a percentage of total revenues or profits, this year and compared to previous years
- Percentage increase or decrease in total overhead costs as a percentage of total sales, revenues, or profits, this year and compared to previous years
- Percentage increase or decrease in total operating costs as a percentage of total sales, revenues, or profits, this year and compared to previous years
- Percentage increase or decrease in total administrative and sales costs as a percentage of total sales, revenues, or profits, this year and compared to previous years
- Percentage increase or decrease in total cost of poor product quality as a percentage of total sales or profits, this year and compared to previous years
- Percentage increase or decrease in total cost of poor service quality as a percentage of total revenues or profits, this year and compared to previous years
- Percentage increase in underbillings or overbillings to customers. The goal: no under/over billings, just the right billing, right the first time
- Percentage increase or decrease in total fraud costs resulting from known and proven cases expressed as a percentage of total costs, sales, revenues, or profits, this year and compared to previous years
- Percentage increase or decrease in total legal costs resulting from successful lawsuits expressed as a percentage of total costs, sales, revenues, or profits, this year and compared to previous years
- Percentage increase in avoidable litigation expenses that were not avoided, expressed as a percentage of total sales or revenues this year and compared to previous years
- Percentage increase or decrease in total contract-related costs resulting from fines and penalties paid for noncompliance with contractual terms and conditions, expressed as a percentage of total costs, sales, revenues, or profits, this year and compared to previous years
- Percentage decrease in net borrowing costs to the Treasury Management. The metric combines money-borrowing costs (i.e., interest cost and other loan-related costs), earnings on short-term investments, and the cost of investing the idle cash at rates below the cost of borrowing.
- Percentage increase or decrease in total insurance costs, expressed as a percentage of sales, this year and compared to previous years

- Percentage increase or decrease in total self-insurance losses (no insurance coverage), expressed as a percentage of sales, this year and compared to previous years
- Percentage increase or decrease in total interest costs, expressed as a percentage of total loan amounts borrowed, this year and compared to previous years
- Percentage increase or decrease in total cost of administrative staff in the finance function and other functions, expressed as a percentage of total payroll, sales, or revenues, this year and compared to previous years
- Percentage increase or decrease in total hedging costs expressed as a percentage of total amount of foreign currency transacted, this year and compared to previous years. The goal: a zero gain or loss resulting from changes in foreign currency exchange rates, after subtracting for hedging costs

Balance Sheet

- Percentage increase in cash-forecasting accuracy by Treasury management
- The number of times Treasury management failed to deliver cash where and when needed
- Percentage increase in inventory turnover ratio, this year and compared to previous years. The higher the ratio, the better it is, since it indicates higher sales and lower obsolete stock.
- Percentage increase in accounts-receivable turnover ratio, this year and compared to previous years. The higher the ratio, the better it is, since it indicates improvement in the collection of receivables from customers.
- Percentage increase in working capital amount, this year and compared to previous years
- Percentage increase or decrease in investment in inventory assets, this year and compared to previous years
- Percentage increase or decrease in investment in total current assets, this year and compared to previous years
- Percentage increase or decrease in investment in noncurrent (tangible and fixed) assets, this year and compared to previous years
- Percentage increase or decrease in investment in intangible (intellectual property) assets, this year and compared to previous years
- Number of times vendor invoices are paid on the due date without rework
- Number of times employee payroll checks are not distributed on the due date
- Percentage decrease in payroll-related errors

Income Statement and Balance Sheet

- Percentage increase or decrease in earnings per share (EPS) on common stock, this year and compared to previous years
- Percentage increase or decrease in price-earnings (P/E) ratio, this year and compared to previous years
- Percentage increase or decrease in dividends per share (DPS) on common stock, this year and compared to previous years
- Percentage increase or decrease in common stock price, this year and compared to previous years

- Percentage increase or decrease in total stock market capitalization amount for the company, this year and compared to previous years
- Percentage increase or decrease in return on investment (ROI), this year and compared to previous years
- Percentage increase or decrease in return on sales (ROS), this year and compared to previous years
- Percentage increase or decrease in return on total assets (ROTA), this year and compared to previous years
- Percentage increase or decrease in return on net assets (RONA), this year and compared to previous years
- Percentage increase or decrease in rate earned on the total stockholders' equity, this year and compared to previous years
- Percentage increase or decrease in rate earned on common stockholders' equity, this year and compared to previous years
- Percentage increase or decrease in ratio of net sales to assets, this year and compared to previous years. The metric assesses the effectiveness in the use of assets in generating sales.

Cash Flow Statement

- Percentage increase or decrease in cash flows generated from investing activities, this year and compared to previous years
- Percentage increase or decrease in cash flows generated from financing activities, this year and compared to previous years
- Percentage increase or decrease in cash flows generated from operating activities, this year and compared to previous years
- Percentage increase or decrease in "free cash flows," this year and compared to previous years. Increases in free cash flows can fund internal growth, retire debt, and promote financial flexibility.

(e) FINANCE GOALS AND BEST PRACTICES. Leading organizations define four overall goals and 11 best practices as critical to building a world-class finance function.[4]

(i) Goal 1: Make financial management an entity-wide priority. Leading organizations make financial management improvement an entity-wide priority by building a foundation of control and accountability that supports external reporting and performance management, providing clear and strong executive leadership, using training to change the organizational culture, and engaging line management. This requires a total commitment of top management, in both words and actions, to changing the culture, and this commitment must be sustained and demonstrated to staff.

(A) Best Practice 1: Build a Foundation of Control and Accountability that Supports External Reporting and Performance Management

A solid foundation of control and accountability requires a system of checks and balances that provides reasonable assurance that the entity's transactions are appropriately recorded and reported, its assets protected, its established policies followed, and its resources used economically and efficiently for the purposes intended. Organizations

build and maintain this foundation largely through the discipline of preparing routine periodic financial statements and annually subjecting them to an independent audit. However, senior executives at leading organizations recognize that the financial information demanded by decision makers to measure and manage performance requires greater precision and more timely access than that required for the entity to receive an unqualified opinion on its financial statements. To ensure that decision makers have useful, relevant, timely, and reliable information, leading finance functions establish accountability goals that extend well beyond receiving an unqualified audit opinion. In addition, the internal controls at these organizations are designed to efficiently meet the control objectives necessary for performance measurements and management, as well as external financial reporting.

Organizations should do the following:

- Leverage audit resources and the financial-statement audit process to improve data reliability and increase accountability.
- Increase accountability by establishing goals for (1) producing financial and performance reports for major business segments, and (2) moving the organization toward more frequent financial reporting (e.g., quarterly and monthly).
- Use accounting and operational-performance data to support budget formulations and strategic planning.

(B) Best Practice 2: Provide Clear and Strong Executive Leadership

A powerful, visionary leader can change the direction, culture, and perceptions of the finance function. At leading organizations, the CEO understands the important role the CFO and the finance function play in improving the entity's overall business performance. Consequently, the CFO is a central figure in the top management team and heavily involved in strategic planning and decision making. In addition, the senior executives demonstrate their sustained commitment to finance-related improvement initiatives by using key business line managers to drive improvement efforts, attending key meetings, ensuring that the necessary resources are made available, and creating a system of rewards and incentives to recognize those who support improvement initiatives. In fact, the committed support of the CEO and the line managers are critical to the success of finance-related improvement initiatives.

Organizations should do the following:

- Form an executive management team to establish a vision and fundamental goals and provide sponsorship for each major financial-management improvement project.
- Involve key business managers in driving financial improvement initiatives.
- Develop a plan to ensure that all key stakeholders visibly support financial-management improvement initiatives.
- Actively market the benefits of financial-management improvement efforts to secure the necessary resources.
- Establish an expectation that top financial executives, as part of the top management team, provide forward-looking analysis that creates a link between accounting information and budget formulation and contributes to strategic planning and decision making.

(C) Best Practice 3: Use Training to Change the Organizational Culture and Engage Line Management

The key to successfully managing change and changing organizational culture is gaining the support of line management. To change the organizational culture and enlist the support of line managers, many leading organizations utilize training programs. Some are generic in nature and are intended to help employees anticipate and cope with change and to ensure that every employee in the organization understands the need for change. Others are specifically geared toward providing line managers with a greater appreciation of the financial implications of their business decisions. Through these interactions, financial managers gain a better understanding of business problems, and nonfinancial managers gain an appreciation of the value of financial information. This not only produces better managers, it also helps break down functional barriers that can affect productivity and impede improvement efforts. In addition, these organizations provide tools to facilitate and accelerate the pace of the change initiative. A common belief is that slow implementation generally kills a change program, the reason being that employees have too much time to contemplate the potential negative effects of change and to rally opposition that ultimately undermines the effort.

Organizations should do the following:

- Identify key financial and nonfinancial managers and staff whose support is critical to the success of financial-management improvement initiatives.
- Develop curriculum and provide training that teaches key nonfinancial managers and staff how to use financial information to improve operational planning and decision making.
- For all key managers and staff, develop curriculum and provide training that furnishes a framework and tools that can be used to facilitate and accelerate the pace of change initiatives.

(ii) Goal 2: Redefine the role of finance to better support mission objectives. Leading organizations have redefined the role of finance to better support mission objectives by assessing the finance function's current role in meeting mission objectives, maximizing the efficiency of day-to-day accounting activities, and organizing finance to add value.

(A) Best Practice 4: Assess the Finance Function's Current Role in Meeting Mission Objectives

Many leading finance functions assess their current role in supporting mission objectives by comparing the percentage of staff time spent on strategic support activities (such as business performance analysis or cost analysis) with the percentage of resources spent on transaction processing and other routine accounting activities. Many research studies indicated that 70% to 80% of finance resources are spent on transaction processing and other routine accounting activities, such as accounts payable, payroll, and external reporting. While transaction processing will always exist, it does not have to drain the finance function's resources. Therefore, many leading finance functions have calculated and compared these percentages as a general indication of how well they supported the organization's business objectives. A goal for many leading organizations is to reduce the time spent on transaction-processing activities to 20%. This goal is supplemented with external benchmarking and internal customer feedback.

Organizations should do the following:

- Identify all major functions performed by the finance department (e.g., accounts payable, payroll, performance reporting, and performance analysis) and group each function into meaningful categories (e.g., transaction processing, control and compliance, and decision support).
- Establish and monitor organization's specific performance goals and measures that reflect the finance function's role in meeting mission objectives (i.e., the percentage of time or resources devoted to decision support versus transaction processing or control-and-compliance activities).
- Benchmark financial management practices and processes with recognized industry leaders (e.g., the cost of finance as a percentage of total outlays, unit cost per accounting transaction) in order to measure performance and identify best practices.
- Periodically survey internal customers to obtain information related to the quality and value of the products and services they receive and use this information to guide improvement initiatives.
- Develop and track performance metrics and compare a company's average with world-class companies for the following areas:
    - Total finance cost as a percent of revenue
    - Accounts payable productivity per full-time employee
    - Number of transaction-processing locations
    - Number of systems used per transaction
    - Budget cycle in days
    - Month-end accounting closing cycle in days
- Develop and track major finance processes with their measures and compare a company's average with world-class companies for the following areas:
    - Process: Payables, Measure: Invoice
    - Process: Receivables, Measure: Remittance
    - Process: Travel and Expense, Measure: Expense Report
    - Process: Payroll, Measure: Paycheck

(B) Best Practice 5: Maximize the Efficiency Day-to-Day Accounting Activities

As part of an overall strategy to reduce the costs of finance and better support business objectives, many leading organizations have reduced the number of staff required to perform routine transaction-processing activities by eliminating or streamlining inefficient processes and/or consolidating these activities at shared services centers. Activities such as accounts payable, long-term asset accounting, and payroll are performed at the shared service centers. Benefits claimed from the use of shared service centers include reduction in operating costs, better control and standardization of processes, more cost-effective technology deployment, and an enhanced position for continual improvement and customer service.

Leading organizations did not proceed with these improvement activities in one big step, instead going ahead with a staged approach. The first stage is consolidation, which includes changing the organizational structure and gaining control over processes. The second stage is standardization and entails changing processes, adopting

a common technology platform, and fostering continuous improvement. The final stage is reengineering and involves changing workflow and leveraging technology through the use of electronic commerce, data warehousing, and document imaging.

Organizations should do the following:

- Consolidate, standardize, and reengineer transaction processing and other routine accounting activities at a shared service center, initially by department and then across departments and divisions.
- Eliminate, streamline, or reengineer costly, inefficient transaction processing and routine accounting activities.
- Outsource transaction processing and routine accounting activities when the capacity and quality of outsourcing vendors improves.

(C) Best Practice 6: Organize the Finance Function to Add Value to the Organization

Currently, most activities within the finance function are focused primarily on (1) establishing and administering policy, (2) tracking, monitoring, and reconciling account balances, or (3) ensuring compliance with laws and regulations.

Experts predict that future finance function will have fewer people, with a greater percentage of analysts than clerks. Although many leading organizations maintain similar core functions at headquarters (for example, budgeting, treasury management, general accounting, and payroll), their new goals include reducing the cost of finance and organizing the finance function to add value by reallocating finance resources to more productive strategic-support activities.

To accomplish this, leading organizations have realigned their mission and organizational structure to better support the entity's business objectives. Specifically, they have (1) organized around core business processes to simplify work and flatten hierarchies, (2) consolidated certain transaction-processing activities to gain economies of scale, and (3) moved functions, such as cost accounting and financial analysis, to the business units to support the units' strategic planning and decision-making needs. In addition, these organizations have created a coherent human capital strategy—that is, a framework of human capital policies, programs, and practices specifically designed to steer the organization toward its shared vision—and integrated this strategy with the organization's overall strategic planning.

Organizations should do the following:

- Define the finance function's mission, vision for the future, core values, goals, and strategies for supporting the organization's overall mission objectives.
- Develop an explicit workforce planning strategy that is linked to the organization's strategic planning efforts to ensure that financial managers and staff with skills for analyzing and interpreting financial data will support the organization's strategic planning and decision-making needs at both the field and headquarters level.

(iii) Goal 3: Provide meaningful information to decision makers. Financial information is meaningful when it is useful, relevant, timely, and reliable. Global competition and advances in IT have changed information requirements and users' expectations regarding the availability and usefulness of financial information. Financial information that, in the

past, was considered adequate for decision making is now considered overaggregated and too late to be useful. Leading organizations have enhanced their capabilities for providing meaningful information to decision makers by developing management information systems that support the partnership between finance and operations, reengineering processes in conjunction with implementing new technology, and translating data into meaningful information.

(A) Best Practice 7: Develop Systems that Support the Partnership Between Finance and Operations

The leading finance functions have long had general ledger systems capable of generating auditable financial statements efficiently and routinely, thereby providing information on stewardship and accountability at a high level. Further, they historically have had adequate systems for measuring and managing cost and performance. However, new technology has made it possible for these functions to integrate these systems and provide more relevant, accessible information that meets the changing needs of decision makers. Many leading organizations have already implemented, or are in the process of implementing, an enterprise-wide system to integrate financial and operating data to support both management decision making and external reporting requirements. Some abandoned their legacy systems all together and turned to state-of-the-art integrated architectures, while others used well-functioning legacy systems and tied them together with a data warehouse. Regardless of the approach, these systems provided financial analysts, accountants, and business unit managers access to the same cost, performance, and profitability information.

Organizations should do the following:

- Acquire and install a general ledger system adequate for external financial reporting purposes.
- Develop managerially relevant cost-information systems and strategic-performance management systems that access data from financial transaction systems and relevant operating systems.
- Integrate the organization's financial (including budgetary), operating, and management systems, and equip decision makers with the tools to easily access relevant information and perform ad hoc analyses.
- Ensure that financial systems comply with accounting standards, such as GAAP.

(B) Best Practice 8: Reengineer Processes in Conjunction with Implementing New Technology

Many leading organizations are using commercial off-the-shelf (COTS) application packages for financial systems with limited modification to the basic application package itself. The advantages of using COTS software include: (1) COTS software is less costly than applications developed in-house, (2) software upgrades are affordable and regularly available, and (3) COTS software is designed to include best practices.

The key to successfully implementing COTS systems and best practice processes is reengineering business processes to fit the new software applications. In fact, productivity gains typically result from creation of more efficient processes, not from simple automation of old ones. Effectively reengineering business processes, however, requires moving

from a functional-based organization to a process-based organization. For example, the federal procurement process in a process-based organization would start with a solicitation request being issued, continue through contract award and signature, the issuance of purchase/work orders, and receipt of goods, and end when the vendor properly received payment. The business processes would be designed to maximize the efficiency and accuracy of the entire process.

Organizations should do the following:

- Form cross-functional teams to examine existing core business processes and to define user requirements.
- Compare COTS products against the organization's requirements and identify the COTS packages that most closely match the organization's needs.
- Reevaluate user requirements not supported by COTS software and determine, before customizing the software, whether each requirement is still valid or whether alternatives exist that may be more cost-effective.
- Where software modifications are required, implement an effective configuration management system that includes (1) clearly defining and assessing the effects of modifications on future product upgrades before the modifications are approved, (2) clearly documenting software products that are placed under configuration management, and (3) maintaining the integrity and traceability of the configuration throughout the system life cycle.
- Implement a quality assurance process that ensures that project activities and software products adhere to management's established plans, standards, and procedures. This includes ensuring that the configuration management process is effectively implemented and that product changes are clearly documented and tested before being placed into production.
- Implement an effective risk management strategy to ensure that project risks (such as customization and the vendor's ability to deliver a given system) are adequately identified and effective mitigation strategies are implemented.

(C) Best Practice 9: Translate Financial Data into Meaningful Information

While new technology has made financial data more available, decision makers are powerless if they do not have the ability to translate that data into relevant, understandable information. Traditionally, finance functions have used voluminous paper reports, based primarily on the prior month's activity, to communicate financial information. Further, management reports have often been designed around current organizational structures. Consequently, as organizational structures have changed over time, many management reports have become irrelevant.

Today, leading finance functions have eliminated, reduced, and/or redesigned much of their old management-reporting formats to better meet the needs of the user. These companies have designed new reporting formats around key business drivers, not organizational structures, in order to provide executives and managers with relevant, forward-looking information on business unit performance. Periodically, organizations should stop distributing selected management reports to determine whether anyone would miss them. Subsequent lack of reaction can be used as an indicator that the information in the report was no longer relevant. Further, standardized reports should be designed to

present information that is analyzed to bring out pertinent and fundamental points with suitable amounts of detail and explanation. The standardized reports can also be shown on the company's Intranet with multiple levels of detail, so that decision makers can drill down to their desired level of detail.

Organizations should do the following:

- Meet with key decision makers on an ongoing basis to define key business drivers and determine what key business information is needed for management.
- Determine what information is needed by key managers to meet and support key business information requirements.
- Present various reporting format and content options to executives, managers, and other key stakeholders.

(iv) Goal 4: Build a finance team that delivers results. As the finance function has evolved from a paper-driven, labor-intensive, clerical role to a more consultative role as adviser, analyst, and business partner, many leading companies have seen a corresponding shift in the mix of skills and competencies required of the function. Many of these companies have developed finance teams with the right mix of skills and competencies by attracting and retaining talent as part of an overall strategic approach to human capital planning.

(A) Best Practice 10: Develop a Finance Team with the Right Mix of Skills and Competencies

Developing a finance team with the right mix of skills and competencies starts by defining a set of skills and competencies that will enable the finance team to meet the current and future technical, management, and leadership needs of the business. The resulting competency profile is used to assess gaps in individual or group competency levels and to develop human capital strategies to address current or expected future deficiencies.

Leading finance functions have developed training, career development, and succession-planning strategies in order to develop a team with the right mix of skills and competencies. For example, they provide intensive two- to three-year entry-level training programs as well as midcareer and executive-level development programs that use both classroom instruction and rotational assignments to develop technical, management, and leadership skills and competencies. The programs' course work focuses initially on the tools and techniques of advanced accounting and finance, as well as general business skills. Then, the focus shifts to the strategic application of these tools within business-specific environments. However, the key to implementing a successful career development program is to complement course work with real-life business experience through the use of planned rotational assignments. They provide opportunities for staff to rotate through various positions throughout the finance department and the operating divisions. Such opportunities are critical, not only to developing employees who understand the whole business and thereby provide greater value to their customers in the operating divisions, but also to ensuring that an adequate supply of well-prepared financial staff is available to fill key positions (i.e., succession planning).

Organizations should do the following:

- Assess the finance function's human capital policies, programs, and practices to determine whether they support its mission and vision for the future.

- Using classroom training, planned staff rotations, and interdepartmental assignments, design a career development program geared toward (1) improving leadership, management, and traditional financial management competencies, including the analytical skills needed to support decision making, (2) understanding how laws and regulations will affect the finance function's roles, responsibilities, and processes, and (3) understanding the overall organization's operations, including the implications of financial decisions.
- Establish continuing professional-education requirements for financial managers similar to those required for accountants and auditors.

(B) Best Practice 11: Build a Finance Function that Attracts and Retains Talent

Several key factors are important in recruiting, retaining, and rewarding talent. First, recruiting a talented workforce requires the commitment of top leadership. The CFO should be heavily involved in talent assessment, and senior executive leaders should be actively involved in on-campus recruiting. This sends a powerful message to potential new recruits that the position is important enough to the organization that it warrants senior executive attention.

Second, attracting and ultimately keeping a highly qualified and motivated workforce involves providing meaningful career development opportunities, such as the opportunity to (1) participate in exciting groundbreaking projects, (2) build a portfolio of new skills, and (3) choose a variety of career paths.

Third, compensation is a key factor in any career decision. Other nonfinancial factors, such as the desire to effect change and to make a difference to the organization, are also important.

Organizations should do the following:

- Actively work with colleges and universities to market the opportunities available for financial staff.
- Continue to work with the human resource department to provide more flexible career paths that provide opportunities for movement throughout the finance function and other departments.
- Utilize staff development programs and planned staff rotations to expose financial managers and staff to a variety of career paths.

10.4 CAPITAL BUDGET

(a) OVERVIEW. Capital assets, which are long-term assets, represent a major portion of total assets of private- and public sector organizations. Capital assets include facilities (e.g., office buildings, manufacturing plants, power plants, and warehouses and distribution centers), equipment (e.g., machinery and computers), and renovation and improvement of these assets. Capital assets can make organizations strategically competitive in terms of products and services they offer to their customers. Therefore, guidance is needed for linking the entire range of capital decisions to strategic goals and objectives, analyzing and ranking potential investments, and making informed decisions that are based on the full cost and risk of a capital project.[5]

The project manager of a capital project should balance its costs, schedules, risks, and impacts in meeting the defined goals and objectives.

(b) PRINCIPLES AND BEST PRACTICES. Leading organizations use the following five principles and 12 best practices when making decisions about the planning, budgeting, acquisition, or management of capital assets. These principles and practices are reinforced by important success factors such as vision, strategic planning, the availability of good information, and communication. Since each capital asset is big in size and scope, it is considered as a separate investment project for managing purposes.

(i) Principle 1: Integrate organizational goals into the capital decision-making Process

(A) Best Practice 1: Conduct Comprehensive Assessment of Needs to Meet Mission- and Results-Oriented Goals and Objectives

Conducting a comprehensive needs assessment or analysis of the project's requirements is an important first step in an organization's capital decision-making process. Leading organizations conduct comprehensive needs assessments that (1) consider the organization's overall mission, (2) identify the resources needed to fulfill both immediate requirements and anticipated future needs on the basis of the results-oriented goals and objectives that flow from the organization's mission, and (3) consider noncapital approaches (e.g., contracting out and joint ventures) to addressing these goals. The needs assessments by leading organizations are results oriented, in that they determine how specific outcomes might be obtained rather than what is needed to maintain or expand existing capital infrastructure.

(B) Best Practice 2: Identify Current Capabilities Including the Use of an Inventory of Assets and their Condition, and Determine if there is a Gap Between Current and Needed Capabilities

Leading organizations gather and track information that helps them identify the gap between what they have and what they need to fulfill their goals and objectives. To help assess current capabilities and establish a baseline, such organizations maintain systems that track the use and performance of existing assets and facilities. This is an area where current and accurate information is essential. Some functions performed by asset inventory and tracking systems include: (1) identifying the location and status of assets and facilities, (2) tracking and reporting the condition and deferred maintenance needs of assets and facilities, and (3) tracking user satisfaction. A critical step in making deferred maintenance estimates is to take a complete and reliable inventory of capital assets as a basis for assessing maintenance costs.

(C) Best Practice 3: Decide How Best to Meet the Gap by Identifying and Evaluating Alternative Approaches (Including Noncapital Approaches)

Leading organizations consider a wide range of alternatives to satisfy their needs, including noncapital alternatives, before choosing to purchase or construct a capital asset. Managers carefully consider such options as contracting out or divesting the activity

that the asset would support. When it is determined that capital is needed, managers also consider the repair and renovation of existing assets. When evaluating alternatives, prudent decision makers also consider the various funding options available to them. They weigh the different impacts of debt financing, engaging in a joint-venture project, or using current-year appropriations.

(ii) Principle 2: Evaluate and select capital projects using an investment approach

(A) Best Practice 4: Establish Review and Approval Framework Supported by Analyses

Leading organizations found that establishing a decision-making framework that encourages the appropriate level of management review and approval, supported by the proper financial, technical, and risk analyses, is a critical factor in making sound capital investment decisions. A well-thought-out framework for reviews and approval can mean that capital investment decisions are made efficiently and are supported by better information. Some leading organizations have review processes in place that determine the level of analysis and review that will be conducted, depending on the size, complexity, and cost of the project. Projects that are expensive, span a number of years, or are crucial to the organization's strategy or structure usually require more analysis, support, and review than projects that cost less, have shorter time frames, or have less organization-wide impact.

(B) Best Practice 5: Rank and Select Projects on the Basis of Established Criteria

Leading organizations also have defined processes for ranking and selecting projects. The selection of projects is based on preestablished criteria and a relative ranking of investment proposals. They determine the right mix of projects by viewing all proposed investments and current capital assets as a portfolio. Organizations generally find it beneficial to rank projects because the number of requested projects exceeds available funding.

(C) Best Practice 6: Develop a Long-Term Capital Plan that Defines Capital Asset Decisions

Once projects are ranked, they are put into a long-term capital plan. Leading organizations develop long-term capital plans to guide the implementation of organizational goals and objectives and to help decision makers establish long-term priorities. While the capital plans must be responsive to changing requirements, they are based on the strategic plan's long-range visions for the organization. Therefore, any year-to-year changes should be driven by strategic decisions.

(iii) Principle 3: Balance budgetary control and managerial flexibility when funding capital projects

(A) Best Practice 7: Budget for Projects in Useful Segments or Components

One strategy that has proven useful to organizations in dealing with the problems posed by full funding in a capital budget environment is to budget for projects in useful segments. This means that when a decision has been made to undertake a specific capital project, funding sufficient to complete a useful segment of the project is provided in advance. A useful segment is a component that either (1) provides information that allows the organization to plan the capital project, develop the design, and assess the benefits, costs, and risks before proceeding to full acquisition (or canceling the acquisition) or (2) results in a useful asset for which the benefits exceed the costs even if no further funding is appropriated.

(B) Best Practice 8: Consider Innovative Approaches to Full Up-Front Funding

Alternative strategies used by some leading organizations to accommodate the full funding of capital projects in a constrained budget environment include contracting out for capital-intensive services, using an investment component that resembles a savings account, and developing partnership arrangements. These strategies enhance the flexibility an organization needs to finance the full costs of capital projects, but they do so without compromising top management's ability to make decisions that are based on full costs. Approval by senior management and the board are needed in order to establish an investment component.

(iv) Principle 4: Use project management techniques to optimize project's success

(A) Best Practice 9: Monitor Project's Performance and Establish Incentives for Accountability

The successful implementation of a capital investment project is determined primarily by whether the project was completed on schedule, came in within budget, and provided the benefits intended. To accomplish this, the first step is to provide decision makers with good information about cost estimates, risks, and the scope of a planned project before committing substantial resources to it. This, in combination with full up-front funding, can help to prevent cost overruns, project cancellations, and missed deadlines for completion. By monitoring a project's performance against cost, schedule, and technical performance goals, as well as by establishing incentives to meet those goals, organizations can increase the likelihood that a project will be successfully completed.

(B) Best Practice 10: Use Cross-Functional Teams to Plan for and Manage Projects

Leading organizations use multidisciplinary teams, consisting of individuals who are from different functional areas and who are led by a project manager, to plan and manage projects. Typically, a core project team is established early in the life cycle of a project, and additional individuals with particular technical or operational expertise are incorporated during appropriate phases of the project. The team must not only possess technical and operational expertise but also be composed of the "right" people. The selection of the team members is critical—that is, they must be knowledgeable, willing to trade off leadership roles, and able to plan work and set goals in a team setting.

(v) Principle 5: Evaluate results and incorporate lessons learned into the decision-making process

(A) Best Principle 11: Evaluate Results to Determine if Organization-Wide Goals and Objectives Have Been Met

One way of determining if a capital investment achieved the benefits that were intended when it was selected is to evaluate its performance using measures that reflect a variety of outcomes and perspectives. By looking at a mixture of hard and soft measures (for example, financial improvement and customer satisfaction), managers are able to base their assessment of performance on a comprehensive view of the needs and objectives of the organization. To implement this balanced approach to performance measurement, the leading organizations develop financial and nonfinancial criteria for success that link to the organization's overall goals and objectives. Business unit managers can then develop

project-specific performance measures that are tied to these criteria and are used as the basis for developing unit performance measures and goals. The unit measures are ultimately rolled up into a division-wide or organization-wide "scorecard" that measures how well the organization is meeting its goals and objectives.

(B) Best Practice 12: Evaluate the Decision-Making Process: Reappraise and Update to Ensure that Goals and Objectives are Met

Although some organizations evaluate their capital decision-making process on an ongoing basis, many do not. Leading organizations generally revise their processes in response to an internal crisis or to a perception of changing needs and/or a changing environment. Under these situations, organizations conduct self-assessments and undergo major changes in their capital decision-making practices in order to continue successful operation.

10.5 OUTSOURCING FINANCE OPERATIONS

(a) OVERVIEW While outsourcing is growing, the concept is not clearly or uniformly defined. Outsourcing can be defined in ways ranging from the prolonged use of consultants to perform a simple task, on the one hand, to transferring to a third party the responsibility for performing an entire internal function.[6]

In addition, an organization that is considering outsourcing may focus on a complete function or on portions of the function. To illustrate, an organization's finance function comprises processes, activities, and tasks. The payroll process includes various activities, such as calculating employees gross compensation for the pay period, determining and deducting amounts from gross compensation to calculate net pay, and printing and distributing payroll checks. Each activity, in turn, includes one or more tasks. The activity of calculating employee compensation, for example, includes such tasks as collecting time cards, tabulating time worked or leave taken per employee, and multiplying hours worked or leave taken per employee by the appropriate pay rate. An organization would have the option to outsource an entire process, one or more of the activities, or merely one or more of the tasks.

Only a few organizations outsource one or more entire processes, such as accounts payable, pension payments, general ledger accounting, long-term asset accounting, or excise and property tax administration.

Most organizations used other options to improve their financial operations, such as reengineering all or parts of their accounting and finance functions, establishing a shared service center, or upgrading their financial systems. For example, one company's approach to improving financial management consisted of (1) consolidating the accounting function into as few locations as possible and having each location move to a single system to accomplish the function, (2) simplifying existing processes, developing systems that captured data at the point the transaction originated (regardless of location within the organization), and (3) outsourcing all or parts of processes that could be done more efficiently or effectively by a third party. Through these steps, the company was able to reduce the number of accounting staff by approximately two-thirds in a 15-year period. However, most of the efficiencies achieved were due to actions other than outsourcing, and the company estimated that outsourcing accounted for less than 10% of the total savings. Officials from another organization told us that they were able to reduce

the number of personnel involved in processing accounting transactions by an estimated 90% over a 12-year period by using shared service centers, consolidating systems, and reengineering their accounting processes.

A good example of this task-oriented type of outsourcing is found with the accounts payable process, where a company might have a vendor take on check printing and mailing while the company itself continued to handle all other activities and tasks associated with managing accounts payable. Another example is found with payroll processing, where a company might have a vendor compute net pay and take on the printing and distribution of paychecks while the company itself continued to handle the human resource and payroll tasks of entering data and computing employee gross pay amounts. Such arrangements might also require the vendor to do other tasks, such as accumulating employee pay information and preparing and distributing W-2 statements at the end of the year.

Organizations, both private and public, can use a variety of strategies to improve their accounting and financial operations and reduce costs. The financial improvement option is one of other, related options, such as consolidating systems, consolidating operating locations, and reengineering business processes.

To the extent that private organizations have outsourced any portion of their finance and accounting operations, such outsourcing has generally been limited to routine, mechanical tasks, such as check writing and payroll processing. Only a few organizations have outsourced an entire process within a finance and accounting function. The existing limited capacity of outsourcing vendors to perform larger, more complex finance and accounting operations may have constrained wider use of outsourcing by these organizations. Experts in the outsourcing field have estimated that it may be three to five years before this type of capacity is widely available.

The experiences of the leading organizations provide some lessons learned for others to follow. Specifically, the following factors are considered as part of the outsourcing decision process and are often associated with successful outsourcing:

- Establishing an outsourcing policy that specifies what process and criteria to follow in making the outsourcing decision that will achieve the organizations overall goals
- Performing a strategic analysis to determine the organization's core competencies
- Benchmarking the organization's processes against those of world-class organizations to determine comparable costs and identify any deficiencies in its operations
- Performing market research to determine whether a competitive market exists for the outsourcing services the organization needs
- Considering carefully the ramifications of potential job loss and other possible adverse personnel impact that could occur as a result of outsourcing

In addition, after an organization decides to outsource, two key factors are identified with successful outsourcing arrangements. First, successful outsourcing organizations ensure that they maintain sufficient expertise and control to effectively oversee the outsourcing vendor to prevent fraud, waste, and mismanagement. Without effective oversight controls, organizations cannot effectively ensure that vendors carry out their fiduciary responsibilities. Second, successful outsourcing is more likely to happen when

an organization has its outsourcing vendor sign a results-oriented contract that includes appropriate performance measures.

(b) OUTSOURCING FINANCE-OPERATIONS BEST PRACTICES

(i) Current vendor capacity must be assessed to see whether it can meet the outsourcing needs of a large organization. The generally limited use of outsourcing for repetitive, labor-intensive tasks may be attributed, in part, to the lack of a mature vendor marketplace with sufficient capacity to provide the larger-scale, more complex finance and accounting services often required by large organizations. However, there are indications that the outsourcing market may be on the verge of dramatic growth. Some experts in the field have estimated that organizations with large, complex finance and accounting operations will be able to outsource the entire accounting or finance function.

(ii) Outsourcing should be done in the context of overall outsourcing policy. A corporate outsourcing policy can ensure that all factors associated with an outsourcing decision are identified and addressed. Concerns over whether, and the extent to which, outsourcing may affect an organization's goals and operations must be carefully considered. Such a policy should be explicit as to the extent to which outsourcing will be used to reduce costs, improve efficiency, and increase organizational flexibility. The overall view is that decision and implementation related to outsourcing should involve the same type of rigorous analysis, careful planning, and thorough management involvement as any other major business decision.

The policy should require (1) clear objectives for outsourcing, (2) a recognition of all available service delivery options (e.g., internal staff versus third party), (3) a rigorous cost-benefit analysis and risk analysis, (4) buy-in by all affected parties, (5) communication with employees throughout the outsourcing decision-making process, (6) consideration of the potential impact of outsourcing on such key areas as cost, savings, service quality, system conversion, and retraining of personnel, and (7) consideration of the potential for disruption of services.

(iii) Core competencies should be assessed when determining what to outsource. Decisions on outsourcing are becoming part of the organizational strategic planning process, with the goal of increasing competitiveness in the world market. In considering whether to outsource, leading organizations have assessed essential functions strategically in terms of their relationship to core competencies. A hospital's core competencies, for example, would be those directly associated with caring for patients. Core competencies have also been defined as those few functions within a company that are important to the customers, that the company can dominate, and that are embedded in the organization's systems.

Regarding accounting and finance, managerial analysis and decision support work is considered a core activity and therefore should not be outsourced. However, activities such as the clerical aspects of the accounts payable and payroll processes are noncore activities and therefore candidates for outsourcing.

Organizations should not outsource any finance and accounting activity that (1) is important to maintaining control of the business, (2) is important to maintaining the company's competitive position, (3) involves company confidential information, (4) involves a critical expertise that the company cannot afford to lose, or (5) is used to develop staff

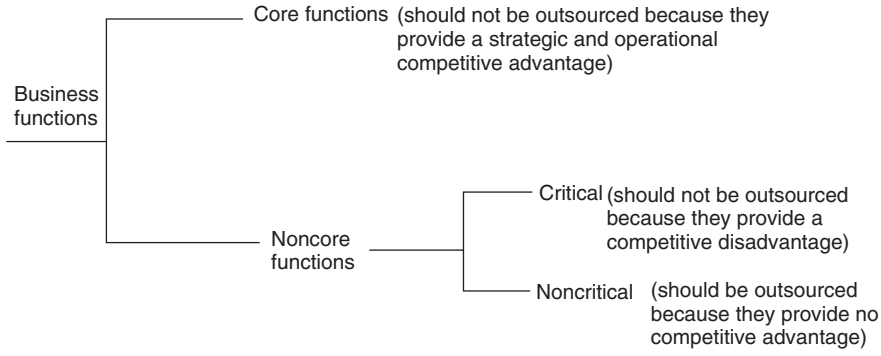

Exhibit 10.1 What to Outsource and What Not to Outsource

for managerial advancement. Exhibit 10.1 shows core and noncore functions, and breaks the noncore into critical and noncritical functions.

Some leading organizations further break down the noncore functions into critical or noncritical. Noncore critical functions are important to an organization but are not directly linked to what the organization perceives as its primary mission. If they are not performed at a world-class level, however, these functions can place an organization at a competitive disadvantage or even endanger its existence. For most organizations, such functions include finance, accounting, and human resources administration. Noncritical functions are those that provide no competitive advantage and that may not seriously harm an organization in the event of their being performed badly. Examples of noncritical functions would include cafeteria services, groundskeeping, and laundry.

Outsourcing arrangements for many organizations usually start with noncritical functions. As the organization becomes more accustomed to relying on others to perform simple, noncritical functions, the organization tends to consider outsourcing a more diverse and critical set of activities. Reasons that an organization might want to outsource one or more of its critical but noncore functions (such as finance and accounting) include the potential for (1) significant cost savings, (2) access to needed skills and expertise, (3) access to the latest technology or world-class capabilities, (4) accelerated implementation of planned improvements, and (5) freeing management resources for other purposes.

(iv) Deficiencies should be identified through benchmarking, a key factor for outsourcing decisions. Benchmarking generally involves identifying organizations that have developed world-class processes, and then using applicable performance measures (such as cost per transaction, average processing time, or error rate) to compare an organization's performance to that of the world-class organizations. Benchmarking lets an organization know how well it is doing and puts it in a better position to assess which improvement initiative, if any, best fits its situation. A key result of an effective benchmarking process will be a full understanding of the extent and nature of any existing deficiencies in an organization's finance and accounting operations. This understanding is critical to successfully establishing and monitoring an outsourcing contract.

Consistent, objective, and measurable baseline data on operations compared with baseline data from a world-class organization is essential to a reliable benchmarking assessment. An organization must develop reliable, quantitative data on costs and other objective measures of the area being considered for outsourcing. Failure to obtain reliable data can increase the risk that data will be manipulated to achieve a desired result. For example, the organizational component being considered for outsourcing may have an incentive to exclude relevant costs so that the costs of its operations appear to be lower than they actually are. Outsourcing vendors performing this analysis, on the other hand, may be inclined to include as many costs as possible.

(v) Personnel issues must be addressed. Organizations cited outsourcing's potential impact on personnel as a particularly sensitive issue in considering whether and what finance and accounting operations to outsource. Outsourcing is likely to result in a reduction in the number of an organization's employees. Addressing sensitive issues associated with potential job loss and other possible adverse personnel impacts will be critical to dealing with potential resistance to outsourcing and to building momentum for change.

The issue of job loss resulting from outsourcing is the most difficult hurdle to overcome in reaching a decision to outsource all or part of an organization's finance and accounting operations. Some organizations have delayed outsourcing specific activities because the affected employees may not have the necessary skills to transfer to other areas in the accounting department. Organizations, rather than displacing existing staff, continue to pursue internal operating efficiencies and will wait for the employees to leave through reassignment or normal attrition before outsourcing those positions.

(vi) Effective oversight of the outsourcing vendor is essential. Ensuring that an organization maintains sufficient expertise and has an effective set of controls in place to oversee the vendor's operations is essential to successful outsourcing. Common contract-monitoring techniques used by organizations to maintain control over the outsourcing vendor's operations include retaining the right to audit the vendor's operations, insisting on periodic reports of cost and service performance, and holding meetings to discuss performance. Maintaining oversight requires the internal audit department to review the vendor's records, procedures, policies, and controls related to the outsourced function.

(vii)Performance measures must be established and used to monitor outsourcing. A well-defined results-based contract—based on clearly defined, results-oriented performance measures rather than on the processes to be followed—is recognized as one of the primary ways of helping to ensure that an organization will achieve the desired level of benefits. While a results-based contract will not guarantee good contractor performance, it will help in measuring the contractor's performance and the extent to which expected benefits have been achieved.

Service providers, consultants, and end users agree that outsourcing contract should be results-based rather than process-based. Process-based requests for proposals and contract documents often preclude providers from developing the most appropriate outsourcing solution. A better move is to use a results-based request for proposals that is descriptive of current functions and also of what is expected from the vendor in terms of improved performance. The results-based contract should detail performance expectations for the outsourced processes, including the timing of reports

and the presentation, availability, and quality of accounting and finance information. The results-based contract should also establish a related set of performance measures intended to help determine the extent to which the goals of the outsourcing arrangement are achieved.

An example of a process-based contract would be to process accounts payable requiring the vendor to manually match the purchase order, receiving report, and invoice. This process of matching may require more vendor staff, which limits the vendor in implementing efficiencies and changing processes to improve operations and reduce costs. If the contract had been based on results, it would state that the vendor is responsible for making timely and correct payments for 99.5% of the dollar value of the invoices processed. In this results-based contract, the vendor would be able to take advantage of such techniques as electronic data interchange and evaluated receipts, thus enabling payments to be based upon efficient and accurate computerized matches of key elements on the purchase order and receiving report.

10.6 STANDARDS FOR INTERNAL CONTROL

(a) DEFINITIONS AND OBJECTIVES. Internal control is a major part of managing an organization. It comprises the plans, methods, and procedures used to meet missions, goals, and objectives and, in doing so, support performance-based management. Internal control also serves as the first line of defense in safeguarding assets and preventing and detecting errors and fraud. In short, internal control, which is synonymous with management control, helps organization managers achieve desired results through effective stewardship of resources.[7]

Internal control should provide reasonable assurance that the objectives of the organization are being achieved in the following categories:

- Effectiveness and efficiency of operations, including the use of the entity's resources
- Reliability of financial reporting, including reports on budget execution, financial statements, and other reports for internal and external use
- Compliance with applicable laws and regulations

A subset of these objectives is the safeguarding of assets. Internal control should be designed to provide reasonable assurance regarding prevention of or prompt detection of unauthorized acquisition, use, or disposition of an organization's assets.

(b) FUNDAMENTAL CONCEPTS. The fundamental concepts provide the underlying framework for designing and applying the standards for internal control.

(i) Concept 1: Internal control is a continuous built-in component of operations. Internal control is not one event, but a series of actions and activities that occur throughout an entity's operations and on an ongoing basis. Internal control should be recognized as an integral part of each system that management uses to regulate and guide its operations, not as a separate system within an organization. In this sense, internal control is management control that is built into the entity as a part of its infrastructure to help managers run the entity and achieve their aims on an ongoing basis.

(ii) Concept 2: Internal control is affected by people. People are what make internal control work. The responsibility for good internal control rests with all managers. Management sets the objectives, puts the control mechanisms and activities in place, and monitors and evaluates the control. However, all personnel in the organization play important roles in making it happen.

(iii) Concept 3: Internal control provides reasonable assurance, not absolute assurance. Management should design and implement internal control based on the related cost and benefits. No matter how well designed and operated, internal control cannot provide absolute assurance that all organization objectives will be met. Factors outside the control or influence of management can affect the entity's ability to achieve all of its goals. For example, human mistakes, judgment errors, and acts of collusion to circumvent control can affect meeting organization objectives. Therefore, once in place, internal control provides reasonable, not absolute, assurance of meeting organization objectives.

(c) INTERNAL CONTROL STANDARDS. Five standards define the minimum level of quality acceptable for internal control and provide the basis against which internal control is to be evaluated. These five standards are (1) control environment, (2) risk assessment, (3) control activities, (4) information and communication, and (5) monitoring. These standards apply to all aspects of an organization's operations (financial and nonfinancial), including compliance with laws and regulations. Management is responsible for developing the detailed policies, procedures, and practices to fit their organization's operations and to ensure that they are built into and serve as an integral part of operations.

(i) Internal Control Standard 1: Control environment. A positive control environment is the foundation for all other standards. It provides discipline and structure and shapes the prevailing mindset, which influences the quality of internal control. Several key factors affect the control environment.

Factor 1: Integrity and Ethical Values. One factor is the integrity and ethical values maintained and demonstrated by management and staff. Organization management play a key role in providing leadership in this area, especially in setting and maintaining the organization's ethical tone, providing guidance for proper behavior, removing temptations for unethical behavior, and providing discipline when appropriate.

Factor 2: Management's commitment to competence. Another factor is management's commitment to competence. All personnel need to possess and maintain a level of competence that allows them to accomplish their assigned duties, as well as understand the importance of developing and implementing good internal control. Management needs to identify appropriate knowledge and skills needed for various jobs and provide needed training, as well as candid and constructive counseling and performance appraisals.

Factor 3: Management's philosophy and operating style. Management's philosophy and operating style also affect the control environment. This factor determines the degree of risk the organization is willing to take on and management's philosophy toward performance-based management. Further, the attitude and philosophy of management toward information systems, accounting, human resource functions, monitoring, and audits and evaluations can have a profound effect on internal control.

Factor 4: Entity's organizational structure. Another factor affecting the control environment is the entity's organizational structure. It provides management's framework for planning, directing, and controlling operations to achieve the entity's objectives. A good internal control environment requires that the entity's organizational structure clearly defines key areas of authority and responsibility and establishes appropriate lines of reporting.

Factor 5: Delegation of authority and responsibility. The control environment is also affected by the manner in which the organization delegates authority and responsibility throughout the organization. This delegation covers authority and responsibility for operating activities, reporting relationships, and authorization protocols.

Factor 6: Good human capital policies and practices. Good human capital policies and practices are another critical factor. This includes establishing appropriate practices for hiring, orienting, training, evaluating, counseling, promoting, compensating, and disciplining personnel. It also includes providing a proper amount of supervision.

Factor 7: Senior management's relationship with the board of directors. A final factor affecting the control environment is senior management's relationship with the board of directors, the internal/external auditors, the Inspector General, and the corporate counsel. Senior management councils and steering committees can contribute to a good overall control environment.

(ii) Internal Control Standard 2: Risk assessment. A precondition to risk assessment is the establishment of clear, consistent organization objectives. Risk assessment is the identification and analysis of relevant risks associated with achieving given objectives—such as those defined in strategic and annual performance plans—and the formulation of a basis for determining how the risks should be managed.

Management needs to comprehensively identify risks and should consider all significant interactions between the entity and other parties, as well as internal factors at both the entity-wide and activity level. Risk identification methods may include qualitative and quantitative ranking activities, management conferences and meetings, forecasting and strategic planning, and consideration of findings from audits and other assessments.

Once risks have been identified, they should be analyzed for their possible effect. Risk analysis generally includes estimating the risk's significance, assessing the likelihood of its occurrence, and deciding on the actions needed to manage the risk. The specific risk analysis methodology used can vary by organization because of differences in organizations' missions and the difficulty of qualitatively and quantitatively assigning risk levels.

(iii) Internal Control Standard 3: Control activities. Control activities are the policies, procedures, techniques, and mechanisms that enforce management's directives, such as the process of adhering to requirements for budget development and execution. They help ensure that actions are taken to address risks. Control activities are an integral part of an entity's planning, implementing, reviewing, and accountability for stewardship of organization resources and achieving effective results.

Control activities occur at all levels and functions of the entity. They include a wide range of diverse activities such as approvals, authorizations, verifications, reconciliations, performance reviews, maintenance of security, and creation and maintenance

of related records, which provide evidence of execution of these activities as well as appropriate documentation. Control activities may be applied in a computerized information-system environment or through manual processes.

(A) Common and Manual Control Activities

There are 11 common control activities, which are mostly manual processes. These are described next.

1. **Senior management–level reviews of actual performance.** Senior management should track major achievements, compare these to the organization's plans, goals, and objectives, and take corrective actions as needed.
2. **Reviews by management at the functional or activity level.** Functional business managers also need to compare actual performance to planned or expected results throughout the organization, analyze significant differences, and take corrective actions as needed.
3. **Management of human capital.** Effective management of an organization's work force—its human capital—is essential to achieving results and an important part of internal control. Management should view human capital as an asset rather than a cost. Operational success becomes possible when the right personnel for the job are on board and are provided with the right training, tools, structure, incentives, and responsibilities. Management should ensure that skills needs are continually assessed and that the organization is able to obtain a workforce that has the required skills that match those necessary to achieve organizational goals. Training should be aimed at developing and retaining employee skill levels to meet changing organizational needs. Qualified and continuous supervision should be provided to ensure that internal control objectives are achieved. Performance evaluation and feedback, supplemented by an effective reward system, should be designed to help employees understand the connection between their performance and the organization's success. As a part of its human capital planning, management should also consider how best to retain valuable employees, plan for their eventual succession, and ensure continuity of needed skills and abilities.
4. **Controls over information processing.** A variety of control activities are used in information processing. Examples include edit checks of data entered, accounting for transactions in numerical sequences, comparing file totals with control accounts, and controlling access to data, files, and programs.
5. **Physical control over vulnerable assets.** An organization must establish physical control to secure and safeguard vulnerable assets. Examples include security for and limited access to assets such as cash, securities, inventories, and equipment, which might be vulnerable to risk of loss or unauthorized use. Such assets should be periodically counted and compared to control records.
6. **Establishment and review of performance measures and indicators.** Activities need to be established to monitor performance measures and indicators. These controls could call for comparisons and assessments relating different sets of data to one another so that analyses of the relationships can be made and appropriate actions taken. Controls should also be aimed at validating the proprietary and integrity of both organizational and individual performance measures and indicators.

7. **Segregation of duties.** Key duties and responsibilities need to be divided or segregated among different people to reduce the risk of error or fraud. This should include separating the responsibilities for authorizing transactions, processing and recording them, reviewing the transactions, and handling any related assets. No one individual should control all key aspects of a transaction or event.
8. **Proper execution of transactions and events.** Transactions and other significant events should be authorized and executed only by persons acting within the scope of their authority. This is the principal means of assuring that only valid transactions to exchange, transfer, use, or commit resources and other events are initiated or entered into. Authorizations should be clearly communicated to managers, supervisors, and employees.
9. **Accurate and timely recording of transactions and events.** Transactions should be promptly recorded to maintain their relevance and value to management in controlling operations and making decisions. This applies to the entire process or life cycle of a transaction or event, from the initiation and authorization through its final classification in summary records. In addition, control activities help to ensure that all transactions are completely and accurately recorded.
10. **Access restrictions to and accountability for resources and records.** Access to resources and records should be limited to authorized individuals, and accountability for their custody and use should be assigned and maintained. Periodic comparison of resources with the recorded accountability should be made to help reduce the risk of errors, fraud, misuse, or unauthorized alteration.
11. **Appropriate documentation of transactions and internal control.** Internal control and all transactions and other significant events need to be clearly documented, and the documentation should be readily available for examination. The documentation should appear in management directives, administrative policies, or operating manuals and may be in paper or electronic form. All documentation and records should be properly managed, maintained, and retained.

(B) Control Activities Specific for Computerized Information Systems

There are two broad groupings of information system control—general control and application control. General control applies to all information systems—mainframe, minicomputer, network, personal computer, and end-user environments. Application control is designed to cover the processing of data within the application software.

General and application controls over computer systems are interrelated. General control supports the functioning of application control, and both are needed to ensure complete and accurate information processing. If the general control is inadequate, the application control is unlikely to function properly and could be overridden.

Because IT changes rapidly, controls must evolve to remain effective. Changes in technology and its application to electronic commerce and expanding Internet applications will change the specific control activities that may be employed and how they are implemented, but the basic requirements of control will not change. As more powerful computers place more responsibility for information processing in the hands of the end users, the needed controls should be identified and implemented.

General Control. This category includes entity-wide security program planning, management, control over data center operations, system software acquisition and maintenance, access security, and application system development and maintenance.

- Data-center and client-server operations controls include backup and recovery procedures, and contingency and disaster planning. In addition, data-center operations controls also include job set-up and scheduling procedures and controls over computer operator activities.
- System software control includes control over the acquisition, implementation, and maintenance of all system software, including the operating system, database management systems, telecommunications, security software, and utility programs.
- Access security control protects the systems and network from inappropriate access and unauthorized use by hackers and other trespassers, and from inappropriate use by organization personnel. Specific control activities include frequent changes of dial-up numbers; use of dial-back access; giving users access only to system functions that they need; use of software and hardware firewalls to restrict access to assets, computers, and networks by external parties; and frequent changes of passwords and deactivation of former employees' passwords.
- Application-system development and maintenance control provides the structure for safely developing new systems and modifying existing systems. Included are documentation requirements, authorizations for undertaking projects, and the necessary reviews, testing, and approvals of development and modification activities before systems are placed into operation. An alternative to in-house development is the procurement of commercial software, but control is necessary to ensure that selected software meets the user's needs and is properly placed into operation.

Application Control. This category of control is designed to help ensure completeness, accuracy, authorization, and validity of all transactions during application processing. Control should be installed at an application's interfaces with other systems to ensure that all inputs are received and are valid and that all outputs are correct and properly distributed. An example is computerized edit checks built into the system to review the format, existence, and reasonableness of data.

(iv) Internal Control Standard 4: Information and communication. For an entity to run and control its operations, it must have relevant, reliable, and timely communications relating to internal as well as external events. Information is needed throughout the organization to achieve all of its objectives.

(A) Information

Pertinent information should be identified, captured, and distributed in a form and time frame that permit employees to perform their duties efficiently.

Business and program managers need both operational and financial data to determine whether they are meeting their organizations' strategic and annual performance plans and meeting their goals for accountability for effective and efficient use of resources.

For example, operating information is required for development of financial reports. This covers a broad range of data from purchases, subsidies, and other transactions to data on long-term assets, inventories, and receivables. Operating information is also needed to determine whether the organization is achieving its compliance requirements under various laws and regulations.

For example, financial information is needed for both external and internal uses. It is required to develop financial statements for periodic external reporting, and, on a day-to-day basis, to make operating decisions, monitor performance, and allocate resources.

(B) COMMUNICATION

Effective communications should occur in a broad sense, with information flowing down, across, and up the organization. In addition to internal communications, management should ensure there are adequate means of communicating with, and obtaining information from, external stakeholders that may have a significant impact on whether and how the organization achieves its goals. Moreover, effective IT management is critical to achieving useful, reliable, and continuous recording and communication of information.

(v) Internal Control Standard 5: Monitoring. Internal control should generally be designed to assure that ongoing monitoring occurs in the course of normal operations. It is performed continually and is ingrained in the organization's operations. It includes regular management and supervisory activities, comparisons, reconciliations, and other actions employees take in performing their duties.

Separate evaluations to control can also be useful by focusing directly on the controls' effectiveness at a specific time. The scope and frequency of separate evaluations should depend primarily on the assessment of risks and the effectiveness of ongoing monitoring procedures. Separate evaluations may take the form of self-assessments as well as review of control design and direct testing of internal control. Separate evaluations also may be performed by an agency's Inspector General, an organization's internal auditor, or by an independent (external) auditor. Deficiencies found during ongoing monitoring or through separate evaluations should be communicated to the individual responsible for the function and also to at least one level of management above that individual. Serious matters should be reported to top management.

Monitoring of internal control should include policies and procedures for ensuring that the findings of audits and other reviews are promptly resolved. Managers are to (1) promptly evaluate findings from audits and other reviews, including those showing deficiencies and recommendations reported by auditors and others who evaluate organizations' operations, (2) determine proper actions in response to findings and recommendations from audits and reviews, and (3) complete, within established time frames, all actions that correct or otherwise resolve the matters brought to management's attention. The resolution process begins when audit or other review results are reported to management, and it ends only after action has been taken that (1) corrects identified deficiencies, (2) produces improvements, or (3) demonstrates that the findings and recommendations do not warrant management action.

10.7 APPLICABLE LAWS, REGULATIONS, STANDARDS, AND PRINCIPLES

Organizations have a legal and ethical obligation to comply with the various federal, state, and local laws, regulations, circulars and bulletins, directives and executive orders, government orders, and ordinances pertinent to a specific business area. Noncompliance with these laws and regulations can lead to fines, civil and/or criminal penalties, probation, and jail punishments (prison time), thus creating reputation (image) risk.

Compliance with industry and/or organization standards, including professional standards, can increase the quality of products and services, which, in turn, can enhance an organization's reputation and image in the marketplace. Adherence to generally accepted business principles and practices could have a similar effect as complying with standards. Specifically, accountants, auditors, and finance professionals must abide to their professional standards and code of ethics and must use professional skepticism during their work.

A brief roundup of information about major laws, regulations, and standards is provided here as a reminder for checklist purposes. Note that these laws and regulations are subject to change as new ones are added and existing ones are amended or repealed. The reader is advised to obtain the original laws, regulations, and standards from the official sources for a better understanding of the provisions, requirements, and conditions of the laws, regulations, and standards (www.regulations.gov). Although some of the following laws, regulations, and standards directly affect public sector organizations (i.e., government agencies), private-sector organizations can read, learn, and apply them to improve their business operations on a proactive basis.

U.S. organizations should comply with the following laws, regulations, standards, and principles pertinent to accounting, treasury, and finance management:

Sarbanes-Oxley Act

Overview. As a result of recent corporate scandals resulting from management's "lack of integrity," management fraud, accounting firms' negligence, and use of earnings management techniques, both investors and creditors have lost confidence in corporate America. In light of this financial crisis and credibility gap, the U.S. Congress passed the Sarbanes-Oxley (SOX) Act of 2002 to reform the accounting profession and corporate management and governance.

Essentially, the Act creates a five-member Public Company Accounting Oversight Board (PCAOB), which has the authority to set and enforce auditing, attestation, quality control, and ethics (including independence) standards for auditors of public companies. It is also empowered to inspect the auditing operations of public accounting firms that audit public companies, and to impose disciplinary and remedial sanctions for violations of the board's rules, securities laws, and professional auditing and accounting standards.

Other provisions affecting the accounting profession include requiring the rotation of the lead audit partner and reviewing audit partner every five years, and extending the statute of limitations for the discovery of fraud to two years from the date of discovery and five years after the act. The law restricts the consulting work that auditors can perform for their publicly traded audit clients, and it establishes harsh penalties for securities law violations, corporate fraud, and document shredding. Fines range from $100,000 for individual negligent conduct to $15 million

to a firm for knowing or intentional conduct, including recklessness and repeated acts of negligence.

The Act also requires CEOs and CFOs to certify their company's financial statements as part of the annual report to stockholders. They also have a greater duty to communicate and coordinate with corporate audit committees, who are now responsible for hiring, compensating, and overseeing the independent auditors. There are new requirements regarding enhanced financial disclosures as well.

Provisions of the SOX Act. Those sections of the Act that apply to audit community include sections 301, 302, 404, and 409. Section 301 focuses on public company audit committees. Section 302 deals with quarterly CEO/CFO certification of financial statements and disclosure controls. Section 404 addresses annual evaluation of internal control over financial reporting. Section 409 focuses on real-time issuer disclosure requirements. Now we will focus on Sections 404 and 409.

Section 404 of the Act requires the auditor to document and test the effectiveness of internal controls over information technology and computer application systems. The scope of this review includes general computer controls, application controls, and systems software controls. Specifically, the scope can include security controls, the disaster-recovery and business continuity plan, and IT infrastructure. Compliance with Section 404 requires companies to establish an infrastructure designed to protect and preserve vital records and data from destruction, loss, unauthorized alteration, or other misuse. This infrastructure is designed to ensure there is no room for unauthorized alteration of records vital to maintaining the integrity of data and availability of business processes. Since CEOs and CFOs need to certify the financial statements, it is very important to ensure the integrity of financial data and availability of financial systems. The documentation effort should not be viewed as a sunk cost; instead it should be treated as return on investment with decreased reputation cost.

Note that Section 404 substantially increases the role (and importance) of auditors when it comes to the audit. Internal controls over transaction cycles (e.g., sales and collection cycle) were formerly performed on a rotational basis, but now all controls over all cycles must be tested every year.

Section 409 of the Act requires the issuer (firm) to disclose to the public, in plain English and on a rapid and current basis, any additional information concerning material changes in the financial condition or operations of the issuer. This may include trend and qualitative information and graphic presentations. The purpose of the section is to inform investors in a timely, clear, and user-friendly manner.

For a full text of the SOX Act, visit www.aicpa.org or www.pcaobus.org.

Financial Accounting Standards Board. The mission of the Financial Accounting Standards Board (FASB) is to establish and improve standards of financial accounting and reporting for the guidance and education of the public, including issuers, auditors, and user of financial information. FASB standards are related to GAAP (www.fasb.org).

Government Accounting Standard Board. The mission of the Government Accounting Standards Board (GASB) is to establish and improve standards of state and local governmental accounting and financial reporting that will result in useful information

for users of financial reports and guide and educate the public, issuers, auditors, and users of these reports (www.gasb.org).

Bank Secrecy Act. The Bank Secrecy Act (BSA) of 1970 was designed to fight drug trafficking, money laundering, and other crimes. The U.S. Congress enacted the BSA to help prevent banks and other financial service providers from being used as intermediaries for criminal activity or as concealers of the transfer or deposit of money derived from such activity. Among other things, the BSA created an investigative "paper trail" by establishing regulatory reporting standards and requirements (e.g., the Currency Transaction Report). Through a later amendment, it also established record-keeping requirements for wire transfers. Some of the internal reports routinely available through bank service providers include cash transaction reports, wire transfer records and logs, monetary instrument records, and velocity-of- funds reports.

Money Laundering Control Act. The Money Laundering Control Act of 1986 amended the BSA to enhance its effectiveness and to strengthen the government's ability to fight money laundering by making the act a federal crime and by making a criminal offense of structuring transactions to avoid BSA reporting requirements.

Money laundering is the criminal practice of filtering ill-gotten or "dirty" money through a series of transactions so that the funds are "cleaned" to look like proceeds from legal activities. Money laundering is driven by criminal activities and conceals the true source, ownership, or use of funds. Money laundering is a diverse and often complex process that need not involve cash transactions. It basically involves three independent steps that can occur simultaneously:

1. **Placement**—placing, through deposits or other means, unlawful proceeds into the financial system
2. **Layering**—separating proceeds of criminal activity from their origin through the use of layers of complex financial transactions
3. **Integration**—using additional transactions to create the appearance of legality through the purchase of assets

An effective anti–money laundering program will help minimize exposure to transaction, compliance, and reputation risk. Such a program should include account-opening controls and the monitoring and reporting of suspicious activity.

USA Patriot Act. The USA Patriot Act of 2001 evolved as a response by the U.S. government to combat international terrorism. The Act contained strong measures to prevent, detect, and prosecute terrorism and international money laundering. The Act establishes new rules and responsibilities affecting U.S. banking organizations, other financial institutions, and nonfinancial commercial businesses.

Electronic Funds Transfer Act. The Electronic Funds Transfer (EFT) Act of 1978 establishes the basic rights, liabilities, and responsibilities of consumers who use electronic transfer services and of the financial institutions that offer these services. The Act requires disclosures of specific information regarding EFT services offered by the bank, such as issuance of access devices, liability for unauthorized transfers (both consumer and bank), and billing-error resolution procedures.

Fair Debt Collection Practices Act. The Fair Debt Collection Practices Act was passed to eliminate the abusive debt collection practices being used by debt collectors and financial institutions. The Act requires debt collectors and banks to use common

courtesy when collecting a debt, such as stating who they are, their reasons for calling, and what they want.

Truth in Lending Act. The Truth in Lending Act is intended to promote the education of the consumer by requiring specific disclosures relating to the terms and conditions of an applicant's request for credit. The Act is not intended to govern the charges that creditors impose for the acquisition of consumer credit.

Fair Credit Reporting Act. The Fair Credit Reporting Act was passed to establish safeguards for the reporting of information on consumers and to ensure that the information being reported was confidential, accurate, relevant, and properly utilized.

Federal Managers Financial Integrity Act. The Federal Managers Financial Integrity Act (FMFIA) of 1982 requires agencies to establish and maintain internal control. Under sections 2 and 4, respectively, the agency head must annually evaluate and report on the control and financial systems that protect the integrity of federal programs. The requirements of FMFIA serve as an umbrella under which other reviews, evaluations, and audits should be coordinated and considered to support management's assertion about the effectiveness of internal control over operations, financial reporting, and compliance with laws and regulations.

Federal Financial Management Improvement Act. The Federal Financial Management Improvement Act (FFMIA) of 1996 requires agencies to have financial management systems that substantially comply with federal financial-management systems requirements, standards that are promulgated by the Federal Accounting Standards Advisory Board (FASAB) and the U.S. Standard General Ledger at the transaction level. Financial management systems shall have general and application controls in place in order to support management decisions by providing timely and reliable data. The agency head shall make a determination annually about whether the agency's financial management systems substantially comply with the FFMIA. If the systems are found not to be compliant, management shall develop a remediation plan to bring those systems into substantial compliance.

Government Performance and Results Act. The Government Performance and Results Act (GPRA) of 1993 requires agencies to develop strategic plans, set performance goals, and report annually on actual performance compared to goals. With the implementation of this legislation, these plans and goals are integrated into (1) the budget process, (2) the operational management of agencies and programs, and (3) accountability reporting to the public on performance results and on the integrity, efficiency, and effectiveness with which the results are achieved.

Chief Financial Officers Act. The Chief Financial Officers (CFO) Act of 1990 requires agencies to both establish and assess internal control related to financial reporting. The Act requires the preparation and audit of financial statements. In this process, auditors report on internal control and compliance with laws and regulations related to financial reporting.

Inspector General Act. The Inspector General (IG) Act of 1978 provides for independent reviews of agency programs and operations. IGs are required to submit semiannual reports to Congress on significant abuses and deficiencies identified during the reviews and on the recommended actions to correct those deficiencies As part of the financial statement audit, inspector generals and /or external auditors are required by the Government Auditing Standards and OMB Requirements of Federal

Financial Statements (Bulletin No. 01-02) to report material weaknesses in internal control related to financial reporting and noncompliance with laws and regulations.

Improper Payments Information Act. The Improper Payments Information Act of 2002 requires agencies to review and identify programs and activities that may be susceptible to significant improper payments. Agencies must annually submit estimates of improper payments, corrective actions to reduce the improper payments, and statements as to whether the given agency's current information systems and infrastructure can support the effort to reduce improper payments. The nature and incidence of improper payments shall be considered when assessing the effectiveness of internal control.

Single Audit Act. The Single Audit Act requires financial statement audits of nonfederal entities that receive or administer grant awards of federal moneys. The financial statement audits include testing the effectiveness of internal control and determining whether the award moneys have been spent in compliance with laws and regulations.

Government Management Reform Act. The Government Management Reform Act (GMRA) of 1994 was passed, in part, to help the government remedy its lack of useful, relevant, timely, and reliable financial information. Under this program, designated agencies will provide common administrative support services such as personnel, payroll, or accounting service through self-supporting organizations in a businesslike manner.

Clinger-Cohen Act. The Clinger-Cohen Act of 1996 builds on the best practices of leading public and private-sector organizations by requiring agencies to better link their IT planning and investment decisions to program missions and goals. The Act contains critical provisions requiring federal agencies to use investment and capital-planning processes to manage their IT portfolios. Further, the Act requires that agencies modernize inefficient administrative and mission-related work processes before making significant technology investments to support them.

OMB Circulars. Various circulars issued by the U.S. Office of Management and Budget (OMB) affect financial statements, audits, and internal controls (www.omb.gov). Some of these circulars include the following:

- Preparation, submission, and execution of the budget (A-11)
- Management's responsibility for internal control (A-123)
- Financial management systems (A-127)
- Management of federal information resources (A-130)
- Audits of state, local governments, and nonprofit organizations (A-133)
- Financial accounting principles and standards (A-134)
- Financial reporting requirements (A-136)

Foreign Corrupt Practices Act. In addition to antibribery provisions, the Foreign Corrupt Practices Act of 1977 (FCPA) contains provisions pertaining to accounting and internal control. These provisions require corporate management to maintain books, records, and accounts that accurately and fairly reflect transactions and dispositions relating to the corporation's assets, and to devise and maintain a system of internal accounting control adequate to accomplish certain financial objectives. Thus, a key theme underlying the FCPA is that sound internal control should provide an effective deterrent to illegal payments.

U.S. Federal Sentencing Guidelines. The U.S. federal sentencing guidelines for organizational defendants became effective in November 1991. These guidelines provide judges with a compacted formula for sentencing business organizations for various white-collar crimes. Included are federal securities, antitrust, and employment and contract laws, as well as the crimes of mail and wire fraud, kickbacks and bribery, and money laundering.

To launder money is to disguise the origin or ownership of illegally gained funds to make them appear legitimate. Hiding legitimately acquired money to avoid taxation also qualifies as money laundering. The crime is not limited to drug trafficking. It is associated with nearly all kinds of "crimes for profit," such as real estate fraud and savings and loan abuses.

The federal sentencing guidelines represent a unique "carrot and stick" approach that requires business organizations found guilty of crimes to face sanctions reaching potentially hundreds of millions of dollars (the "stick"). Organizations may be given offsetting credits against these penalties if they can demonstrate that (a) they exercised due diligence (reasonable care) prior to the offense, (b) the wrongdoing was investigated, and (c) they cooperated with government investigators (the "carrot"). The fines and penalties are adjusted depending upon whether an organization has an effective program to prevent or detect violations of law.

An organization is well advised to be able to demonstrate, prior to the accusation of any offense, that it exercised due diligence in seeking to prevent and detect criminal conduct by its agents. Due diligence requires that the organization has taken, at a minimum, the following seven steps:

1. Established compliance policies that define standards and procedures
2. Assigned specific high-level responsibility to ensure compliance with these standards and procedures
3. Used due care in not delegating substantial discretionary authority to individuals who could engage in illegal activities
4. Communicated standards and procedures to all employees (by requiring participation in training programs and disseminating publications)
5. Took reasonable steps to achieve compliance with standards (by utilizing monitoring and auditing systems including a system, for employees to report violations without fear of reprisal)
6. Consistently enforced standards through appropriate disciplinary mechanisms
7. Took all reasonable steps to prevent future similar offenses

Right to Financial Privacy Act. Few countries require banks and financial institutions to report currency transactions that exceed a specified amount. However, many other countries require banks to record transactions over some specified amount. These records can then be made available to law enforcement officials under the terms of that country's bank secrecy laws.

Many countries also either require or encourage financial institutions to report transactions that are considered suspicious or indicative of criminal activity. However, certain provisions in the Right to Financial Privacy Act of 1978 generated questions in the banking community about the type of customer information that could be disclosed in reporting a suspicious transaction, as well as concerns about potential liability

for such disclosure. Subsequent legislation provided certain protections against civil liability for institutions reporting suspicious transactions.

The Money Laundering Control Act of 1986 amended the Right to Financial Privacy Act of 1978 to explicitly define the specific types of account information that financial institutions could disclose without customer permission or a subpoena, summons, or search warrant. The intent was to protect the privacy rights of customers while allowing financial institutions to give government investigators enough information about the nature of possible violations for the investigators to determine whether there was a basis to proceed with a summons, subpoena, or search warrant for additional information. The 1986 amendments also established a limited "good faith" defense, whereby financial institutions and their employees, when making a disclosure of certain specified information, would be shielded from a civil liability to the customer for such disclosure or for any failure to notify the customer of such disclosure. Despite this provision, many banks were concerned that they might still be liable under the Right to Financial Privacy Act for disclosures made on a voluntary basis.

The Racketeer Influenced and Corrupt Organizations Act. In 1970, the U.S. Congress enacted the Racketeer Influenced and Corrupt Organizations Act (RICO) as a weapon against mobsters and racketeers who were influencing legitimate business. The Act defines the term "racketeering activities" to include crimes such as mail fraud and fraud committed in the sale or purchase of securities.

The RICO Act can bring civil or criminal cases, with treble damages being possible under the former. For civil cases, the standard of proof requires a "preponderance of evidence." The plaintiff must prove that the defendant (1) employed any device to defraud, (2) made an untrue statement of material fact or omitted material fact, and (3) engaged in an act, practice, or course of business to commit fraud or deceit in connection with the purchase or sale of securities. The plaintiff must also prove damages sustained, material misstatement or omission, reliance, and a deceit.

For criminal cases, the standard of proof is "beyond a reasonable doubt." Section 32(a) of the Act establishes criminal liability for "willfully" and "knowingly" making false or misleading statements in reports under the Security Exchange Act of 1934. This section provided for criminal penalties consisting of fines of not more than $100,000, imprisonment of not more than five years, or both.

Sherman Antitrust Act. The Sherman Act of 1890 prohibits actions that are "in constraint of trade" or actions that attempt to monopolize a market or create a monopoly. Legal actions under this act typically involve price fixing or other forms of collusion among sellers. However, the law also prohibits reciprocity or reciprocal purchase agreements.

Clayton Antitrust Act. The Clayton Act of 1914 makes price discrimination illegal and prohibits sellers from exclusive arrangements with purchasers and/or product distributors.

Robinson-Patman Act. The Robinson-Patman Act of 1936 further addresses the issue of price discrimination established in the Clayton Act. It prohibits sellers from offering a discriminatory price where the effect of discrimination may limit competition or create a monopoly. There is also a provision that prohibits purchasers from inducing a discriminatory price. While a seller may legally lower price as a concession during

negotiations, the purchaser should not mislead or trick the seller, which would result in a price that is discriminatory to other buyers in the market.

Federal Trade Commission Act. The Federal Trade Commission Act of 1914 authorizes the Federal Trade Commission (FTC) to interpret trade legislation, including the provisions of the Sherman Antitrust Act that deal with restraint of trade. The Act also addresses unfair competition and unfair or deceptive trade practices.

U.S. Securities Regulations. The primary purpose of U.S. federal securities regulation is to prevent fraudulent practices in the sale of securities and thereby to foster public confidence in the securities market. Federal securities law consists principally of two statutes: the Securities Act of 1933, which focuses on the issuance of securities, and the Securities Exchange Act of 1934, which deals mainly with trading in issued securities. These "secondary" transactions greatly exceed in number and dollar value the original offerings by issuers. The Securities and Exchange Commission (SEC) administers both of these securities acts (www.sec.gov).

Gramm-Leach-Bliley Act. The Gramm-Leach-Bliley Act (GLBA) requires financial institutions to protect their customers' information against security threats. For example, log management can be helpful in identifying possible security violations and resolving them effectively. The Act also protects nonpublic personal information collected and used by financial institutions.

Voice of the Customer. "Voice of the customer" (VOC) means organizations should listen to and understand the external customers' needs, wants, and expectations (i.e., customers' voice), and provide products and services that truly meet such needs, wants, and expectations. The same thing applies to internal customers' needs (i.e., departments or functions within an organization).

Voice of the Process. "Voice of the process" means understanding and evaluating the nature of process flows, process variations, and process characteristics and capabilities for both products and services. The goal is to reduce process variations in order to make the process stable and predictable and to reduce the cycle times.

New work processes must be designed to reduce the cycle time by eliminating stop points, chokepoints, pain points, or fault points in a process that enjoys the support and availability of resources such as tools, technology, people, equipment, and information. Existing work processes must be (1) streamlined by reviewing the upstream and downstream work steps, (2) simplified by removing unnecessary handoffs, stop points, chokepoints, pain points, or fault points, (3) standardized based on "lessons learned," and (4) institutionalized by being rolled out to the entire organization.

American Institute of Certified Public Accountants. The American Institute of Certified Public Accountants (AICPA) is a professional organization and the voice of THE public accounting profession. It establishes professional certification (Certified Public Accountant, CPA), professional standards such as generally accepted accounting principles (GAAP) and generally accepted auditing standards (GAAS), and a code of ethics for public accountants and independent auditors to follow (www.aicpa.org).

Institute of Management Accountants. The Institute of Management Accountants (IMA) is a professional organization and the voice of the management accounting profession. It establishes professional certification (Certified Management Accountant, CMA), professional standards, and a code of ethics for management accountants to follow (www.imanet.org).

Association for Financial Professionals. The Association for Financial Professionals (AFP) is a professional organization and the voice of the treasury and finance profession. It establishes professional certification (Certified Treasury Professional, CTP), professional standards, and a code of ethics for finance professionals to follow (www.afponline.org).

Institute of Internal Auditors. The Institute of Internal Auditors (IIA) is a professional organization and the voice of the internal auditing profession worldwide. It establishes professional certifications (CIA and CCSA), professional standards, and a code of ethics for internal auditors to follow. CIA is Certified Internal Auditor and CCSA is Certification in Control Self-Assessment (www.theiia.org).

International Federation of Accountants. The mission of the International Federation of Accountants (IFAC) is the worldwide development and enhancement of an accountancy profession with harmonized standards, one able to provide services of consistently high quality in the public interest (www.ifac.org).

Chartered Financial Analyst Institute. The Chartered Financial Analyst Institute (CFA Institute) is a professional organization and is the voice of financial and investment analysts. It establishes professional certification (Certified Financial Analyst, CFA), professional standards, and a code of ethics for financial analysts to follow (www.cfainstitute.org).

The American College. The American College is an educational organization and is the voice of underwriters, financial planners, and others. It establishes professional certifications (e.g., CLU and CFP), professional standards, and a code of ethics for underwriters and financial planners to follow. CLU is Chartered Life Underwriter and CFP is Certified Financial Planner (www.theamericancollege.edu).

Additional Resources

Anand, Sanjay. *Sarbanes-Oxley Guide for Finance and Information Technology Professionals*. Hoboken, NJ: John Wiley & Sons, 2006.

Bragg, Steven M. *Accounting Best Practices*, fifth edition. Hoboken, NJ: John Wiley & Sons, 2007.

Bragg, Steven M. *Accounting Control Best Practices*. Hoboken, NJ: John Wiley & Sons, 2006.

Horcher, Karen A. *Essentials of Measuring Treasury*. Hoboken, NJ: John Wiley & Sons, 2005

Institute of Management and Administration. *Cost Reduction and Control Best Practices*, second edition Hoboken, NJ: John Wiley & Sons, 2005.

Notes

1. U.S. General Accounting Office, *Executive Guide: Creating Value Through World-Class Financial Management* (GAO/AIMD-00-134), Washington, DC: April 2000.
2. GAO, *Financial Management: Outsourcing of Finance and Accounting Functions* (GAO/AIMD/NSIAD-98-43), Washington, DC: Oct. 1997.
3. *See* note 1.
4. *Id.*
5. GAO, *U.S. Infrastructure: Funding Trends and Opportunities to Improve Investment Decisions* (GAO/RCED/AIMD-00-35), Washington, DC: Feb. 2000.
6. *See* note 2.
7. GAO, *Standards for Internal Control in the Federal Government* (GAO/AIMD-00-21.3.1), Washington, DC: Nov. 1999.

CHAPTER 11

INFORMATION-TECHNOLOGY MANAGEMENT BEST PRACTICES

11.1 OVERVIEW

The information technology (IT) vision must support an organization's mission and be closely aligned with its strategic business plan and the organization's budget. The vision also serves as a framework for IT decision making and support standards, and it facilitates the sharing of information across the organization.

IT Fiscal Authority and Strategic Vision

Centralize IT fiscal authority, since doing so increases the likelihood of success in organization-wide implementation of a strategic vision.

Strategic management of information should include the definition and improvement of business practices that support the organization's mission. Management's goals are information sharing, information integration, and systems standardization on an organization-wide basis. The results can be improved customer support, reduced costs, or cost savings.

The lack of a company-wide focus on information management often leads to the development of and perpetuation of stovepipe (legacy) systems. These systems are characteristically developed to solve a specific problem, have a limited focus and functionality, and contain data that cannot be easily shared with other systems. Stovepipe systems represent a common barrier to successful corporate information management, and investment in such systems should be reduced drastically to facilitate information sharing across organizational boundaries. The goal is to provide information in a seamless manner, transparent to the end user or customer.

11.2 ROLES AND RESPONSIBILITIES OF CHIEF INFORMATION OFFICER

The Chief Information Officer (CIO) is a key person in the C-level executive suite and has the following roles and responsibilities:

- Linking IT strategy with business strategy
- Integrating IT administration, planning, system development and maintenance, telecommunications and networks, and computer operations functions for maximum efficiency and effectiveness

- Delivering value-based information to functional management and senior management to facilitate quality decision making and to gain a competitive advantage
- Reducing investment in stovepipe (legacy) systems and slowly retire them by developing new systems that integrate seamlessly with other systems
- Aligning system processes with business processes to increase employee performance and productivity by reducing paper-driven manual systems and end-user ad hoc systems
- Ensuring that business application systems (e.g., accounts payable and inventory) are flexible and that they do not limit internal and external customer service offerings
- Improving data quality, data usability, data integration, data communications, and data sharing to authorized individuals
- Implementing a business continuity plan to provide a stable business functions and operations with resilient computer systems.
- Implementing data dictionaries and metadata repositories to facilitate data management and control
- Linking IT service costs to cash flows and gross profits
- Increasing faster IT-service deliveries to internal customers to achieve their total satisfaction
- Implementing new IT technologies and processes by leveraging technology to improve quality and to reduce costs
- Eliminating non-value-added activities in IT service to trim waste and lower costs
- Focusing more on value-added activities in IT services to provide a solid value to the internal customers and to the organization
- Identifying key drivers of cost, quality, risks, expenses, revenues, profits, business growth, competition, and performance. Focus on the root causes of these drivers and understand why these drivers go up and down
- Seamlessly integrating the back-end systems with the front-end systems for (1) maximum data consistency, completeness, and accuracy, (2) better customer service and satisfaction, and (3) stronger connection of disparate and disconnected business processes
- Building standardized, transparent, and repeatable IT service processes to provide the stable, consistent, and quality products and services that customers expect
- Understanding that increases in sales velocity increase inventory velocity, which, in turn, increases production or service velocity, finance velocity, human capital velocity, and systems velocity. His goal is to synchronize these velocities in a cohesive manner.
- Implementing the goal congruence concept by linking individual employee goals with those of the department/division and the organization. He must remove or reduce the competing or conflicting goals.
- Implementing crosscutting best practices across business units, divisions, departments, and functions through busting silos and building bridges

- Linking employee rewards, bonuses, and promotions to employees' true performance and tangible results, and empower employees
- Building solid working relationships with C-level executives in marketing, manufacturing, finance, human resources, and other functions through formal and informal approaches at the workplace
- Fostering ethical values and cultural sensitivity in light of workforce diversity
- Encouraging employees to continuously acquire and improve their knowledge, skills, and abilities (KSAs) through targeted training courses, management development programs, and professional certifications
- Establishing a solid and sustainable chain of knowledge linked through the entire management hierarchy to ensure adequate core knowledge competencies for all levels of employees in the organization
- Inviting IT audits, special management reviews, and self-assessments periodically and proactively to ensure continuous improvement in IT service quality, cost, and delivery
- Encouraging employees at all levels of the organization to think differently and radically (i.e., out-of-the-box thinking) at all times, which can lead to new perspectives providing best-of-breed solutions
- Participating in the succession-planning process for key positions
- Adhering to IT professional and ethical standards established by the relevant professional bodies
- Analyzing outside-in views (i.e., views of stakeholders about company management) and inside-out views (i.e., views of company management about stakeholders) to identify disconnections between these views and to integrate them in a coherent manner

11.3 WORLD-CLASS INFORMATION TECHNOLOGY MANAGEMENT

(a) IT STRATEGY. The focus of IT management should be on strategic issues and not so much on technical issues. This is because the impact of IT is pervasive, affecting the entire organization. What IT management does and does not do directly affects the quality of data, quality of systems, and quality of decision making in the organization. In short, wrong data can lead to wrong decisions. Since IT function is so critical to the overall success and survival of an organization, senior executives should pay attention to IT governance and control structures and, despite the area's technical nature, should not delegate this important responsibility to lower-level managers.

CRITICAL SUCCESS FACTORS FOR A WORLD-CLASS IT FUNCTION

Critical success factors for a world-class IT function include value creation to organizations; meeting organization mission needs; IT governance and control; hardware and software reliability, redundancy, and recovery capabilities; quality of interconnecting systems; listening to stakeholder voices; leadership; organizational culture; customer service; organizational structure; technology; process; and people.

(b) LISTENING TO STAKEHOLDER VOICES. IT management, as a developer and maintainer of computer systems for the company, should pay close attention in understanding and listening to the following "voices" to achieve organizational goals and to improve overall performance. When these "voices" are heard together, they bring attention to new perspectives and creative conflicts, forcing new thinking that leads to new solutions (i.e., best-of-breed solutions). Listening to the collective voice of many stakeholders at once will have a greater impact than listening to one voice at a time in isolation, because the former requires a balanced approach after considering all party's concerns.

For each content of each voice, a T-Column analysis should be prepared, with "what happens if I listen to this voice" in the left column (benefits) and "what happens if I don't listen to this voice" in the right column (costs and risks). A comparative analysis of each content in each column will point to new problems requiring new solutions.

- Voice of the customer (external customers such as suppliers, vendors, contractors, consultants, key customers, regulators, investors, creditors, the stock market, and media/press, and internal customers such as the board of directors, corporate management, and employees in other functional departments, such as manufacturing, marketing, finance, and human resources)
- Voice of the process (process flows, process variations, process delays and waste, and process inefficiencies)
- Voice of quality (TQM principles and practices; mistake-proofing; continuous improvement; cost of poor quality; quality assurance, quality control, quality audits, quality council, and quality circles; walkthroughs and desk reviews during system planning, design, programming, and testing)
- Voice of standards (business-application system design, programming, and testing standards; telecommunications and network standards; system security standards; data/information sharing and integration standards; Web-based standards; IT architecture standards; data/information privacy standards; and software piracy standards)
- Voice of partners (system development and maintenance contractors and consultants; electronic-commerce trading firms; outsourcing vendors; IT contingency-plan support vendors; insurance companies, supply chain members; financial institutions; shipping/transportation carriers; governmental agencies; and third-party computer service providers)
- Voice of regulators (federal, state, and local laws and regulations)
- Voice of competitors (press releases, Web site pressrooms, industry magazines, daily business newspapers, advertising magazines, industry trade shows, product demonstrations and promotions, direct mail, e-mail campaigns, copyright/ trademark/ patent news, business intelligence news, banner advertising, billboard and street advertising, product sponsorships, and online events and chat rooms)

(c) IT CYCLE TIME MEASURES. Cycle time reduction in IT deals with reducing the system-initiation-to-system-implementation cycle time, with associated benefits such as increased productivity, improved utilization of human and machine resources, decreased costs, and improved customer service. The goal is to develop and implement new computer systems on time and on budget, all the time. To attain these benefits, organizations must:

- Eliminate or decrease non-value-added activities (e.g., legacy [stovepipe] systems; fully paper-driven manual systems; transferring manually keyed data into computer systems; printing computer system data into forms for further manual processing; transaction-processing systems with a repeated sequence of computer-manual-computer work steps instead of computer-to-computer work steps; manual processing of computer operations work; rework steps; waiting time; and delays at the interdepartmental and interdivisional boundaries and at intradepartmental work stations).
- Enhance or increase value-added activities (e.g., seamless integration of back-end systems with front-end systems; data transfer points between internal systems and external systems; integration between the Internet, Intranet, and Extranet systems; data backup and archiving points; integration between computer systems, phone, facsimile, and voice response technologies; connection points between wired systems and wireless systems; decision-support systems for managers and executives; internal/external-customer access points to business application systems; IT project hold points, and IT-management decision points and control points).

This requires having the right employees enjoying the right access to the right systems from anywhere and at anytime so that delays in IT systems and operations are decreased and data/information sharing is facilitated.

(d) IT METRICS. IT management should develop and measure the following metrics to improve its overall performance:

- Percentage increase or decrease in IT's annual operating budget, expressed as a percentage of organization's sales, revenues, costs, or profits this year and compared to previous years
- Percentage increase or decrease in IT's workforce count, expressed as a percentage of organization's total workforce count this year and compared to previous years
- Percentage increase or decrease in IT employees' annual training, development, and education budget, expressed as a percentage of the organization's total budget for employees' annual training, development, and education, this year and compared to previous years
- Number of times a new business-application-system development project was completed on time in a given time period
- Number of times a new business-application-system development project was completed on budget in a given time period
- Ratio of a specific business application system's maintenance cost to the same system's development cost. As this ratio reaches 1.0, it is an indication of a functionally unstable system requiring redesign.
- Number of legacy systems that are still in operation
- Total amount of fines and penalties paid, this year and compared to previous years, due to use of pirated software by employees. This includes both illegally copied software and software that violated licensing restrictions.
- Percentage increase or decrease in system uptime. The higher the system uptime, the greater system availability is for system users.

- Average time to grant, change, and remove system access privileges for an individual
- Number of times the IT service level agreements (SLAs) with internal customers were met
- Percentage increase or decrease in server utilization rates, this year and compared to previous years
- Percentage increase or decrease in data storage utilization rates, this year and compared to previous years
- Percentage decrease in the number of computer security breaches, this year and compared to previous years
- Percentage of sensitive data protected from internal and external threats, this year and compared to previous years
- Elapsed time between computer workload–forecasting periods. Delayed forecasting leads to inaccurate or inadequate capacity planning, which in turn causes poor system performance and degradation of services to system users.

(e) STRATEGIC INFORMATION-MANAGEMENT BEST PRACTICES. Strategic information management typically involves defining a mission based on customer segments and needs; establishing core processes that accomplish the mission; understanding the key decisions that guide mission delivery processes; supporting those decisions by making the right information available to the right people at the right time; and using technology to collect, process, and disseminate information in ways that improve the delivery of products, goods, and services to customers.[1]

Leading organizations have used a consistent set of best practices to improve mission performance through strategic information management. These practices worked because, over time, they institutionalized new ways of doing business that are required for capturing the value of information and information technology. They are most effective when implemented together as mutually reinforcing activities, rather than as ad hoc efforts.

These best practices are grouped into three functions critical to building a modern information-management infrastructure: (1) deciding to change and work differently (i.e., initiate, mandate, and facilitate major changes in information management to improve performance), (2) directing resources toward high-value uses or changes (i.e., establish an outcome-oriented, integrated strategic information-management process), and (3) supporting the change or improvement with the right skills, roles, and responsibilities (i.e., build organization-wide information management capabilities to address mission needs).

(i) Function 1: Decide to Change. Senior management in leading organizations made a personal commitment to improve by: (1) recognizing the need to fundamentally change information management, (2) creating line management ownership in order to incorporate information management into business planning, and (3) taking specific actions to maintain momentum over time. The result of this commitment was a serious, motivated, sustainable improvement effort that had a wide impact throughout the entire organization.

Best Practice 1: Recognize and communicate the urgency of changing information management practices. The successful implementor will (1) assess mission performance and the contribution made by information and technology assets (i.e., knowledge assets), (2) clearly understand how information management is critical to

solving performance-related problems and exploiting opportunities, and (3) communicate specific mission-related performance problems and make the business case for changing the current information management approach.

Best Practice 2: Get line management involved and create ownership. The successful implementor will (1) hold line management accountable for the mission impact of information management and (2) get line managers meaningfully involved in critical information management decisions.

Best Practice 3: Take action and maintain momentum. The successful implementor will (1) act short term—exploit or create windows of opportunity to signal or reinforce an improvement initiative, (2) think long term—clearly set directions, goals, and milestones for an information management program, (3) pick and place internal champions who will shepherd day-to-day improvement actions, and (4) establish incentives tied to successful resolution of performance problems identified by top management.

(ii) Function 2: Direct Change. Once an organization has made a serious commitment to change its management of information and technology, it is paramount that an outcome-oriented, integrated strategic information-management process be institutionalized. This requires that organizations (1) make external-customer needs and mission goals the central driver of all organizational improvement efforts, (2) make serious efforts to objectively measure performance, (3) focus on process improvement, (4) tightly control information technology investments, and (5) integrate the planning, budgeting, and performance assessment processes.

Best Practice 4: Anchor strategic planning in customer needs and mission goals. The successful implementor will (1) match external- and internal-customer group needs with specific products and services, (2) link customer group needs to specific mission problems and assess corresponding opportunities, (3) focus strategic planning on highest-priority customer needs and mission goals, and (4) set explicit mission goals that tailor products and services to the needs of key customer groups.

Best Practice 5: Measure the performance of key mission-delivery processes. The successful implementor will (1) focus performance measures on gauging service to key external customers within individual customer groups, (2) embed performance measures in key management processes—including planning, budgeting, investment selection, and performance evaluation—to influence decision making and support continuous improvement, (3) use internal and external benchmarks to help assess relative performance, and (4) tailor performance measures to gauge the mission value of information management (e.g., clearly show whether information-systems projects make a difference).

Elements of IT Strategic Planning Cycle

- Long-term strategic and information planning
- Systems life cycle and project level planning
- Budget review
- Performance assessment
- IT architecture management

Best Practice 6: Focus on process improvement in the context of IT architecture. The successful implementor will (1) establish and manage a comprehensive architecture

that ensures the appropriate integration of mission-critical information systems through common standards and that emphasizes local control and flexibility in adapting to new processes and technologies, (2) distinguish large-scale improvement efforts from others by concentrating on order-of-magnitude improvements in cost, quality, or timeliness, (3) focus strategic resources, at the right time, on a limited number of large-scale process improvement efforts, (4) target efforts at core mission-delivery processes (defined as those that, because of their cost and/or importance to customers, have a unique potential for return on investment), and (5) use a combination of controlled development and rapid prototyping to minimize risk and maximize benefits.

Best Practice 7: Manage IT projects as investments. The successful implementor will (1) link information systems decisions tightly to budget decisions and focus them on mission improvement, (2) establish a high-level investment review board that fully involves senior managers to help in key decision throughout a project's life cycle, (3) use a disciplined process—based on explicit decision criteria and quantifiable measures assessing mission benefits, risk, and cost—to select, control, and evaluate IT projects using post-implementation reviews, (4) make IT projects as narrow in scope and brief in duration as possible in order to reduce risk and increase the probability of success, and (5) balance the proportion of system maintenance expenditure versus strategic investment in system development.

Best Practice 8: Integrate the planning, budgeting, and evaluation processes. The successful implementor will (1) put all five elements of the strategic planning cycle in place—long-term strategic and information planning, systems life-cycle and project-level planning, budget review, performance assessment, and architecture management, (2) require executive and senior management to fully participate in and take responsibility for all major IT project decisions throughout their life cycle, (3) integrate key elements of the strategic planning process by ensuring that outputs of one are used as inputs for the next, and (4) use the strategic planning process to manage operations and make key decisions and assessments by top management—especially those involving budgets and IT investments.

(iii) Function 3: Support Change. Neither a commitment to change nor directed activities can succeed unless the necessary skills and resources have been defined and provided. The goal is to build a new level of sustainable organization-wide capabilities that address mission needs. In order to achieve this goal, leading organizations have defined clear responsibilities for line managers and IT professionals, established a CIO as a senior management partner, and worked to anticipate and define necessary key skills. Consequently, their management processes work have begun working fluidly, rates of innovation have increased, and conflict has been minimized.

Best Practice 9: Establish customer/supplier relationships between line and IT professionals. The successful implementor will (1) make line managers responsible for identifying critical information and performance needs, work requirements, and economic benefits of mission improvement projects, (2) make IT professionals responsible for supporting line managers as investment counselors and product/service providers, (3) clarify roles and responsibilities at the corporate, mission, and project levels, focusing corporate management on reinforcing accountability and facilitating mission success, (4) manage the organizational architecture with a bias toward local control and ownership,

but with a strong central counterbalance to maximize cross-cutting systems integration needs, and (5) rigorously understand the economies of IT functions as well as the product/service needs of line management customers.

Best Practice 10: Position a CIO as a senior management partner. The successful implementor will (1) understand the mission and work closely as a peer with top management to help increase awareness, understanding, and skill in identifying and resolving information management issues, (2) catalyze, design, and facilitate implementation of new organizational capabilities by clearly articulating the role of IT in mission improvement, and (3) bridge gaps between top management, line-user management, and IT management by acting as an adviser and architect.

Best Practice 11: Upgrade skills and knowledge of user line management and IT professionals. The successful implementor will (1) teach line executives and managers how to identify important IT issues, opportunities, and decisions, (2) ensure that IT professionals acquire line-management and leadership skills, (3) identify existing skills, explicitly target future skills, and move systematically to new levels of capability, and (4) find the right mix of technology-dependent and -independent skills.

(iv) Benefits of Strategic Information Management. Implementing these 11 best practices, combined with other mutually reinforcing management-improvement initiatives such as total quality management, can yield the following benefits:

- *Increased productivity:* Productivity benefits allow an organization to cope with rising workloads in an environment of shrinking resources.
- *Improved customer service:* Fewer mistakes and faster, easier, and more valuable services narrow the gap between customer expectations and delivery of products and services.
- *Higher returns on IT investments:* Investments are made today based on the promise of achieving net benefits in mission performance tomorrow.
- *Lower risks of failure, delay, and overspending:* With established, systematic processes, IT projects can be more predictable, timely, carefully managed, and affordable on a consistent basis. In the near term, low-value projects can be eliminated or stopped, unnecessary risks can be uncovered and mitigated, existing projects can be given an increased likelihood of success, and productivity improvements in IT operations can be stimulated. In the long term, the combination of process improvement and technology has the potential to reduce costs, improve quality of products and services, and increase responsiveness to customers.

Exhibit 11.1 summarizes the 11 best practices needed to build a modern IT management infrastructure.

(f) CRITICAL SUCCESS FACTORS FOR A CIO. Leading organizations found with regards to information technology that there are three critical success factors and six fundamental principles. Along with these, we list key characteristics of organizations that successfully execute a given principle. These key characteristics can provide insights into what constitutes successful CIO.[2]

(i) Critical Success Factor 1: Align IT leadership for value creation. **Principle 1: Recognize the role of IT in creating value.** Key characteristics include (1) IT

Decide to Change	Direct Change	Support Change
1. Recognize and communicate the urgency of changing information management practices	4. Anchor strategic planning in customer needs and mission goals	9. Establish customer/supplier relationships between line and IT professionals
2. Get line management involved and create ownership	5. Measure the performance of key mission-delivery processes	10. Position a CIO as a senior management partner
3. Take action and maintain momentum	6. Focus on process improvement in the context of IT architecture	11. Upgrade skills and knowledge of user line management and IT professionals
	7. Manage IT projects as investments 8. Integrate planning, budgeting, and evaluation processes	

Exhibit 11.1 Summary of Best Practices for Building a Modern IT Management Infrastructure

organizational functions and processes are incorporated into the overall business process, and (2) Mechanisms and structures are adopted that facilitate an understanding of IT and its impact on the organization's overall strategic direction.

Principle 2: Position the CIO for success. Key characteristics include (1) The CIO model is consistent with organizational and business needs, (2) The roles, responsibilities, and accountabilities of the CIO position are clearly defined, (3) The CIO has the right technical and management skills to meet business needs, and (4) The CIO is a full member of the senior-management team.

(ii) Critical Success Factor 2: Promote organizational credibility. **Principle 3: Ensure the credibility of the IT organization.** Key characteristics include (1) The CIO has a legitimate and influential role in leading top managers to apply IT to meet business objectives, (2) The CIO has the commitment of line management and its cooperation and trust in carrying out IT projects and initiatives, (3) The CIO accomplishes quick, high-impact, and visible IT successes in balance with longer term strategies, and (4) The CIO learns from and partners with successful leaders in the external IT community.

Principle 4: Measure success and demonstrate results. Key characteristics include (1) IT managers engage both their internal and external partners and customers when defining measures, (2) Management at all levels ensures that technical measures are balanced with business measures, and (3) Managers continually work at establishing active feedback between performance measures and business measures.

(iii) Critical Success Factor 3: Execute IT responsibilities. **Principle 5: Organize IT to meet business needs**. Key characteristics include (1) The IT organization has a clear understanding of its responsibilities in meeting business needs, (2) The extent of

decentralization of IT resources and decision making is driven by business needs, (3) The structure of the IT organization is flexible enough to adapt to changing business needs, (4) Outsourcing decisions are made based on business requirements and the IT organization's human capital strategy, and (5) The IT organization executes its responsibilities reliably and efficiently.

Principle 6: Develop IT human capital. Key characteristics include (1) The IT organization identifies the skills necessary to effectively implement IT in line with business needs, (2) The IT organization develops innovative ways to attract and retain human talent, and (3) The IT organization provides training, tools, and methods to skilled IT professionals in order to perform their duties.

11.4 INFORMATION TECHNOLOGY GOVERNANCE

(a) IT GOVERNANCE DEFINITION. IT governance is and should be a part of corporate governance. In the information economy, successful enterprises integrate IT and business strategies, culture, and ethics in order to attain business objectives, optimize information value, and capitalize on technologies. Extended enterprises, which incorporate customers, business partners, vendors, stakeholders, and constituents, rely on the efficient and effective sharing of information, including goals, expectations, status, and ultimately knowledge. Making this happen at all is mission-critical to most enterprises—and making it happen as it should happen requires IT governance.[3]

Effective enterprise governance focuses on individual and group expertise and experience where it can be most productive, monitors and measures performance, and provides assurance regarding critical issues. IT, long considered solely an enabler of an enterprise's strategy, must now be regarded as an integral part of that strategy. CEOs, CFOs, and CIOs alike agree that strategic alignment between IT and enterprise objectives is a critical success factor.

IT governance helps ensure achievement of this critical success factor by efficiently and effectively deploying secure, reliable information and applied technology. IT governance is a structure of relationships and processes used to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes. The relationships are between management and its governing body. The processes cover setting objectives, giving direction on how to attain them, and measuring performance.

Simply put, IT is so critical to the success of enterprises that it is an issue that cannot be relegated solely to management or to IT specialists, but must instead receive the focused attention of both.

(b) RELATIONSHIP OF ENTERPRISE AND IT GOVERNANCE. Looking at the interplay of enterprise and IT-governance processes in more detail, enterprise governance (the system by which entities are directed and controlled) drives and sets IT governance. At the same time, IT should provide critical input to and form an important component of strategic plans. IT may in fact influence strategic opportunities outlined by the enterprise.[4]

Enterprise activities require information from IT activities in order to meet business objectives. Successful organizations ensure interdependence between their strategic planning and their IT activities. IT must be aligned with and enable the enterprise to take full advantage of its information, thereby maximizing benefits, capitalizing on opportunities, and gaining a competitive advantage.

(c) HOW ENTERPRISE AND IT GOVERNANCE WORK. Enterprises set objectives, the attainment of which is governed by generally accepted good (or best) practices.[5] From these objectives flows the organization's direction, which dictates certain enterprise activities and deployment of enterprise resources. The results of the enterprise activities are measured and reported on, which provides input for the constant revision and maintenance of the controls and thus launches the cycle again.

IT also is governed by good (or best) practices to ensure that the enterprise's information and related technology support its business objectives, that its resources are used responsibly, and that risks are managed appropriately. These practices form a basis for direction of IT activities, which can be characterized as planning and organizing, acquiring and implementing, delivering and supporting, and monitoring, for the dual purposes of managing risks (to gain security, reliability, and compliance), and realizing benefits (increasing effectiveness and efficiency). Reports are issued on the outcomes of IT activities, which are measured against the various practices and controls, and the cycle begins again.

IT governance is an inclusive term, which encompasses:

- Information systems, technology, and communication
- Business, legal, and other issues
- All concerned stakeholders, directors, senior management, process owners, IT suppliers, users, auditors, etc.

How can IT governance, control, and assurance impact an enterprise's effectiveness?

- By addressing business issues, such as electronic commerce and enterprise resource planning (ERP)
- By assuring security, reliability, and integrity of strategic information
- By protecting the enterprise's investment in IT, including systems and networks
- By ensuring the appropriate management of an entity's information assets, which are often directly responsible for the success and survival of the entity itself

Simply put, IT governance is good business.

(d) IT GOVERNANCE BEST PRACTICES. Organizations should do the following to establish and maintain their IT governance function:

- Develop a charter for the IT governance function describing the function's mission, vision, goals and objectives, duties and responsibilities, and authority in the organization.
- Appoint an IT Corporate Governance Officer reporting to the CGO and not to the CIO. Similarly, an IT Security Governance Officer should report to the IT Corporate Governance Officer, not to the CIO.
- Link IT governance objectives to corporate governance objectives.
- Link IT security governance objectives to IT governance objectives.
- Allocate budget to the proper functioning of IT governance function.
- Prepare periodic reports to the Board of Directors of the organization on IT Governance issues and problems, explaining their resolution along with open issues and problems.

11.5 INFORMATION TECHNOLOGY CHANGE MANAGEMENT

(a) OVERVIEW. The scope of IT change management includes changes in systems software, hardware, applications software, and networks and their associated equipment. For example, applications software for an order-processing system may require changes if a company acquires or merges with another company.

Organizational culture (employees) can be the most troubling factor in implementing organizational changes. Organizational culture may be defined as the underlying assumptions, beliefs, values, attitudes, and expectations shared by an organization's employees. An organization's beliefs and values affect the behavior of its employees. Many organizations are actively trying to perpetuate some cultural values and change others to increase their chances for being competitive or effective.

(i) Principle 1: Become a facilitator of change and orchestrate management of change associated with IT implementation. **Best Practices and Procedures for Principle 1**. The IT function should serve as a facilitator on organization-wide information support issues such as change management. Change in an environment or work system can have a tremendous impact upon people, processes, and products. The impact goes beyond change in work processes to the introduction of new technology. Perhaps the biggest effect is on the people in the environment that is changing.

Most people find change unsettling. It can cause failures in implementing new business practices if not well planned. In fact, most failures of system changes can be attributed to poorly managed effects on people, not to the complexity of the technology change. This applies whether one personal computer is introduced into the workplace or an entire work system is redesigned and supported with brand-new equipment. People are the most valuable asset for any organization, and any transition affecting this precious investment must be well thought out and implemented, not left to chance. Change management skills are essential during change, and such skills should either be developed or acquired.

(ii) Principle 2: Develop and enforce policies and procedures for definition and assignment of accountability and authority. **Best Practices and Procedures for Principle 2**. Line executives must have the final responsibility for decisions on the use of IT products and services. With responsibility comes accountability for ensuring the realization of promised benefits. Placing accountability and responsibility at the appropriate level will enable the organization and its departments to be more effective in achieving mission-aligned outcomes and meeting customers' needs.

(iii) Principle 3: Build relationships with business unit function heads and their staff. **Best Practices and Procedures for Principle 3**. Good customer relationships between the IT function and other business functions are important for achieving high performance levels. Communication about IT issues must occur throughout the organization. One approach is through the installation of a high-level chief information officer (CIO) to serve as a bridge between functional management and the IT function. A CIO is a member of the executive team, involved in all aspects of the IT function, and helps senior management develop a strategic vision and leadership in IT.

(iv) Principle 4: Manage current and emerging trends. **Best Practices and Procedures for Principle 4**. It is critical that the IT function stay abreast of changing technologies and trends affecting information management, and that it position the organization to take advantage of those that apply. Implementation of specific trend adaptations that will accommodate an organization's unique context is crucial to success. Examples of current and emerging trends include electronic commerce, open systems environments, energy-efficient computers, remote computing, outsourcing, and virtual departments/divisions.

11.6 INFORMATION TECHNOLOGY UTILITY SERVICE AND VALUE

(a) OVERVIEW. The concept of technology utility service is similar to other utilities, such as telephone, electricity, gas, and water services. A primary goal is that IT systems and services should be available to authorized individuals, any time and anywhere, with the click of a mouse or by the touch of a keyboard. A secondary goal is to provide information value to end users, with the right information put into the hands of the right people at the right time. To accomplish these goals of utility and value, a concept of system uptime is essential, which is expressed as the percentage of time a computer system is available for the end users to do their work.

(i) Principle 1: Provide an IT utility service function within an organization. **Best Practices and Procedures for Principle 1**. The primary objective of building an IT utility strategy is to put in place a comprehensive organization-wide IT management infrastructure that will support the general needs of the functional-user community. The underlying premise of this "public utility" concept or model is that the greatest economies can be derived from a fully integrated organization-wide technology platform, the promulgation and enforcement of standards, and the centralized provision of certain types of common services. To put the utility service function into effect requires (1) implementation of a comprehensive IT base focusing on attributes such as flexibility, expandability, portability, compatibility, and standardization, (2) end-user business units assuming the responsibility for identifying and planning for development of new computer-based application systems and applying the IT utility strategy to better achieve their objectives, and (3) establishing and enforcing organization-wide standards, methodologies, and tools. A top-down standardization program will include wide-ranging elements such as communications protocols, a prescribed set of data management tools, a life-cycle methodology, documentation standards, and security standards.

One example of implementation of the IT utility concept is a bank that implemented a comprehensive base of central-computing resources and a global communications network. This utility now supports the bank's operations in thousands of locations worldwide. Implementation was characterized by strong direction and control of the technology architecture, application of standards, the delegation of responsibility for the application of technology to line business areas, and a linkage between IT and business strategy within each area.

Another example of implementation of the IT utility concept is an insurance company that implemented a comprehensive base of central-computing resources, tools, and methodologies over thousands of databases and a global communications network to support a staff of thousands. The technology base is now used as a utility to support

individual business areas that form "partnerships" with the central information-support service units. Among the characteristics of this successful program were centralized planning of the technology base, company-wide standards, methodologies and tools, organization-wide architecture encompassing many field offices, and the support of all levels of management.

(ii) Principle 2: Market IT services internally to senior management and functional-user management. **Best Practices and Procedures for Principle 2**. IT management should educate all levels of management within an organization regarding the type of services the IT function can offer them. IT staff should be seen as internal consultants, technical assistants, and problem-solving partners.

IT management should obtain periodic input from the business functions of the organization. This feedback can take the form of surveys, face-to-face meetings, group interviews, newsletters, and focus groups. From this information, internal customer needs are identified and plans can be established to address their needs.

(iii) Principle 3: Increase system uptime to 99.5% or higher in order to provide a greater utility and value to system customers. **Best Practice 1: Develop and Monitor Hardware Reliability Metrics.** The hardware metrics are a means of evaluating the amount of processing time lost due to the failure of the computer system or a specific system component. Among the measurements of interest are (1) the number of times the hardware ceases to function on a given time period (i.e., failure rate), (2) the average length of time the hardware is functional (i.e., mean time between failures [MTBF]), (3) the amount of time it takes to resume normal operation (i.e., mean time to repair [MTTR]), and (4) the quantity of service (i.e., system availability).[6]

Best Practice 2: Develop and monitor software reliability metrics. Hardware metric should be supplemented with the software metrics. Hardware failures are either transient or repeatable, and they result from design, development, and component fault, whereas software failures are almost always repeatable and originate in design and development. Software metrics include (1) the number of errors that occur in the source code, (2) percentage of errors during a given time interval, (3) the number of error types and the name of program modules in which they occur, and (4) errors caused by deficiencies or the inclusion of extraneous functions in the system design specification, documentation, or source code. The metrics should be limited to errors caused by software deviating from its specifications while the hardware is functioning correctly.

Best Practice 3: Develop and monitor human reliability metrics. Human reliability metrics differs from those for hardware or software. Differences stem from the ability of a person to make decisions, to learn from experience, and to continue functioning in spite of a mistake or failure. The failures that should be assessed by the metrics include (1) incorrect diagnosis of a problem, (2) misinterpretation of instructions, (3) inadequate support or environmental conditions, and (4) insufficient attention or caution.

Best Practice 4: Develop and monitor system availability metrics. System availability is the amount of time the overall computer system is operational and usable. The achievement of a predetermined availability threshold can be used to indicate acceptable, substandard, or unacceptable performance levels. The subsystems (such as CPU memory, disk storage, server, or printer) that are causing downtime should be measured, tracked, and corrected.

Best Practice 5: Develop and monitor system stability metrics. System stability is the average amount of time the system is operational before user services are interrupted, loss of work results, or a system reboot is required. The achievement of a predetermined stability threshold can be used to indicate acceptable, substandard, or unacceptable performance levels. The subsystems (such as CPU memory, disk storage, and software module 1 through N) that are causing downtime and interruptions should be measured, tracked, and corrected.

Best Practice 6: Develop and monitor system survivability metrics. System survivability is the probability that the system will continue to perform after a portion of the system becomes inoperable. Examples of metrics include (1) the number of hardware and software failures, (2) the ability of the system to recover from the failure, (3) the amount of system usage, and (4) the amount of damage that could result from a failure.

Best Practice 7: Develop and implement fault avoidance techniques. The goal of a fault avoidance approach is to reduce or eliminate the possibility of a fault through design practices such as using quality components, integrating system components, and verifying, validating, and testing conducted throughout the system development life cycle (SDLC) to ensure the correctness, completeness, and consistency of the final software product. To achieve fault avoidance, all components of the system (hardware and software) must function correctly at all times.

Best Practice 8: Develop and implement fault tolerance techniques. The goal of a fault tolerance approach is to preserve the continued correct execution of functions after the occurrence of a selected set of faults. This is achieved through redundancy techniques such as the addition of hardware and software or repetition of operations beyond those minimally required for normal system operation. Both timers and timeouts are used to control a computer process.

Best Practice 9: Develop and implement system redundancy principles. A system planner can establish several principles of redundancy such as switching between duplicate systems, providing system and power backups, performing system reconfigurations, keeping software archives, establishing preventive maintenance policies, and requiring support personnel (i.e., operators, analysts, and technicians) to diagnose and act when a problem occurs and to prevent or minimize loss of information or loss of system availability.

Redundant array of inexpensive or independent disks (RAID) technology uses several disks in a single logical subsystem. The main purpose of RAID is to provide backup so if one disk fails, all of the data is immediately available from the other disks. To reduce or eliminate downtime from disk failure, database servers may employ disk shadowing, disk duplexing, and disk/server mirroring concepts. A disk-shadowing subsystem includes two physical disks. User data is written to both disks at once. If one disk fails, all of the data is immediately available from the other disk. In disk duplexing, a disk controller is duplicated (whereas in disk mirroring a physical disk is duplicated). In a server-mirroring concept, there are two servers, the primary and secondary, operating in parallel. When the primary server fails, the secondary server automatically takes control of the network.

Best Practice 10: Develop and implement system recovery strategies. The purpose of recovery is to restore the computer system to a correctly functioning state from an erroneous one. The reliability objectives, the effects of a fault, and the system's

tolerance of the resulting errors must be understood and considered in the determination of a recovery strategy. The strategy requires two things: (1) establishing procedures to recover from a failure and restart the system quickly and (2) implementing recovery levels (i.e., full, degraded, and safe shutdown) to establish the level of computing achieved through recovery procedures.

1. **Recovery Procedures.** The system planner needs to evaluate the system requirements with respect to (1) the amount of time between the occurrence of a failure and the start of the recovery process, (2) the amount of time between the initiation of recovery and the restoration of the system, and (3) the amount of human interaction in terms of maintenance required to restore the system.
2. **Recovery Levels.** Full recovery returns the system to the set of conditions existing prior to the failure. Degraded recovery means the system is returned to an operational state but with a reduced computing capacity. Safe shutdown occurs when the system cannot maintain a minimum level of computing capacity. The system is shut down with as little damage and as much warning as possible. The objective of these recovery levels is to avoid a hard, complete crash of the system.

11.7 INFORMATION TECHNOLOGY PERFORMANCE MANAGEMENT

(a) OVERVIEW. In leading organizations, there is commitment to IT measures and their rigorous use in decision making at all management levels in order to improve IT performance. IT performance management and measures are considered subsets of overall performance-management systems for the entire organization. Moreover, an effective partnership is forged between IT and the enterprise and operational customers so that IT objectives and measures are jointly achieved. Organizational goals and objectives drive IT goals, functions, and measures. Organizational customers define the mission objectives, while IT management and staff determine how IT can best support them. The three primary practice areas that characterize IT performance management are align, construct, and implement, which in turn are supported by one reinforce area.[7]

(i) Practice Area 1: Align—Aligning IT systems with organization's missions, goals, and programs. **Best Practice 1: Follow an IT "results chain."** Leading organizations build and enforce a disciplined flow from goals to objectives to measures and individual accountability. They define specific goals, objectives, and measures, and use a diversity of measure types, and describe how IT outputs and outcomes impact operational-customer and enterprise-business delivery requirements. The IT-performance management system does not optimize individual customer results at the expense of an enterprise perspective.

(ii) Practice Area 2: Construct—Constructing measures that determine how well IT is supporting strategic, customer, and internal business needs. **Best Practice 2: Follow a balanced scorecard approach.** Leading organizations translate organizational strategy and IT performance expectations into a comprehensive view of both operational and strategic measures. Four generic goal areas include meeting the strategic needs of the enterprise, meeting the needs of individual operational customers, addressing internal IT business performance, and addressing ongoing IT innovation and learning.

(iii) Practice Area 3: Implement—Implementing performance measurement mechanisms at various decision-making levels within an organization. **Best Practice 3: Target measures, results, and accountability at different decision-making levels.** For the balanced scorecard areas, leading organizations match measures and performance results to various decision-making tiers or levels. These tiers include enterprise executives, senior- to mid-level managers responsible for program or support units, and lower-level management running specific operations or projects. Individual appraisals tie IT performance to incentives.

(iv) Practice Area 4: Reinforce—Emphasizing the baselining, benchmarking, and improving. **Best Practice 4: Build a comprehensive measure, data collection, and analysis capability.** Leading organizations give considerable attention to baselining, benchmarking, and the collection and analysis of IT performance information. They use a variety of data collection and analysis tools and methods that serve to keep them informed without imposing unnecessary reporting burdens. They also periodically review the appropriateness of their current measures.

Best Practice 5: Improve performance of IT business processes to better support mission goals. In the leading organizations, IT performance improvement begins and ends with IT business processes. Organizations map their IT business processes and prioritize among those processes that must be improved to support enterprise and operational customers' business processes.

(v) Practice Area 5: Develop and monitor performance measurements for major IT programs. **Best Practices and Procedures for Practice Area 5.** Developing performance measures has many tangible benefits. Performance measures provide a way of quantifying the relative success or failure of an organization program. A system of performance measures can provide a methodology for focusing on an organization's mission, quantifying the business process that contributes to the mission, and evaluating among competing priorities for improvement. This can be accomplished, in part, through outcome-based goals and sound workforce plans.

Examples of Performance Measures

- Mission support
- Quality
- Time
- Cost
- Customer satisfaction

Through performance measures, an IT organization can establish yardsticks against which to evaluate progress in attaining its information goals. Business processes must first be understood and baselined before they can be improved—then the impact of changes can be measured and consciously selected. To be successful in supporting the organization's mission, IT measures must relate to business processes. Performance measures must be defined and monitored and adjustments must be made throughout the life cycle and across key processes, through collaboration between IT and other business functions.

Performance measures also provide a means for evaluating customer satisfaction with the organization's products and services.

When developing performance measures, the old adage "less is more" is appropriate. A few meaningful measures that focus on effectiveness should be developed, since they are the key indicators of performance. Efficiency measures, which look at "pieces" of processes, are generally more numerous and represent resource consumption, such as personnel and expenditures. Costs must be associated with key programs and activities; they can thus provide important inputs to the funding process.

EXAMPLES OF IT PERFORMANCE-MEASUREMENT TECHNIQUES (PERFORMANCE INDICATORS)

1. Balanced Scorecard—IT Strategic Measures

Objective	Enterprise mission goals
Sample Measures	Percentage of mission improvements (cost, time, quality) attributable to IT solutions and services
	Percentage of planned IT benefits projected versus realized
Objective	Portfolio analysis and management
Sample Measures	Percentage of IT portfolio reviewed and disposed
	Percentage of old applications retired
	Percentage of applications retirement plan achieved
	Percentage of reusable core application modules
	Percentage of new IT investment versus total spending
Objective	Financial and investment performance
Sample Measures	Percentage and cost of services provided in-house versus industry standard
	IT budget as a percentage of operational budget and compared to industry average
	Net present value, internal rate of return, return on investment, and return of net assets
Objective	IT resource usage
Sample Measures	Percentage of consolidated/shared resources across units
	Percentage of cross-unit shared database and applications
	Percentage of hardware/software with interoperability capabilities

2. Balanced Scorecard—IT Customer Measures

Objective	Customer partnership and involvement
Sample Measures	Percentage of projects using integrated project teams
	Percentage of joint IT customer/supplier service-level agreements
Objective	Customer satisfaction
Sample Measures	Percentage of customers satisfied with IT product delivery
	Percentage of customers satisfied with IT problem resolution
	Percentage of customers satisfied with IT maintenance and support
	Percentage of customers satisfied with IT training
	Percentage of service-level agreements met
	Percentage of products launched on time
Objective	Business process support
Sample Measures	Percentage of IT solutions supporting process-improvement projects
	Percentage of users covered by training to use new IT solutions
	Percentage of new users able to use applications unaided after initial training

3. Balanced Scorecard—IT Internal Business Measures

Objective	Applications development and maintenance
Sample Measures	Number of function points delivered per labor hour
	Number of defects per 100 function points at user acceptance
	Number of critical defects per 100 function points in production
	Percentage of decrease in application-software failures, problems
	Mean time to resolve critical defects
	Cycle time for development
Objective	Project performance
Sample Measures	Percentage of projects on time, on budget
	Percentage of projects meeting functionality requirements
	Percentage of projects using standard methodology for systems analysis and design
Objective	Infrastructure availability
Sample Measures	Percentage of computer availability
	Percentage of communications availability
	Percentage of applications availability (uptime)
	On-line systems availability (uptime)
Objective	Enterprise-architecture standards compliance
Sample Measures	Number of variations from standards detected by review and audit per year
	Percentage of increase in systems using architecture
	Percentage of staff trained in relevant standards

4. Balanced Scorecard—IT Innovation and Learning Measures

Objective	Workforce competency and development
Sample Measures	Percentage of staff trained in use of new technologies and techniques
	Percentage of staff professionally certified
	Percentage of IT management staff trained in management skills
	Percentage of IT budget devoted to training and staff development
Objective	Advanced technology use
Sample Measures	Percentage of employees skilled in advanced technology applications
	Number of dollars available to support advanced-technology-related skills development
Objective	Methodology currency
Sample Measures	Currency of application-development methods used
	Percentage of employees skilled in advanced-application development methods
	Percentage of projects developed using recognized methods and tools
Objective	Employee satisfaction and retention
Sample Measures	Percentage of employee satisfaction with the capability of the existing technical and operating environment to support mission
	Percentage of employee turnover by function

11.8 INFORMATION TECHNOLOGY CONTRACT MANAGEMENT

(a) OVERVIEW. In acquiring IT goods and services, organizations will identify business requirements, including consideration of security and control of resources, and protection of privacy. Prior to entering into a contract, organizations should analyze risks, benefits, and costs.[8]

(b) MANAGEMENT OF RISK. Types of risk may include schedule risk, risk of technical obsolescence, cost risk, risk implicit in a particular contract type, technical feasibility, dependencies between a new project and other projects or systems, the number of simultaneous high-risk projects to be monitored, funding availability, and management risk.

Appropriate techniques should be applied to manage and mitigate risks during the acquisition of IT resources. Techniques include but are not limited to: (1) prudent project management, (2) use of modular contracting, (3) thorough acquisition planning tied to budget planning, (4) continuous collection and evaluation of risk-based assessment data, (5) prototyping prior to implementation, (6) post-implementation reviews to determine actual project cost, benefits, and returns, and (7) focusing on risks and returns using quantifiable measures.

(c) MODULAR CONTRACTING. Modular contracting means use of one or more contracts to acquire IT systems in successive, interoperable increments. Modular contracting is applied to acquisition of major systems and is intended to reduce risk and to increase incentives for contractor performance.

(d) CONTRACT TYPES. There are several contract types, including fixed-price contracts, cost-reimbursement contracts, incentive contracts, time-and-materials contracts, and performance-based contracts.

- **Fixed-Price Contracts.** Fixed-price types of contracts provide for a firm price or, in appropriate cases, an adjustable price. Fixed-price contracts providing for an adjustable price may include a ceiling price, a target price (including target cost), or both.
- **Cost-Reimbursement Contracts.** Cost-reimbursement types of contracts provide for payment of allowable incurred costs, to the extent prescribed in the contract. These contracts establish (1) an estimate of total cost for the purpose of obligating funds, and (2) a ceiling that the contractor may not exceed (except at its own risk) without the approval of the contracting officer.
- **Incentive Contracts.** Incentive contracts are applicable when a firm fixed-price contract is not appropriate and the required goods or services can be acquired at lower costs and, in certain instances, with improved delivery or technical performance. Incentive contracts relate the amount of profit or fee to the contractor's performance.
- **Time-and-Materials Contract.** A time-and-materials contract may be used only when it is not possible at the time of signing the contract to estimate accurately the extent or duration of the work or to anticipate costs with any reasonable degree of confidence.
- **Performance-Based Contracts.** Performance-based contracting methods are intended to ensure that required performance-quality levels are achieved and that total payment is related to the degree that services performed meet contract standards.

  Performance-based contracts (1) describe the requirements in terms of results required rather than the methods of performance of the work, (2) use measurable

performance standards (e.g., quality, timeliness, quantity) and quality-assurance surveillance plans, (3) specify procedures for fee reductions and reductions to the price of a fixed-price contract when services are not performed or do not meet contract requirements, and (4) include performance incentives where appropriate.

Factors in Selecting Contract Types

- Price competition
- Price analysis
- Cost analysis
- Type and complexity of the requirement
- Urgency of the requirement
- Period of performance or length of production run
- Contractor's technical capability and financial responsibility
- Concurrent contracts
- Extent and nature of proposed subcontracting
- Acquisition history

(e) COMPETITION REQUIREMENTS. "Full and open competition" means that all responsible sources are permitted to compete. Contracts based on anything other than full and open competition must be justified in writing.

"Sole source acquisition" means the organization has solicited and negotiated with only one source. All single-source acquisitions must be justified in writing.

"Sealed bidding" is used if (1) time permits the solicitation, submission, and evaluation of sealed bids, (2) the award will be made on the basis of price and other price-related factors, and (3) there is a reasonable expectation of receiving more than one sealed bid.

"Competitive proposals" are used if sealed bids are not appropriate.

(f) VALUE ENGINEERING. Value engineering is the formal technique by which contractors may (1) voluntarily suggest methods for performing more economically and share in any resulting savings, or (2) be required to establish a program to identify methods for performing more economically. Value engineering attempts to eliminate, without impairing essential functions or characteristics, anything that increases acquisition, operation, or support costs.

(g) QUALITY ASSURANCE. Contracts must safeguard the organization's quality and quantity requirements, including inspection, acceptance, warranty, and other measures associated with quality requirements.

(h) CONTRACT CLAUSES. The contracting officer shall insert in solicitations and contracts for IT a Privacy or Security Safeguards clause to define necessary security measures, and/or clauses spelling out requirements for the design, development, or operation of computer systems.

11.9 INFORMATION TECHNOLOGY INVESTMENT MANAGEMENT

(a) INTEGRATED APPROACH TO IT INVESTMENT MANAGEMENT. An IT-investment management process is an integrated approach to managing IT investments that provides for the continuous identification, selection, control, life cycle management, and evaluation of IT investments. This structured process provides a systematic method for organizations to minimize risks while maximizing the return on IT investments.[9]

To be most successful, an IT-investment management process should have elements of three essential phases—Select, Control, and Evaluate. However, each phase should not be viewed as a separate step. Rather, each is conducted as part of a continual, interdependent management effort. Information from one phase is used to support activities in the other two phases.

SELECT VERSUS CONTROL VERSUS EVALUATE

Select	How do you know you have selected the best projects?
Control	What are you doing to ensure that the projects will deliver the benefits projected?
Evaluate	Based on your evaluation, did the system deliver what you expected?

(b) CRITICAL SUCCESS FACTORS IN IT-INVESTMENT MANAGEMENT. To be successful, an organization's IT-investment management processes should generally include the following elements or factors:

- Key organizational decision-makers are committed to the process and are involved throughout each project's life cycle. Projects are assessed jointly by operational, financial, and IT managers.
- The investment management process is repeatable, efficient, and conducted uniformly and completely across the organization.
- The process includes provisions for continually selecting, managing, and evaluating projects in the investment portfolio.
- Decisions are made consistently throughout the organization:
  - Decisions at any level of the organization are made using uniform decision criteria.
  - Decisions are driven by accurate and up-to-date cost, risk, and benefit information.
  - Decisions are made from an overall mission focus (there is an explicit link with the goals and objectives established in the organization's strategic plan or annual performance plans and with the organization's IT architecture).
- Accountability and learning from previous projects are reinforced.
- The emphasis is on optimizing the portfolio mix in order to manage the risk and maximize the rate of return.
- The process incorporates all IT investments but recognizes and allows for differences between various project types (mission-critical, administrative, infrastructure) and phases (proposed, under development, operational, etc.).

(c) DIMENSIONS OF THE IT-INVESTMENT EVALUATION APPROACH. Investment evaluators can assess the Select, Control, and Evaluate phases from three review levels—process, data, and decisions. In addition to these three phases, there are three critical attributes—repeatability, efficiency, and completeness—that cut across each phase and that should be assessed at each review level.

(i) Process. This is an assessment of the investment management processes that the organization is following to select IT investments, control the investments and monitor their progress, and evaluate final results. The central question to be answered is "Does the organization have defined, documented processes for selecting, controlling, and evaluating its IT investments?" The goal in assessing an organization's processes is to identify to what extent the organization has a structure in place for managing and evaluating IT investments.

(ii) Data. An IT investment process cannot operate without accurate, reliable, and up-to-date data on project costs, benefits, and risks. It is the basis for informed decision making. In addition, documentation of management decisions is essential to begin to assemble a track record of results. Evaluating the data involved in the IT-investment management process requires evaluating two different types of data:

- ex ante—the information that is being used as inputs to the IT investment process (e.g., the cost, benefit, and risk analyses that are used to justify the selection and continued funding of projects, the performance measures that are used to monitor a project's progress, etc.)
- ex post—information that is produced based on decisions that are made (e.g., project review schedules and risk mitigation plans should be developed once a decision is made to fund a project)

All projects (proposed, under development, operational, etc.) should have complete and accurate project information—cost and benefit data, risk assessments, links to business goals and objectives, and performance measures, as well as up-to-date project-specific data, including current costs, implementation plans, staffing plans, and performance levels. In addition, the organization should have qualitative and quantitative project requirements and decision criteria in place to help screen IT projects, assess and rank projects, and control and evaluate the projects as they move through the various phases of their life cycle.

All management actions and decisions that are made should be documented and maintained. Moreover, some decisions require that additional information be produced. For instance, after a project is selected, project-specific review schedules and risk mitigation plans should be developed.

(iii) Decisions. After evaluating the processes that the organization uses to select, control, and evaluate IT investments and the data that are used to make decisions, evaluators will be in a much better position to reach conclusions about the specific decisions that the organization is making. The central focus of analysis is on whether management decisions and actions are being taken using the investment control processes and requisite project data.

The IT investment portfolio should represent a mixture of those projects that best meet the mission needs of the organization. Projects in the portfolio should be consistently monitored, and decisions should be made at key milestones to ensure that the project continues to have its expected business impact with a focus on minimizing risk and maximizing return. Completed projects are evaluated to compare actual performance levels to estimated levels, and to feed lessons learned back into the Selection and Control phases.

(iv) Repeatability. Repeatability focuses on the extent to which the processes, data, or decisions being reviewed are conducted consistently over time and across different organizational units (recognizing that processes should naturally evolve as lessons are learned and improvements are made).

- Projects are selected uniformly across more than one budget cycle; project reviews are conducted for all projects at established intervals; an evaluation methodology is in place and is used to assess all fully implemented projects.
- The organization has identified all necessary information (cost/benefit/risk analyses, proposed schedule, user and business requirements, etc.) for making decisions, and this information is maintained, updated, and used to drive all project decisions. Specific, quantifiable decision criteria have been established and are used at all decision levels.
- Projects are selected and managed based on established criteria or documented justifications.

Two essential aspects of repeatability are whether (1) roles, responsibilities, and authority have been defined and documented, and (2) uniform decision criteria are in place.

(v) Efficiency. Efficiency focuses on how well management processes, the generation of project data, and the function of decision making are working together. The focus is on the overall quality (the accuracy, reliability, and timeliness) of the investment approach. In addition, the same data generated to support IT investment selection, control, and evaluation should be used to manage IT projects through their life cycle.

- All projects are subjected to a similar investment management process (consisting of Select, Control, and Evaluate phases), and this process is documented so that everyone knows the steps that are conducted and the analyses that are required.
- Cost, risk, and benefit data, both qualitative and quantitative, are accurate and are updated as information is gained. Project information is readily available, and an organization track record is maintained. Project results and lessons learned are tracked and aggregated in order to further refine and improve decision-making.
- Decisions are being made at the right level. Senior managers' limited time is being utilized to the best extent possible. Actions are quickly taken to address deficiencies

(vi) Completeness. Completeness focuses on the extent to which all phases of the process (Select, Control, and Evaluate) are being followed and whether use of the IT investment process is institutionalized across the organization. As the evaluation is conducted and questions are asked, a concerted effort should be made to keep these three critical factors in mind. Evaluators should continually ask themselves whether the processes, data, or decisions that they are assessing are repeatable, efficient, and complete.

(d) KEY ELEMENTS IN IT INVESTMENT MANAGEMENT. Below is a combination of three phases (i.e., Select, Control, and Evaluate) with three review levels (i.e., Process, Data, and Decisions):

- **Select-Process.** Selection processes include (1) screening projects, (2) analyzing and ranking all projects based on benefit, cost, and risk criteria, (3) selecting a portfolio of projects, and (4) establishing project-review schedules.
- **Select-Data.** Selection data include (1) evidence that each project has met project submission requirements, (2) analyses of each project's costs, benefits, and risks, (3) data on the existing portfolio, and (4) scoring and prioritization outcomes, and (5) project-review schedules.
- **Select-Decisions.** Selection decisions include (1) determining whether projects met process-stipulated requirements, and (2) deciding upon the mixture of projects in the overall IT investment portfolio.
- **Control-Process.** Control processes include (1) consistently monitoring projects, (2) involving the right people, (3) documenting all major actions and decisions, and (4) feeding lessons learned back in to the Selection phase.
- **Control-Data.** Control data include (1) measures of interim results and (2) updated analyses of each project's costs, benefits, schedule, and risks.
- **Control-Decisions.** Control decisions include (1) deciding whether to cancel, modify, continue, or accelerate a project, and (2) aggregating data and reviewing collective actions taken to date.
- **Evaluate-Process.** Evaluation processes include (1) conducting post-implementation reviews using a standard methodology and (2) feeding lessons learned back into the selection and control phases.
- **Evaluate-Data.** Evaluation data include (1) measurements of actual versus projected performance, and (2) a documented "track record" (project and process).
- **Evaluate-Decisions.** Evaluation decisions include (1) assessing the project's impact on mission performance and determining future prospects for the period, and (2) revising the Selection and Control phases based on lessons learned.

11.10 SYSTEM DEVELOPMENT AND ACQUISITION METHODOLOGY

(a) OVERVIEW. The system-development life cycle (SDLC) is the overall process of developing, implementing, and retiring information systems through a multistep process that continues from initiation, analysis, design, implementation, and maintenance to disposal. There are many different SDLC models and methodologies, but each generally consists of a series of defined steps or phases.[10]

Various SDLC methodologies have been developed to guide the processes involved, and some methods work better than others for specific types of projects.

Regardless of the type of life cycle used by an organization, information security must be integrated into the SDLC to ensure appropriate protection for the information that the system is intended to transmit, process, and store. Security is most useful and cost-effective when such integration begins with a system-development or integration-project initiation and is continued throughout SDLC by means of system disposal.

SDLC framework can consist of five phases to ensure the selection, acquisition, and use of appropriate and cost-effective security controls:

1. Initiation Phase
2. Development/Acquisition Phase
3. Implementation Phase
4. Operations/Maintenance Phase
5. Disposal Phase

(b) INITIATION PHASE. All IT projects have a starting point, what is commonly referred to as the initiation phase. During the initiation phase, the organization establishes the need for a particular system and documents its purpose. The information to be processed, transmitted, or stored is typically evaluated, as well as who must have access to such information and how (in high-level terms). In addition, it is often determined whether the project will be an independent information system or a component of an already defined system. A preliminary risk assessment is typically conducted in this phase, and initial security-planning documents are initiated (system security plan).

Once these tasks have been completed and a need has been recognized for a new or enhanced IT product or service, several processes must take place before the project is approved. These include clearly defining project goals and defining high-level information security requirements. Typically, during this phase, the organization defines high-level information security policy requirements as well as the enterprise security system architecture.

(c) DEVELOPMENT/ACQUISITION PHASE. During this phase, the system is designed, purchased, programmed, developed, or otherwise constructed. This phase often consists of other defined cycles, such as the system development cycle or the acquisition cycle.

During the first part of the development/acquisition phase, the organization should simultaneously define the system's security and functional requirements. These requirements can be expressed as technical features (e.g., access control), assurances (e.g., background checks for system developers), or operational practices (e.g., awareness and training). During the last part of this phase, the organization should perform developmental testing of the technical and security features/functions to ensure they perform as intended prior to launching the implementation and integration phase.

(d) IMPLEMENTATION PHASE. In the implementation phase, the organization configures and enables system security features, tests the functionality of these features, installs or implements the system, and then obtains formal authorization to operate the system. Design reviews and system tests should be performed before placing the system into operation, to ensure that it meets all required security specifications. In addition, if new controls are added to the application or the support system, additional acceptance tests of those new controls must be performed. This approach ensures that new controls

meet security specifications and do not conflict with or invalidate existing controls. The results of the design reviews and system tests should be fully documented, updated as new reviews or tests are performed, and maintained in the official organization records.

(e) OPERATIONS/MAINTENANCE PHASE. An effective security program demands comprehensive and continuous understanding of program and system weaknesses. In the operation and maintenance phase, systems and products are in place and operating, enhancements and/or modifications to the system are developed and tested, and hardware and/or software is added or replaced. During this phase, the organization should continuously monitor performance of the system to ensure that it is consistent with preestablished user and security requirements, and that needed system modifications are incorporated.

For configuration management (CM) and control, it is important to document the proposed or actual changes in the security plan of the system. Information systems are typically in a constant state of evolution, with upgrades to hardware, software, and firmware, and possible modifications to the surrounding environment where the system resides. Documenting information system changes and assessing the potential impact of these changes on the security of a system is an essential part of continuous monitoring, and key to avoiding a lapse in the system security accreditation.

Monitoring security controls helps to identify potential security-related problems in the information systems that are not identified during the security impact analysis, which is conducted as part of the CM and control process.

(f) DISPOSAL PHASE. The disposal phase of the system life cycle refers to the process of preserving (if applicable) and discarding system information, hardware, and software. This step is extremely important because, during this phase, information, hardware, and software are moved to another system, archived, discarded, or destroyed. If performed improperly, the disposal phase can result in the authorized disclosure of sensitive data. When archiving information, organizations should consider the need and methods for future retrieval. While electronic information is relatively easy to store and retrieve, problems can arise if the technology used to create the records is no longer available in the future as a result of obsolescence or incompatibility with new technologies. Additionally, the organization should consider what measures must be taken for the future use of data that has been encrypted, such as taking appropriate steps to ensure the secure long-term storage of cryptographic keys. It is equally important to consider legal requirements for records retention when disposing of information systems. For federal systems, system management officials should consult with their office responsible for retaining and archiving federal records.

The removal of information from a storage medium, such as a hard disk or tape, is called sanitization. There are four categories of media sanitization: disposal, clearing, purging, and destroying. Because different kinds of sanitization provide different levels of information protection, organizations should use information security requirements as a guide for selecting the sanitization method that best suits their needs.

(g) SYSTEM-DEVELOPMENT BEST PRACTICES. Organizations should develop and monitor the following metrics for SDLC:

- Percentage of systems that have the costs of their security controls integrated into the life cycle of the system. The purpose is to quantify the percentage of systems that are in compliance with the organization's requirement for integrating security costs into the system-development life cycle.
- Percentage of systems recertified if security controls are added or modified after the system was developed. The purpose is to measure compliance with a requirement for system review and recertification when security controls are added or modified after the system's development.
- Percentage of total systems that have been authorized for processing following certification and accreditation. The purpose is to determine the percentage of systems that are certified and accredited.

11.11 INFORMATION SECURITY MANAGEMENT

(a) OVERVIEW. Information systems have long been at some risk from malicious actions or inadvertent user errors and from natural and man-made disasters. In recent years, systems have become more susceptible to these threats because computers have become more interconnected and, thus, both more interdependent and accessible to a larger number of individuals. In addition, the number of individuals with computer skills is increasing, and intrusion or "hacking" techniques are becoming more widely known via the Internet and other media.[11]

(b) RISK MANAGEMENT CYCLE. Risk assessment is an essential element of risk management. Other elements include establishing a central-management focal point, implementing appropriate policies and related controls, promoting awareness, and monitoring and evaluating policy and control effectiveness.

Although all elements of the risk management cycle are important, risk assessments provide the foundation for other elements of the cycle. In particular, risk assessments provide a basis for establishing appropriate policies and selecting cost-effective techniques to implement these policies. Since risks and threats change over time, it is important that organizations periodically reassess risks and reconsider the appropriateness and effectiveness of the policies and controls they have selected. This is a continuing cycle of activity.

(c) RISK ASSESSMENT PROCESS. Risk assessments, whether they pertain to information security or other types of risk, are a means of providing decision makers with the information they need to understand factors that can negatively influence operations and outcomes and to make informed judgments concerning the extent of actions needed to reduce risk.

Regardless of the types of risk being considered, all risk assessments generally include the following elements:

- Identifying threats that could harm and, thus, adversely affect critical operations and assets. Threats include such things as intruders, criminals, disgruntled employees, terrorists, and natural disasters.
- Estimating the likelihood that such threats will materialize based on historical information and judgment of knowledgeable individuals

- Identifying and ranking the value, sensitivity, and criticality of the operations and assets that could be affected should a threat materialize in order to determine which operations and assets are the most important
- Estimating, for the most critical and sensitive assets and operations, the potential losses or damage that could occur if a threat materializes, including recovery costs
- Identifying cost-effective actions to mitigate or reduce the risk. These actions can include implementing new organizational policies and procedures as well as technical or physical controls.
- Documenting the results and developing action plan

There are various models and methods for assessing risk, and the extent of an analysis and the resources expended can vary depending on the scope of the assessment and the availability of reliable data on risk factors. In addition, the availability of data can affect the extent to which risk assessment results can be reliably quantified. A quantitative approach generally estimates the monetary cost of risk and risk reduction techniques based on (1) the likelihood that a damage event will occur, (2) the costs of potential losses, and (3) the costs of mitigating actions that could be taken. When reliable data on likelihood and costs are not available, a qualitative approach can be taken by defining risk in more subjective and general terms, such as high, medium, and low. In this regard, qualitative assessments depend more on the expertise, experience, and judgment of those conducting the assessment. It is also possible to use a combination of quantitative and qualitative methods.

(d) CRITICAL SUCCESS FACTORS IN RISK ASSESSMENT. Efficient and effective implementation of the organization's information security risk-assessment programs depends on a set of critical success factors. These factors help ensure that the organization benefits fully from the expertise and experience of its senior managers and staff, that risk assessments are conducted efficiently, and that the assessment results lead to appropriate remedial actions. The successful implementor should:

- *Obtain senior management support and involvement.* This support extends to participating in key aspects of the process, such as (1) assisting in determining the assessment's scope and the participants at the start of a new assessment, and (2) approving the action plan developed to respond to recommendations at the end.
- *Designate focal points at the corporate level to oversee and guide the organization's risk assessment processes.* These focal points facilitate the planning, performance, and reporting associated with the organization's risk assessment programs and help ensure that organization-wide issues are appropriately addressed.
- *Define procedures.* Each organization defines and documents procedures for conducting risk assessment and develops tools to facilitate and standardize the process. These, along with the use of focal points, help institutionalize the process, ensure a level of assessment consistency, and prevent individual business units from "reinventing the wheel" each time a new assessment is required. To provide flexibility, business units could supplement or alter procedures when needed. These modifications are often shared with other units in an effort to promote the use of best practices.

- *Involve business and technical experts.* Drawing on knowledge and expertise from a wide range of sources should be viewed as essential to ensuring that all-important risk factors are considered. Meetings conducted during the risk assessment process usually include a variety of individuals from the business unit, with expertise in business operations and processes, security, IT, audit, legal, and contractors as needed. It is good to rely exclusively on in-house personnel to perform the risk assessment rather than contractors, in order to keep the expertise in-house on a continuous basis.
- *Hold business units responsible.* Responsibility for initiating and conducting risk assessments, as well as following up on resulting recommendations, should lie primarily with the individual business units. Business units are considered to be in the best position to determine when an assessment is needed and to ensure that recommendations for risk reduction techniques resulting from the assessment are implemented effectively.
- *Limit scope of individual assessments.* Rather than conducting one large risk assessment covering all of an entity's operation at once, it is good to conduct a series of narrower assessments on various individual segments of the business. Consequently, the scope of each assessment is limited to a particular business unit or facility, or to a logically related set of operations or systems. Segmenting operations into logical units generally reduces the size of each assessment, making it more manageable to schedule and perform. In addition, segmenting operations provides organizations a means of ranking units to determine the order in which risk assessments would be performed and which units might merit more frequent risk assessments.
- *Document and maintain results.* Risk assessment results should be documented and maintained so that managers can be held accountable for the decisions made and a permanent record can be established. In this way, risk assessment records are available to serve as the starting point for subsequent risk assessments and as a ready source of useful information for managers new to the business unit. Documenting the process undertaken also permits others, such as the internal audit department, to ensure that organizational units are complying with company policy.
- *Develop tools to facilitate risk assessments.* Tools such as tables and matrices, databases, questionnaires, custom software, and standard report formats facilitate the conduct of the risk assessments. These tools help ensure a consistent and standardized approach throughout the organization and prevent teams from "reinventing the wheel" each time a new assessment is initiated.

(e) PRINCIPLES AND BEST PRACTICES IN RISK MANAGEMENT. Many leading organizations, both public and private, have adopted the following five principles and have implemented the following five principles and 16 best practices in their risk management cycle in order to manage the information security function.[12]

Principles

1. Assess risk and determine needs.
2. Establish a central-management focal point.

3. Implement appropriate policies and related controls.
4. Promote awareness.
5. Monitor and evaluate policy and control effectiveness.

Best Practices to Implement Principle 1: Assess Risk and Determine Needs

1. Recognize information resources as essential organizational assets that must be protected.
2. Develop practical risk assessment procedures that link security to business needs.
3. Hold business and program managers accountable.
4. Manage risk on a continuing basis.

Best Practices to Implement Principle 2: Establish a Central- Management Focal Point

5. Designate a central group to carry out key activities.
6. Provide the central group with ready and independent access to senior executives.
7. Designate dedicated funding and staff.
8. Enhance staff professionalism and technical skills.

Best Practices to Implement Principle 3: Implement Appropriate Policies and Related Controls

9. Link policies to business risks.
10. Distinguish between policies and guidelines.
11. Support policies through the central-security group.

Best Practices to Implement Principle 4: Promote Awareness

12. Continually educate users and others on risks and related policies.
13. Use attention-getting and user-friendly techniques.

Best Practices to Implement Principle 5: Monitor and Evaluate Policy and Control Effectiveness

14. Monitor factors that affect risk and indicate security effectiveness.
15. Use results to direct future efforts and hold managers accountable.
16. Be alert to new monitoring tools and techniques.

(f) IT-SECURITY ENGINEERING PRINCIPLES

(i) Purpose. The purpose of the engineering principles for IT security is to present a list of system-level security principles to be considered in the design, development, and operation of an information system. Ideally, the principles would be used from the onset of a program—at the beginning of or during the initiation phase—and then employed throughout the system's life cycle. However, these principles are also helpful in affirming and confirming the security posture of already deployed information systems. The principles are short and concise and can be used by organizations to develop their system life cycle policies.[13]

Effective *information assurance* rests on several system security concepts, namely (1) managing risk, not preventing it, (2) acknowledging that security is a system-level attribute, (3) recognizing that changes in mission or organization business processes increase the need for technical protection methods, (4) recognizing that the enterprise is made up of interrelated security domains, and (5) providing security mechanisms and services to support security implementation, both domain-specific and inter-domain–related.

(ii) Principles. There are 33 principles, grouped into six categories.

Category 1: Security Foundation

- Principle 1. Establish a sound security policy as the "foundation" for design.
- Principle 2. Treat security as an integral part of the overall system design.
- Principle 3. Clearly delineate the physical and logical security boundaries governed by associated security policies.
- Principle 4. Ensure that developers are trained in how to develop secure software.

Category 2: Risk Based

- Principle 5. Reduce risk to an acceptable level.
- Principle 6. Assume that external systems are insecure.
- Principle 7. Identify potential tradeoffs between risk reduction versus increased costs and decreases in other aspects of operational effectiveness.
- Principle 8. Implement tailored system security measures to meet organizational security goals.
- Principle 9. Protect information while it is being processed, in transit, and in storage.
- Principle 10. Consider custom-developed products to achieve adequate security. According to the Office of Management and Budget (OMB) Circular A-130, adequate security is defined as security commensurate with risk, including the magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.
- Principle 11. Protect against all likely classes of "attacks."

Category 3: Ease of Use

- Principle 12. Where possible, base security on open standards so as to promote portability and interoperability.
- Principle 13. Use common language in developing security requirements.
- Principle 14. Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process.
- Principle 15. Strive for operational ease of use.

Category 4: Greater Resilience

- Principle 16. Implement layered security to ensure no single point of vulnerability.
- Principle 17. Design and operate an IT system to limit damage and to be resilient in response.
- Principle 18. Provide assurance that the system is, and continues to be, resilient in the face of expected threats.

- Principle 19. Limit or contain vulnerabilities.
- Principle 20. Isolate public access systems from mission critical resources (e.g., data and processes).
- Principle 21. Use boundary mechanisms to separate computing systems and network infrastructures.
- Principle 22. Design and implement audit mechanisms to detect unauthorized use and to support incident investigations.
- Principle 23. Develop and exercise contingency or disaster-recovery procedures to ensure appropriate availability.

Category 5: Reduced Vulnerabilities

- Principle 24. Strive for simplicity.
- Principle 25. Minimize the system elements to be trusted.
- Principle 26. Implement "least privilege" access principle.
- Principle 27. Do not implement unnecessary security mechanisms.
- Principle 28. Ensure proper security in the shutdown or disposal of a system.
- Principle 29. Identify and prevent common errors and vulnerabilities.

Category 6: Network-Minded Design

- Principle 30. Implement security through a combination of measures distributed physically and logically.
- Principle 31. Formulate security measures to address multiple overlapping information domains.
- Principle 32. Authenticate users and processes to ensure appropriate access control decisions both within and across domains.
- Principle 33. Use unique identities to ensure accountability.

11.12 COMPUTER SECURITY INCIDENTS

(a) OVERVIEW. Attacks on information systems and networks have become more numerous, sophisticated, and severe in recent years. Preventing all such attacks would be the ideal course of action for organizations, but achieving this goal is not possible. Every organization that depends on information systems and networks to carry out its mission should identify and assess the risks to its systems and its information and reduce those risks to an acceptable level. An important component of this risk management process is to perform trending analysis on past computer security incidents and identify effective ways to deal with them. A well-defined incident response capability helps the organization detect incidents rapidly, minimize loss and destruction, identify weaknesses, and restore IT operations rapidly.[14]

(b) INCIDENT LIFE CYCLE. The major phases of the incident response process are preparation, detection and analysis, containment/eradication/recovery, and postincident activity. Exhibit 11.2 illustrates the incident response life cycle.

Exhibit 11.2 Incident Response Life Cycle

(i) Phase 1: Preparation. Incident preparation involves not only establishing an incident response capability so that the organization is ready to respond to incidents, but also preventing incidents by ensuring that systems, networks, and applications are afforded sufficient security. Incident prevention is now considered a fundamental component of incident response programs, also known as incident management programs, although the incident response team is not typically responsible for it. The incident response team's expertise should be used to establish recommendations for securing systems and preventing incidents, as much as possible. This section provides an overview of actions needed to prevent and handle incidents, including incident data-collection preparation.

(A) Preparing for Incident Response

Organizing an effective incident response capability involves the participation of many people within the organization. Making the right planning and implementation decisions is key to establishing a successful incident response program. One of the first planning tasks should be to develop an organization-specific definition of the term "incident" so that the scope of the term is clear. Additional tasks that should be performed during the preparation phase include the following:

(B) Creating an Incident Response Policy

The policy should define what events are considered incidents, establish the organizational structure for incident response, define roles and responsibilities, and list the organization's incident-reporting requirements.

(C) Developing Incident Response and Reporting Procedures

Based on the incident response policy, standard operating procedures (SOPs) are a delineation of the specific technical processes, techniques, checklists, and forms used by the incident response team. SOPs should be comprehensive and detailed to ensure that the organization's priorities are properly reflected in response operations. In addition, following standardized response procedures is also an effective way to minimize errors, particularly those that might be caused by incident-handling pace and stress. Prior to implementation, the organization should test incident response SOPs in order to validate their accuracy and usefulness. Once validated, the SOPs must be widely disseminated throughout the organization. Incidents can occur in countless and unpredictable ways; therefore, it is impractical to develop comprehensive procedures with step-by-step

instructions for handling every incident. The best that the organization can do is prepare to handle any type of incident and, more specifically, to handle common types of incidents.

(D) Establishing Guidelines for Communicating with External Parties

During the incident response process, the organization may need to communicate with outside parties, including other incident response teams, law enforcement, the media, vendors, and external victims. Because such communications often need to occur quickly, organizations should have predetermined communication guidelines so that only the appropriate information is shared with the right parties. If sensitive information is inappropriately released, it can lead to greater disruption and financial loss than the incident itself. Creating and maintaining a list of internal and external points of contact (POCs), along with backups for each contact, should assist in making communications among parties easier and faster.

(E) Defining Incident-Response Team Services

Although the main focus of an incident response team is performing incident response, most teams offer additional services. Examples of the types of services an incident response team can provide to the organization include security advisory distribution, vulnerability assessment, intrusion detection, and education and awareness.

(F) Selecting a Team Structure and Staffing Model

The organization should select the team structure and staffing model best suited to its needs. When contemplating the best team structure and staffing model, an organization should considers several factors, such as the size of the organization, the geographic diversity of major computing resources, the need for 24/7 availability, cost, and staff expertise.

(G) Staffing and Training the Incident Response Team

Members of the incident response team should have excellent technical and problem-solving skills because these are critical to the team's success. Excellent teamwork, organizational, communication, and speaking skills are important as well. Most incident response teams have a team manager and a deputy team manager who assumes authority in the absence of the team manager. In addition, some teams also have a technical lead who assumes oversight of and final responsibility for the quality of the technical work performed by the entire incident response team. Also, larger teams often assign an incident lead as the primary POC for handling a specific incident.

Organizational complexity typically makes it a challenge to handle large-scale incidents. Many people within the organization may play a role in the incident response, and the organization may need to communicate rapidly and efficiently with various external groups. Collecting, organizing, and analyzing all the pieces of information so that the right decisions can be made and executed are not easy tasks. The key to maintaining situational awareness is to prepare thoroughly to handle large-scale incidents. Two specific actions that support this matter are as follows:

(H) Establishing and Maintaining Accurate Notification Mechanisms

Organizations should establish, document, maintain, and exercise on-hour and off-hour contact and notification mechanisms for various individuals and groups within the organization (e.g., CIO, head of information security, IT support, business continuity planning) and outside the organization (e.g., incident response organizations, counterparts at other organizations).

(I) Developing Written Guidelines for Prioritizing Incidents

Incident response teams should assign each incident the appropriate priority, based on the criticality of the affected resources and the current and potential technical effect of the incident. For example, data destruction at a user workstation might result in a minor loss of productivity, whereas root compromise of a public Web server might result in a major loss of revenue, productivity, access to services, and reputation, as well as the release of confidential data (e.g., credit card numbers, social security numbers). Because incident responders normally work under stressful conditions ripe for human error, it is important to clearly define and articulate the incident-handling priority process. The incident-handling priority process should include a description of how the incident response team should react under various circumstances, as well as a service-level agreement (SLA) that documents appropriate actions and maximum response times. This prioritization should facilitate faster and more consistent decision making.

(J) Preparing to Collect Incident Data

Organizations should be prepared to collect a set of objective and subjective data for each incident. Over time, the incident data collected by the organization can be used for many ends. For example, data on the total number of hours the incident response team has dedicated to incident response activities, and the activities' cost over a particular period of time, may be used to justify additional funding of the incident response team. A study of incident characteristics may reveal systemic security weaknesses and threats, changes in incident trends, or other data that can be used in support of the risk assessment process. Another good use of the data is measuring the success of the incident response team. If incident data is collected and stored properly, it should provide several measures of the success (or at least the activities) of the incident response team.

In the process of preparing to collect incident data, organizations should focus on collecting data that is actionable, rather than collecting data simply because it is available. Absolute numbers are not informative—what matters is to understand how findings represent threats to and vulnerabilities of the organization's business processes. Organizations should decide what incident data to collect based on reporting requirements and on the expected return on investment from the data (e.g., identifying a new threat and mitigating the related vulnerabilities before they can be exploited).

(K) Preventing Incidents

Preventing problems is normally less costly and more effective than reacting to them. Thus, incident prevention is an important complement to an incident response capability. If security controls are insufficient, high volumes of incidents may occur, overwhelming the resources and capacity for response, which would result in delayed or incomplete recovery, possibly more extensive damage, and longer periods of service unavailability. Incident handling can be performed more effectively if organizations complement their

incident response capability with adequate resources to actively maintain the security of networks, systems, and applications. This process is intended to reduce the frequency of incidents, thereby allowing the incident response team to focus on handling serious incidents.

Examples of best practices that help to prevent incidents are as follows:

- Having a patch management program to assist system administrators in identifying, acquiring, testing, and deploying patches that eliminate known vulnerabilities in systems and applications
- Hardening all hosts appropriately to eliminate vulnerabilities and configuration weaknesses
- Configuring the network perimeter to deny all activity that is not expressly permitted
- Deploying software throughout the organization to detect and stop malicious code
- Making users aware of policies and procedures on the appropriate use of networks, systems, and applications

(ii) Phase 2: Detection and Analysis. For many organizations, the most challenging aspects of the incident response process are detection and analysis—that is, determining whether an incident has occurred and, if so, the type, extent, and magnitude of the problem. Incidents can be detected through many different means, with varying levels of detail and fidelity. Automated detection capabilities include network-based and host-based intrusion detection systems (IDSs), anti-virus software, and log analyzers. Incidents may also be detected through manual means, such as user reports. Some incidents have overt signs that can be easily detected, whereas others are virtually undetectable without automation.

In a typical organization, the thousands or millions of possible signs of incidents that occur any given day are recorded mainly by computer security software. Automation is needed to perform an initial analysis of the data and select events of interest for human review. Event correlation software and centralized logging can be of great value in automating the analysis process. However, the effectiveness of the process depends on the quality of the data that goes into it. Organizations should establish logging standards and procedures to ensure that logs and security software collect adequate information and that the data is reviewed regularly. Proper and efficient reviews of incident-related data require people with extensive, specialized technical knowledge and experience.

When a potential incident is identified, the incident response team should work quickly to analyze and validate it, documenting each step taken. The team should rapidly perform an initial analysis to determine the incident's scope, attack methods, and targeted vulnerabilities. This analysis should provide enough information for the team to prioritize subsequent activities, including the containment of the incident. When in doubt, incident handlers should assume the worst until additional analyses indicate otherwise. In addition to prioritization guidelines, organizations should also establish an escalation process for those instances when the incident response team fails to respond to an incident within the designated time.

The incident response team should maintain records about the status of incidents, along with other pertinent information. Using an application or database for this purpose is necessary to ensure that incidents are handled and resolved in a timely manner.

The incident response team should safeguard this data, and other data related to incidents, because it often contains sensitive information concerning recent security breaches, exploited vulnerabilities, and users that may have performed inappropriate actions.

(iii) Phase 3: Containment, Eradication, and Recovery. To avoid overwhelming resources and to keep damage in check, it is important to contain an incident before it spreads. Most incidents require containment, so it is important to consider it early in the course of handling each incident. An essential part of containment is decision making, such as choosing to shut down a system, disconnect it from the network, or disable certain system functions. Such decisions are much easier to make if strategies and procedures for containing the incident have been predetermined.

Organizations should define acceptable risks in dealing with incidents and develop strategies accordingly.

Containment strategies vary based on the type of incident. For example, the overall strategy for containing an e-mail–borne virus infection is quite different from that used against a network-based distributed denial of service (DoS) attack. Organizations should create separate containment strategies for each major type of incident. The criteria for choosing the appropriate strategy should be documented clearly to facilitate quick and effective decision making. Examples of criteria include potential damage to and theft of resources, the need to preserve evidence, the effectiveness of the strategy, the time and resources needed to implement the strategy, and the duration of the solution.

After an incident has been contained, eradication may be necessary to eliminate components of the incident, for instance by deleting malicious code and disabling breached user accounts. For some incidents, eradication is either unnecessary or is performed during recovery. During recovery, administrators restore systems to normal operation and (if applicable) harden systems to prevent similar incidents. Recovery may involve such actions as:

- Restoring systems from clean backups
- Rebuilding systems from scratch
- Replacing compromised files with clean versions
- Installing patches
- Changing passwords
- Tightening network perimeter security (e.g., firewall rule sets)

It is also often desirable to employ higher levels of system logging or network monitoring as part of the recovery process. Once a resource is successfully attacked, it is often attacked again or other resources within the organization are attacked in a similar manner.

(iv) Phase 4: Postincident Activity. After a major incident has been handled, the organization should hold a lessons-learned meeting to review the effectiveness of the incident-handling process and identify necessary improvements to existing security controls and practices. Lessons-learned meetings should also be held periodically for lesser incidents. The information accumulated from all lessons-learned meetings, as well as the data collected while handling each incident, should be used to identify systemic security weaknesses and deficiencies in policies and procedures. Follow-up reports generated for

each resolved incident can be important for evidentiary purposes, used as a reference in handling future incidents, and used in training new incident response team members. An incident database, with detailed information on each incident that occurs, can be another valuable source of information for incident handlers.

Organizations should decide what incident data to collect based on reporting requirements and on the expected return on investment from the data (e.g., identifying a new threat and mitigating the related vulnerabilities before they can be exploited).

(c) COMPUTER-SECURITY INCIDENTS BEST PRACTICES. Organizations should develop and monitor the following metrics to manage computer security incidents properly:

- **Number of unauthorized access-incidents performed by insiders.** A large number in this metric could prompt stronger policy provisions concerning background investigations for personnel, misuse of computing resources, and the safeguarding of internal networks by security controls (e.g., deploying intrusion detection software to more internal networks and hosts).
- **Number of incidents handled.** Handling more incidents is not necessarily better—for example, the number of incidents handled may decrease because of better network- and host-security controls, not because of negligence by the incident response team. The number of incidents handled is best taken as a measure of the relative amount of work that the incident response team had to perform, not as a measure of the quality of the team.
- **Time per incident.** For each incident, time can be measured in several ways, such as (1) total amount of labor spent working on the incident, (2) elapsed time from the beginning of the incident to its resolution, (3) elapsed time for each stage of the incident-handling process (e.g., containment and recovery), and (4) elapsed time before the team's responding to the initial report of the incident.
- **Objective assessment of each incident.** The response to an incident that has been resolved can be analyzed to determine how effective it was. Examples of performing an objective assessment of an incident include (1) reviewing logs, forms, reports and other incident documentation for adherence to established incident-response policies and procedures, (2) identifying which precursors and indications of the incident were recorded, so as to determine how effectively the incident was logged, (3) determining if the incident caused damage before it was detected, (4) determining if the actual cause of the incident was identified, (5) calculating the estimated monetary damage from the incident, and (6) identifying which measures, if any, could have prevented the incident.
- **Subjective assessment of each incident.** Incident response team members may be asked to assess their own performance, as well as that of other team members and of the entire team. Another valuable source of input is the owner of a resource that was attacked; ask if the owner thinks the incident was handled efficiently and if the outcome was satisfactory.
- **Compliance.** Percentage of business units with computer-incident handling and response capability. The purpose is to ensure that there is an organization-wide computer-incident response capability in place.

- **Reporting.** Number of computer incidents reported to local law enforcement authorities. The purpose is to determine the level of appropriate and timely reporting to local law enforcement authorities.

(d) CONTROLS FOR HANDLING COMPUTER SECURITY INCIDENTS BY LIFE CYCLE PHASE

(i) Phase 1. Preparation. Below is a summary of controls required to handle computer security incidents in the preparation phase:

General

- Acquire tools and resources that may be of value during incident handling.
- Prevent incidents from occurring by ensuring that networks, systems, and applications are sufficiently secure.

Denial of Service (DoS) Incidents

- Configure firewall rule sets to prevent reflector attacks. In a reflector attack, a host sends many requests with a spoofed source address to a service (user datagram protocol, UDP) located on an intermediate host.
- Configure border routers to prevent amplifier attacks. In an amplifier attack, a host sends many requests with a spoofed source address to a service (UDP and Internet control message protocol, ICMP) located on a whole network of intermediate hosts.
- Determine how the organization's Internet service providers (ISPs) and second-tier providers can assist in handling network-based denial of service (DoS) attacks.
- Configure security software to detect DoS attacks.
- Configure the network perimeter to deny all incoming and outgoing traffic that is not expressly permitted.

Malicious Code Incidents

- Make users aware of malicious code issues.
- Read anti-virus vendor bulletins.
- Deploy host-based IDSs, including file integrity checkers, to critical hosts.
- Use anti-virus software, and keep it updated with the latest virus signatures.
- Configure software to block suspicious files.
- Limit the use of nonessential programs with file transfer capabilities (e.g., peer-to-peer file- and music-sharing programs, instant messaging software, and Internet relay chat (IRC) clients and servers. These programs are frequently used to spread malicious code among users).
- Educate users on the safe handling of e-mail attachments (e.g., look for suspicious attachments or attachments from unknown sources such as .bat, .com, .exe, .pif, .vbs).
- Eliminate open Windows shares.
- Use Web browser security to limit mobile code (e.g., unsigned Active X).
- Configure e-mail clients to act more securely.

Unauthorized Access Incidents

- Configure intrusion detection software to alert on attempts to gain unauthorized access.
- Configure all hosts to use centralized logging.
- Establish procedures for having all users change their passwords.
- Configure the network perimeter to deny all incoming traffic that is not expressly permitted.
- Secure all remote access methods, including modems and virtual private networks (VPNs).
- Put all publicly accessible services on secured demilitarized (DMZ) network segments.
- Disable all unneeded services on hosts and separate critical services.
- Use host-based firewall software to limit individual hosts' exposure to attacks.
- Create and implement a password policy.

Inappropriate Usage Incidents

- Discus the handling of inappropriate usage incidents with the organization's human resources and legal departments.
- Discuss liability issues with the organization's legal department.
- Configure network-based intrusion detection software to detect certain types of inappropriate usage (e.g., use of unauthorized services, outbound reconnaissance activity and attacks, and improper e-mail relay usage for sending spam).
- Log basic information on user activities (e.g., file transfer protocol (FTP) commands, Web requests, and e-mail headers), which may be valuable for investigative and evidentiary purposes.
- Configure all e-mail servers so they cannot be used for unauthorized mail relaying. Mail relaying is commonly used to send spam.
- Implement spam-filtering software on all e-mail servers.
- Implement uniform resource locator (URL) filtering software.

Multiple Component Incidents

- Use centralized software for logging and event correlation. Incident handlers can identify an incident as having multiple components more quickly when all precursors and indications are accessible from a single point of view.

(ii) Phase 2. Detection and Analysis. Below is a summary of controls required to handle computer security incidents in the detection and analysis phase:

- Identify precursors and indications through alerts generated by several types of computer security software.
- Establish mechanisms for outside parties to report incidents.
- Require a baseline level of logging and auditing on all systems, and a higher baseline level on all critical systems.
- Profile networks and systems.
- Understand the normal behaviors of network, systems, and applications through log entries and security alerts.

- Use centralized logging and create a log retention policy.
- To determine if an incident has occurred, perform event correlation on data logged by multiple sources. Centralized logging makes event correlation easier and faster.
- Keep all hosts clocks synchronized to facilitate event correlation. Clock discrepancies may also cause issues from an evidentiary standpoint.
- Maintain and use a knowledge base holding commonly used port numbers and links to virus information, data on precursors, and the indications of previous incidents.
- Use Internet search engines for research.
- Run packet sniffers to collect additional data.
- Consider filtering the data.
- Consider experience as being irreplaceable.
- Create a diagnosis matrix for less experienced staff. A diagnosis matrix that lists incident categories and the symptoms associated with each category can provide guidance as to what type of incident is occurring and how the incident can be validated.
- Seek assistance from others.
- Start recording all information with time stamps as soon as the team suspects that an incident has occurred.
- Safeguard incident data, both physically and logically.
- Prioritize incidents by business impact, based on the criticality of the affected resources and the technical impact of the incident.
- Include provisions regarding incident reporting in the organization's incident response policy. This includes which incidents must be reported, when they must be reported, and to whom.

(iii) Phase 3. Containment, Eradication, and Recovery. The following controls are necessary when handling computer security incidents in the containment, eradication, and recovery phase:

General

- Establish strategies and procedures for containing incidents.
- Follow established procedures for evidence gathering and handling.
- Capture volatile data from systems as evidence. This effort includes lists of network connections, processes, log-in sessions, open files, network interface configurations, and the contents of memory.
- Obtain system snapshots through full forensic disk images, not file system backups. Disk images should be made to sanitized write-protectable or write-once media. This process is superior to a file systems backup from an investigatory and evidentiary standpoint. Imaging is also valuable in that it is much safer to analyze an image than it is to perform analysis on the original system because the analysis may inadvertently alter the original.

Denial of Service (DoS) Incidents

- Create a containment strategy that includes several solutions in sequence.

Malicious Code Incidents

- Contain malicious code incidents as quickly as possible.
- Identify and isolate other infected hosts.
- Send unknown malicious code to anti-virus vendors.
- Configure e-mail servers and clients to block e-mails.
- Block particular hosts.
- Shut down e-mail servers.
- Isolate networks from the Internet.

Unauthorized Access Incidents

- Provide change management information to the incident response team.
- Select containment strategies that balance between mitigating risks and maintaining services. Possibilities include isolating the affected system, disabling the affected services (e.g., FTP), eliminating the attacker's route into the environment, disabling user accounts that may have been used in the attack, and enhancing physical security measures such as locking the server room.
- Restore or reinstall systems that appear to have suffered a root compromise. The effects of root compromises are often difficult to identify completely. The system should be restored from a known good backup, or the operating system and applications should be reinstalled from scratch. The system should then be secured properly so the incident cannot recur.

Multiple Component Incidents

- Contain the initial incident and then search for signs of other incident components.

(iv) Phase 4. Postincident Activity. The following controls are necessary when handling computer security incidents in the postincident activity phase:

General

- Hold lessons-learned meetings after major incidents.

Multiple component incidents

- Separately prioritize the handling of each incident component. Resources are probably too limited to handle all incident components simultaneously. Components should be prioritized based on response guidelines for each component and how current each component is.

11.13 INTERCONNECTING SYSTEMS

(a) OVERVIEW. A system interconnection is defined as the direct connection of two or more information systems for sharing data and other information resources. Organizations choose to interconnect their information systems for a variety of reasons based on their organizational needs. For example, they may interconnect information systems to exchange data, collaborate on joint projects, or securely store data and backup files.[15]

EXHIBIT 11.3 INFORMATION SYSTEM INTERCONNECTION

An interconnection is a direct connection between one organization's system with another system of the same or different organization through a mechanism by which they are joined (the "pipe" through which data is made available, exchanged, or passed one way only). The "pipe" may be a dedicated line that is owned by one of the organizations or is leased from a third party (e.g., Integrated Services Digital Network [ISDN], T1 or T3 line). Alternately, the systems may be connected over a public network (e.g., the Internet) using a virtual private network (VPN). Exhibit 11.3 depicts the concept of information system interconnection.

The following are examples of interconnections:

- System A is connected to System B over a subscriber line leased by System A or System B.
- System A is segmented such that System A1 is integrated with System A but is under different management control.
- System B provides data transport services between System A and System C. Here, System B is engaged in two interconnections with Systems A and C.

Levels of system interconnection may vary. For example, some organizations may choose to establish a limited interconnection, whereby users are restricted to a single application or file location with rules governing access. Other organizations may establish a broader interconnection, enabling users to access multiple applications or databases. Still other organizations may establish an interconnection that permits full transparency and access across their respective enterprises.

Interconnecting information systems can expose the participating organizations to risk. If the interconnection is not properly designed, security failures could compromise the connected systems and their data. Similarly, if one of the connected systems is compromised, the interconnection could be used as a conduit to compromise the other system and its data.

(b) MANAGING SYSTEM INTERCONNECTIONS. All federal agencies must explicitly address the subject of interconnecting information systems by establishing formal agreements that specify the technical and security requirements of the interconnection, define the responsibilities of the participating organizations, and specify the rules governing these interconnections.

When organizations are properly managing interconnected systems, the added benefits include greater efficiency, centralized access to data, and greater functionality. The security controls of each of the interconnected systems should be evaluated and meet each system's requirements for implementing security-controls that are appropriate for the particular interconnection.

Information System Connections and Agreements

The organization authorizes all connections from the information system to other information systems outside of the accreditation boundary, and it regularly monitors/controls the system interconnections. Appropriate organizational officials approve information-system interconnection agreements.

It is critical that both organizations maintain clear lines of communication to:

- Ensure that the interconnection is properly maintained and that security controls remain effective.
- Facilitate effective change management activities by making it easy for both sides to notify each other about planned system changes that could affect the interconnection.
- Enable prompt notification by both sides of security incidents and system disruptions.
- Facilitate a coordinated response.

Identifying and implementing security controls is vital in protecting the confidentiality, integrity, and availability of the connected systems and the data that is transferred between the systems. If security controls are not in place, or if they are configured improperly, the process of establishing the interconnection could expose the information systems to unauthorized access. The security controls should be appropriately selected in consideration of the systems that will be connected and the environment in which the interconnection will operate.

One or both organizations should review the security controls for the interconnection, at least annually and whenever a significant change occurs to either system or the operational environment. This review is intended to ensure that all controls are operating properly and still providing the requisite degree of system and data security.

(c) INTERCONNECTION LIFE CYCLE MANAGEMENT. A four-phase "life cycle management" approach to interconnecting information systems that emphasizes proper attention to information security includes the following:

Phase 1: Planning the Interconnection
Phase 2: Establishing the Interconnection
Phase 3: Maintaining the Interconnection
Phase 4: Disconnecting the Interconnection

(i) Phase 1: Planning the Interconnection. The process of connecting two or more information systems begins with a planning phase, where the participating organizations perform preliminary activities and examine all relevant technical, security, and administrative issues. The planning phase ensures that the interconnection will operate as efficiently and securely as possible. Six steps are recommended for planning a system interconnection.

(A) Step 1: Establish a Joint Planning Team

The organizations should consider establishing a joint planning team composed of appropriate management and technical staff that includes program managers, system security officers, system administrators, network administrators, and system architects. The

typical joint planning team is responsible for coordinating all aspects of the planning process and ensuring that the process has both clear direction and sufficient resources. It also must have the commitment and support of the system and data owners, and of other senior managers.

(B) Step 2: Define the Business Case

Both organizations should work together to define the purpose of the interconnection, determine how it will support their mission requirements, and identify potential costs and risks. Defining the business case will establish the basis of the interconnection and facilitate the planning process. Factors that should be considered are estimated costs (e.g., staffing, equipment, facilities), expected benefits (e.g., improved efficiency), and potential risks (e.g., technical, legal, and financial).

(C) Step 3: Perform Certification and Accreditation

Establishing an interconnection may represent a significant change to the connected systems. Before proceeding further, each organization should consider recertification and reaccreditation of its respective system(s) to verify that security protections remain acceptable. A full security certification and accreditation might not be necessary, however, if the system continues to operate within an acceptable level of risk; in that case, an abbreviated certification and accreditation would suffice.

(D) Step 4: Determine Interconnection Requirements

The joint planning team should identify and examine all relevant technical, security, and administrative requirements surrounding the proposed interconnection.

(E) Step 5: Document the Interconnection Agreement

The interconnection security agreement (ISA) is a security document that specifies the technical and security requirements for establishing, operating, and maintaining the interconnection. It also supports the memorandum of understanding/memorandum of agreement (MOU/MOA) between the organizations. Specifically, the ISA documents the requirements for connecting the information systems, describes the security controls that will be used to protect the systems and data, contains a topological drawing of the interconnection, and provides a signature line.

The joint planning team should document an agreement governing the interconnection and the terms under which the organizations will abide. The agreement should be based on the team's review of all relevant technical, security, and administrative requirements identified and examined in Step 4.

The MOU/MOA documents the terms and conditions for sharing data and information resources. It defines the purpose of the interconnection, identifies relevant authorities, specifies the responsibilities of each organization, defines the apportionment of costs, and identifies the timeline for terminating or reauthorizing the interconnection. In order to operate as an instrument that can be enforced by any agency that is a party to the interconnection, the MOU/MOA must be signed by an organization official, typically the authorizing official (AO). Lastly, because the ISA and the MOU/MOA may contain sensitive information, the original document and any copies should be protected appropriately against unauthorized disclosure or modification, damage, or destruction.

(F) Step 6: Approve or Reject System Interconnection

The joint planning team should submit the ISA and the MOU/MOA to the AO of each organization, requesting approval for the interconnection. Upon receipt, the AOs should review the ISA, the MOU/MOA, and any other relevant documentation or activities. Organizations may combine ISAs and MOU/MOAs to simplify their management processes and reduce paperwork if these two documents fall within the purview of the same AO. When combining ISAs and MOU/MOAs, organizations must ensure that the contents and the intent of these two documents remain unaltered.

Based on this review, the AOs should decide on one of the following:

- Approve the interconnection.
- Grant interim approval.
- Reject the interconnection.

(ii) Phase 2: Establishing the Interconnection. After the system interconnection is planned and approved, it can be implemented. The recommended steps for establishing the system interconnection are described below.

(A) Step 1: Develop an Implementation Plan

To ensure that the information systems are connected properly and securely, the joint planning team should develop a system interconnection implementation plan. At a minimum, the implementation plan should:

- Describe the information systems that will be connected.
- Identify the sensitivity or classification level of data that will be made available, exchanged, or passed one way across the interconnection.
- Identify personnel who will establish and maintain the interconnection, and specify their responsibilities.
- Identify implementation tasks and procedures.
- Identify and describe security controls that will be used to protect the confidentiality, integrity, and availability of the connected systems and data.
- Provide test procedures and measurement criteria to ensure that the interconnection operates properly and securely.
- Specify training requirements for users, including a training schedule.
- Cite or include all relevant documentation, such as system security plans, design specifications, and standard operating procedures (SOPs).

(B) Step 2: Execute the Implementation Plan

After the implementation plan is developed, it should be reviewed and approved by senior members of the planning team and then executed. A list of recommended tasks for establishing an interconnection includes:

- Implement or configure security controls.
- Install or configure hardware and software.
- Integrate applications.
- Conduct operational and security assessments.
- Conduct security training and awareness.

- Update system security plans.
- Perform recertification and reaccreditation.

Procedures associated with each task should be described in the implementation plan.

(C) Step 3: Activate the Interconnection

Both parties should activate the interconnection following the implementation plan execution. To make sure the system is operating properly and securely, each organization should closely and frequently examine the system's audit logs and the types of assistance requested by the system's users during this time, Lastly, the appropriate organization should promptly document and address any security weaknesses or problems.

(iii) Phase 3: Maintaining the Interconnection. After the interconnection is established, the participating organizations must actively maintain it to ensure it operates properly and securely. The following activities are recommended for maintaining the interconnection:

- Maintain the equipment.
- Manage user profiles.
- Conduct security reviews.
- Analyze audit logs.
- Report and respond to security incidents.
- Coordinate contingency planning activities.
- Perform change management.
- Maintain system security plans.

(iv) Phase 4: Disconnecting the Interconnection. Phase-out may be planned or it may be in response to an emergency. Organizations may wish to restore some of the disconnections but not others.

(A) Terminating Interconnection

An organization might have a variety of reasons to terminate an interconnection—for instance, changed business needs, cost considerations, or changes in system configuration. The decision to terminate the interconnection should be made by the system owner with the advice of appropriate management and technical staff. Before terminating the interconnection, the initiating party should provide written notice to the receiving party. In turn, the receiving party should acknowledge receipt of the notification. The notification should describe the reason(s) for the disconnection, provide the proposed timeline for the disconnection, and identify technical and management staff that will conduct the disconnection.

The schedule for terminating the interconnection should permit a reasonable time period for internal business planning so both sides can make appropriate arrangements. In addition, staff from both organizations should coordinate to determine the logistics of the disconnection and the disposition of shared data, including purging and overwriting sensitive data. The disconnection should be conducted when the impact on users is minimal. Following the disconnection, each organization should update its system security plan and related documents.

(B) Emergency Disconnection

If one or both organizations detect an attack, intrusion attempt, or other contingency that exploits or jeopardizes the connected systems or their data, it might be necessary to abruptly terminate the interconnection without providing written notice to the other party. This extraordinary measure should be taken only in extreme circumstances and only after consultation with appropriate technical staff and senior management.

The decision to make the emergency disconnection should be made by the system owner (or a designated staff member) and implemented by technical staff. The system owner or designee should immediately notify the other party verbally and receive confirmation of the notification. Both parties should work together to isolate and investigate the incident, in accordance with incident response procedures. If necessary, law enforcement authorities should be notified and evidence should be preserved.

The initiating party should provide a written notification to the other party in a timely manner (e.g., within five days). The notification should describe the nature of the incident, explain why and how the interconnection was terminated, and identify actions taken to isolate and investigate the incident. The notification should also specify when and under what conditions the interconnection might be restored, if appropriate.

(C) Restoration of Interconnection

Both organizations may choose to restore the system interconnection after it has been terminated. The decision to restore the interconnection should be based on the cause and duration of the disconnection. For example, if the interconnection was terminated because of an attack, intrusion, or other contingency, both parties should implement appropriate countermeasures to prevent a recurrence of the problem. If necessary, they also should modify the ISA and MOU/MOA to address issues requiring attention. Alternatively, if the interconnection has been terminated for more than 90 days, each party should perform a risk assessment on its respective system and reexamine all relevant planning and implementation requirements, including developing a new ISA and MOU/MOA.

(d) ELECTRONIC-MAIL BEST PRACTICES. Electronic mail (e-mail), a very popular Internet application, is used on a regular basis by individuals, government, and business organizations throughout the world to exchange personal and business information.[16]

The popularity and widespread use of e-mail systems make them tempting targets for malicious attacks, and all users and organizations should be concerned about protecting the security of their systems and their e-mail communications. Attacks on e-mail systems have taken different approaches. Some attackers with extensive knowledge of the workings of these systems have been able to exploit their weaknesses and use the system to distribute viruses and other malware throughout an organization. Some sophisticated attacks have used e-mail to compromise user workstations within an organization's internal network, and to influence users to provide information to the attackers or unknowingly extend the attacks to other systems. Flaws in systems have enabled unauthorized users to gain access to and to change information not meant to be publicly accessible, and to execute commands and install software on the organization's mail server. Denial of service (DoS) attacks can harm an organization by preventing legitimate users from accessing systems. Attackers have also penetrated e-mail systems to disable other organizational systems and to send false messages to others from the organization.

Organizations should do the following:

1. Plan for Secure Electronic Mail Systems.

Carefully plan and address the security aspects of the deployment of a mail server. Careful planning is critical to the efficient implementation of a secure mail sever. It is more difficult and costly to address security issues once the mail server is deployed. With careful planning, organizations can make sure that their mail servers meet their security requirements and are in compliance with all relevant organizational policies prior to installation, configuration, and deployment. Management controls are especially important in organizations where the IT support structure is highly fragmented. This fragmentation can lead to inconsistencies in managing systems, and these inconsistencies often result in security vulnerabilities.

Organizations are more likely to make decisions about configuring computers appropriately and consistently when they develop and use a detailed, well-designed deployment plan. The development of such a plan will support mail server administrators in making the inevitable tradeoff decisions between usability, performance, and risk.

Some of the issues that should be addressed in the organization's deployment plan include the following:

- Purpose of the mail server and the services to be provided
- Software to be installed
- Users and their privileges
- Security and privacy issues
- Management practices and procedures to assure secure systems
- Types of personnel required for deployment and operational phases of the mail server and the supporting infrastructure. Personnel types that should be considered include system and mail server administrators, network administrators, and information systems security officers.
- Skills and training required by assigned personnel and availability of personnel

2. Implement Secure Electronic Mail Systems.

Implement appropriate security management practices and controls when maintaining and operating a secure mail server. Appropriate management practices are essential to operating and maintaining a secure mail server. As part of their comprehensive planning and management practices, organizations should identify their systems and information to be protected, and then develop, document, and implement the policies, standards, procedures, and guidelines that will help to ensure the confidentiality, integrity, and availability of information system resources.

To ensure the security of a mail server and the supporting network infrastructure, the following best practices should be implemented:

- Organization-wide information-system security policy
- Configuration/change control and management
- Risk assessment and management
- Standardized software configurations that satisfy the information system security policy
- Security awareness and training

- Contingency, continuity of operations, and disaster recovery planning
- System certification and accreditation

Ensure that the mail server operating system is deployed, configured, and managed to meet the security requirements of the organization. The first step in securing a mail server is to secure the underlying operating system. Most commonly available mail servers operate on a general-purpose operating system. Many security issues can be avoided if the operating system's underlying mail servers are configured appropriately. Default hardware and software configurations are typically set by manufacturers to emphasize features, functions, and ease of use (convenience) at the expense of security. Because manufacturers are not aware of each organization's security needs, each mail server administrator must configure new servers to reflect their organization's security requirements and reconfigure them as those requirements change. Using security configuration guides or checklists can assist administrators to secure systems consistently and efficiently.

To secure the operating system, organizations should carry out the following action steps:

- Patch and update the operating system.
- Remove or disable unnecessary services and applications.
- Configure operating-system user authentication.
- Configure resource controls.
- Install and configure additional security controls if needed.
- Perform security tests and audits on the operating system.

Ensure that the mail server application is deployed, configured, and managed to meet the security requirements of the organization. Many of the steps outlined for the security of the operating system apply also to the secure installation and configuration of the mail server application. The basic recommendation is that organizations should install the minimal mail server services required and eliminate any known vulnerabilities through patches or updates. If an installation program installs unnecessary applications, services, or scripts, they should be removed immediately after the installation process has been completed.

The following action steps should be performed in securing the mail server application:

- Patch and upgrade the mail server application.
- Remove or disable unnecessary services, applications, and sample content.
- Configure mail-server user authentication and access controls.
- Configure mail-server resource controls.
- Test the security of the mail server application.

Consider the implementation of cryptographic technologies to protect user authentication and mail data. Most standard mail protocols default to unencrypted user authentication and send e-mail data unencrypted through the network. When unprotected data is sent, an attacker may be able to easily compromise a user account and to intercept or alter unencrypted e-mail messages. Most organizations should consider

encrypting the user authentication session even if they do not encrypt the e-mail data itself. Encrypted user authentication is now supported by most standard and proprietary mailbox protocols.

Organizations should examine closely the decision about whether to encrypt and sign e-mail data. Encrypting and signing e-mail places a greater load on the user's computer and the organization's network infrastructure, and this practice may complicate malware scanning and e-mail content filtering. Encrypting and signing messages may also result in significant administrative overhead and may increase the costs of managing e-mail systems. However, for many organizations, the benefits of e-mail encryption and signatures will outweigh the costs.

Employ the network infrastructure to protect mail servers. The network infrastructure includes the firewalls, routers, and the intrusion-detection and -prevention systems that support the mail server. These systems play a critical role in the security of the mail server. In most configurations, the network infrastructure will be the first line of defense beaten the Internet and a mail server. Network design alone, however, cannot protect a mail server. Because of the frequency, sophistication, and variety of mail server attacks that occur today, organizations should consider protecting their mail servers through layered and diverse protection mechanisms.

Ensure that the mail clients are deployed, configured, and used properly to meet the security requirements of the organization. The client side of the e-mail process may represent a greater risk to the security of the mail system than the mail server functions. Organizations must address numerous issues in order to provide an appropriate level of security for e-mail clients.

The following action steps will help organizations with the secure installation, configuration, and implementation of mail client applications:

- Patch and upgrade the mail client applications.
- Configure mail-client security features, such as disabling automatic opening of messages and enabling anti-spam and anti-phishing features.
- Configure mailbox authentication and access.
- Secure the client host's operating system.

3. Maintain Secure Electronic Mail Systems.

Maintain the security of a mail server as an ongoing process. Organizations should devote constant effort, resources, and vigilance to maintain a secure mail server. The mail server should be monitored and maintained on a daily basis to assure mail security.

To maintain the security of a mail server, organizations should take the following action steps:

- Configure, protect, and analyze mail log files.
- Back up data frequently.
- Protect against malware (e.g., viruses, worms, and Trojan horses).
- Establish and implement procedures for recovering from compromise.
- Test and apply patches in a timely manner.
- Test the security of the system periodically.

(e) ELECTRONIC-COMMERCE BEST PRACTICES

(i) Overview. "Electronic commerce" (e-commerce) is defined as a place where buyers and sellers are connected using computers and networks (the Internet) to buy and sell goods and services. The term "electronic business" (e-business) is much broader than e-commerce because the former includes distribution of information and customer support, which is lacking in the latter. In other words, e-commerce is a subset of e-business.

WHAT IS E-COMMERCE?

E-commerce is a Web-enabled value chain because the Internet is the enabling technology. Business applications are located on the Web servers to provide wide access for employees and selective access for customers and suppliers.

E-commerce can be grouped into four models: business to consumer (B2C), business to business (B2B), consumer to consumer (C2C), and government to citizen (G2C). On-line stores selling goods directly to consumers are an example of the B2C model. Electronic data interchange (EDI) is a critical component of the sales process for many on-line retailers. B2B e-commerce involves the "Internet-enabling" of the exchange of goods and services between two companies with an existing relationship. EDI is the underlying technology enabling on-line catalogs and continuous stock-replenishment programs. Under the C2C model, consumers buy and sell goods with other consumers, such as auction sites (e.g., e-Bay). Under the G2C model, the federal government is using the Internet to reach its citizens for a variety of information-dissemination purposes and transactions (e.g., the Internal Revenue Service, U.S. Postal Service, and Social Security Administration).

For the purposes of exploring the relevant security issues, one can divide e-commerce into four basic classes: electronic mail (e-mail), electronic data interchange (EDI), information transactions, and financial transactions.

$$\begin{aligned}\text{E-commerce security issues} = {} & \text{e-mail security issues} + \text{EDI security issues} \\ & + \text{information-transaction security issues} \\ & + \text{financial-transaction security issues}\end{aligned}$$

(A) E-MAIL SECURITY ISSUES

The use of Internet e-mail to carry business-critical communications is growing exponentially. While e-mail provides a low-cost means of communication with customers, suppliers, and partners, a number of security issues are related to the use of e-mail. Among the security issues: (1) Internet e-mail addresses are easily spoofed. It is nearly impossible to be certain who created and sent an e-mail message based on the address alone. (2) Internet e-mail messages can be easily modified. Standard SMTP (simple mail transfer protocol) mail provides no integrity checking. (3) There are a number of points where the contents of an e-mail message can be read by unintended recipients. (4) There is usually no guarantee of delivery with Internet e-mail. (While some mail systems support return receipts, when such receipts work at all they often only signify that the user's server, not necessarily the user, has received the message.) These weaknesses

make it important for organizations to issue policies defining acceptable use of e-mail for business purposes.

(B) Electronic Data Interchange (EDI) Security Issues

Traditional EDI systems allow preestablished trading partners to electronically exchange business data through value-added networks (VANs). The Internet can provide the connectivity needed to support EDI at substantial cost savings over a VAN. However, the Internet does not provide the security services (e.g., integrity, confidentiality, and nonrepudiation) required for business EDI. Similar to e-mail over the Internet, EDI transactions are vulnerable to modification, disclosure, or interruption when sent over the Internet. The use of cryptography to provide the required security services has changed this; consequently many companies and government agencies are moving to Internet-based EDI.

Scope of E-Commerce

E-commerce encompasses a broader commerce environment than EDI. Because of this, EDI is a subset of e-commerce. Similarly, e-commerce is a subset of e-business.

(C) Information-Transactions Security Issues

Providing information (e.g., stock quotes and news) is a major and costly element of commerce. Using the Internet to provide these services is substantially less expensive than fax, telephone, or postal mail services. Integrity and availability of the information provided are key security concerns that require security controls and policy.

(D) Financial-Transactions Security Issues

Computer networks have been used to process financial transactions such as checks, debit cards, credit cards, and electronic funds transfer (EFT). Similar to EDI over VANs, the connectivity options have been limited, and the leased lines are expensive. The Internet provides an opportunity for cost savings in electronic financial transactions. The use of the Internet to carry these types of transactions replaces the physical presentation or exchange of cash, checks, or debit/credit cards with the electronic equivalent. Each of these forms of transactions involves the use of cryptography to provide for integrity, confidentiality, authentication, and nonrepudiation. For example, a standard known as secure electronic transactions (SET) is used for processing credit card transactions over public networks. Use of SET involves three-way transactions between the buyer, the seller, and a financial institution (a bank).

(ii) E-Commerce Software. E-commerce software should support the following tasks:

- **Catalog Management.** Catalog management software combines different product data formats into a standard format for uniform viewing, aggregating, and integrating catalog data into a central repository for easy access, retrieval, and updating of pricing and availability changes.
- **Product Configuration.** Customers need help when an item they are purchasing has many components and options. Buyers use the new Web-based product configuration software to build the product they need online with little or no help from salespeople.

- **Shopping Cart Facilities.** Today many e-commerce sites use an electronic shopping cart to track the items selected for purchase, allowing shoppers to view what is in their cart, add new items to it, or remove items from it.
- **E-Commerce Transaction Processing.** E-commerce transaction-processing software takes data from the shopping cart and calculates volume discounts, sales tax, and shipping costs to arrive at the total cost.
- **Web Site–Traffic Data Analysis.** Web site–traffic data analysis software captures visitor information, including who is visiting the Web site, what search engine and key words they used to find the site, how long their Web browser viewed the site, the date and time of each visit, and which pages were displayed. These data are placed into a Web log file for future analysis to improve the Web site's performance.

(iii) Sample Best Practices in Electronic Commerce. The following are best practices according to the Information Systems Audit and Control Foundation (ISACF) research publication entitled *E-Commerce Security: Enterprise Best Practices*:[17]

- Have a set of security mechanisms and procedures that, taken together, constitute a security architecture for e-commerce (deals with architecture).
- Have measures in place to ensure the choice of the correct protocols for the application and the environment, as well as the proper use and exploitation of the protocols' features and compensation for their limitations (deals with infrastructure/protocol).
- Have a mechanism in place to mediate between the public networks (the Internet) and the organization's private network (deals with infrastructure/firewall).
- Have a means to communicate across the Internet in a secure manner (deals with infrastructure/virtual private network).
- Have a process whereby participants in an e-commerce transaction can be uniquely and positively identified (deals with authentication/digital certificates).
- Have a mechanism by which the initiator of an e-commerce transaction can be uniquely associated with it (deals with authentication/digital signatures).
- Have an infrastructure to manage and control public key pairs and their corresponding certificates (deals with authentication/public key infrastructure [PKI]).
- Have procedures in place to control changes to an e-commerce presence (deals with applications/change control).
- Make sure e-commerce applications maintain logs of their use, which should be monitored by responsible personnel (deals with applications/logs and monitoring).
- Have methods and procedures to recognize security breaches when they occur (deals with applications/intrusion detection).
- Use e-commerce applications that allows reconstruction of the activity performed by the applications (deals with applications/auditability).
- Use processes that allow a provable association between an e-commerce transaction and the person who entered it (deals with applications/non-repudiation).
- Have protections in place to ensure that data collected about individuals are not disclosed without their consent nor used for purposes other than that for which they were collected (deals with applications/privacy).

- Have a means of ensuring the confidentiality of data communicated between customers and vendors (deals with data protection/encryption).
- Have mechanisms that protect the e-commerce presence and its supporting private networks from computer viruses, and that prevent the presence and its networks from spreading viruses to customers and vendors (deals with data protection/virus scanning).
- Maintain protection for the devices used to access the Internet (deals with availability/protecting the user environment).
- Use e-commerce architecture designed to keep all components from failing simultaneously, and to allow components to repair themselves if they should fail (deals with availability/fault tolerance).
- Have a plan and procedures for continuing e-commerce activities in the event of an extended outage of required resources for normal processing (deals with availability/business continuity planning).
- Have a commonly understood set of practices and procedures to define management's intentions for the security of e-commerce (deals with policy and governance/policy).
- Have measures in place to prevent information about customers from being disclosed. Unless the customer has given permission otherwise, the measures should also make sure the information is not used for purposes other than those for which it was obtained (deals with policy and governance/privacy).
- Share responsibility within an organization for e-commerce security (deals with policy and governance/oversight).
- Ensure there is communication from vendors to customers about the level of security in an e-commerce presence (deals with policy and governance/notification).
- Maintain a regular program of audit and assessment of the security of e-commerce environments and applications in order to provide assurance that controls are present and effective (deals with policy and governance/auditing and assurance).

(f) COMPUTER-SOFTWARE PIRACY BEST PRACTICES

(i) Computer-Software Piracy Policies. Software piracy conveys that the creative and intellectual work of the author has been used or duplicated without permission, compensation, or payment of royalty to the author. Software piracy is an act of infringement on ownership rights, and the person who commits this act could be sued civilly for damages, criminally prosecuted, or both. Software piracy is the most difficult act to control and enforce against. Self-monitoring and honesty are the best controls.

The vast majority of the software involved in software-piracy legal cases is off-the-shelf, PC software for purposes such as word processing, spreadsheets, graphics, and databases. The issue is illegal use, copy, and distribution of software both inside and outside an organization. Here, "illegal" means a user has not paid for the software.

Software piracy policies are needed to protect an organization from legal suits by owners. Such a policy should include:

- Prohibiting illegal copy and use of software
- Developing a software-inventory management system that includes a list of popular application programs. This list can be compared to the organization's purchase orders, original software diskettes, or original documentation manual.

- Checking the hard disks for illegally copied software periodically
- Making illegal copying of software grounds for employee dismissal
- Requiring all employees to sign a statement of not using illegal software at their work and not using the illegal software taken from work to home
- Prohibiting copying of internally developed software
- Prohibiting pirated externally developed software from being brought into an organization
- Monitoring all sensitive programs to protect them from illegal copying

(ii) Sample Software Acquisition Policy

(A) Purpose

This policy is applicable to organizations acquiring computer software in compliance with applicable laws and licensing restrictions. This policy identifies categories of software that violate such laws or licensing restrictions, and it sets forth steps that organizations should take to avoid acquisition of illegal software. In addition, the policy indicates remedial actions that should be taken in the event a software reseller supplies computer software that violates applicable laws or licensing regulations.[18]

(B) Types of Pirated Software

All employees should be cognizant of the different types of pirated software when evaluating bids or engaging in negotiations to acquire computer software. Pirated software includes both illegally copied software and software that violates licensing restrictions.

Illegally Copied Software. Illegally copied software includes counterfeit software, compilation CDs, hard-disk loaded software, online pirated software, and other illegally copied software. Each type is described next.

Counterfeit software: unauthorized copies of software that are duplicated with the intent of directly imitating the copyrighted product. Counterfeit software is typically reproduced and distributed in a form designed to make the product appear legitimate, complete with sophisticated attempts at replicating packaging, documentation, registration, logos, and security features.

Compilation CDs: unauthorized copies of multiple software programs that are compiled onto a single CD. Compilation CDs typically include software programs published by a variety of software publishers.

Hard-disk loaded software: unauthorized copies of software loaded by the hardware dealer onto the hard disk of the computer and then offered to the customer as a free or heavily discounted incentive to purchase the computer.

Online pirated software: unauthorized copies of software that are distributed and downloaded via the Internet.

Other illegally copied software: software that is copied from disks, CDs, or other machines without the authorization of the copyright owner.

License Misuse. Software copies are licensed, and not sold, to the end user. The software publisher's license agreement typically restricts how, and to whom, software copies may be distributed. When acquiring software copies, an organization should review the applicable license and ensure that its use of the software will not violate any restrictions imposed by the software publisher.

License misuse occurs when legitimate copies of software are distributed and used in violation of the applicable license agreement. Examples of license misuse include the following:

- **Original Equipment Manufacturer (OEM) Software:** OEM software is licensed and specifically marked for distribution with new computer hardware. License misuse occurs when OEM software is "unbundled" from the computer and distributed to, and used by, the end user as a stand-alone product, often at a heavily discounted price.
- **Academic Versions:** Academic software is manufactured, licensed, and specifically marked for distribution to educational institutions and students at reduced prices. License misuse occurs when academic software is distributed to, and used by, a nonacademic end user.
- **"Not for Resale" (NFR) Software:** NFR software is marked "not for resale" and typically is distributed as promotional or sample product and not licensed for commercial distribution and use. License misuse occurs when NFR software is distributed in violation of its resale restrictions.
- **Fulfillment Software:** Fulfillment software is licensed solely for distribution to mid- or large-sized end users that currently possess a volume license agreement or valid site license. Fulfillment software is typically distributed in a CD jewel case without the packaging or materials that accompany retail product. License misuse occurs when fulfillment software is distributed to, and used by, end users that lack the necessary licenses for use of the underlying product.
- **Software Upgrades:** Upgrade versions of software programs are licensed and specifically marked for distribution to end users that currently possess a valid license or the original product. License misuse occurs when upgrades are distributed to, and used by, end users that lack a license for the original product. Typically, OEM, fulfillment and other nonretail products are distributed without the colorful packaging and materials that accompany full retail products. Accordingly, these nonretail products are easier to counterfeit. Thus, employees should be aware that deeply discounted nonretail software might in fact be counterfeit.

Operational Defects of Pirated Software. Employees should be cognizant of the risks that accompany the acquisition and use of software in violation of applicable copyrights or licensing restrictions. Beyond the legal risks that accompany copyright and licensing violations, the use of pirated software can jeopardize the effectiveness and integrity of the organization's computer systems. This is because pirated software typically lacks the full package or benefits that accompany legitimate product, including: (i) warranty protection, (ii) notice of, and ability to obtain, upgrades to the software, (iii)) technical support for the software, (iv) assurance that the software is free of computer viruses, and (v) confidence that the most recent version of the software, free from defects, is being obtained.

(C) Steps to Avoid Acquisition of Pirated Computer Software

The organization and any employees authorized to acquire software should take all necessary steps to minimize risk of acquiring pirated software, including the following:

- **Educate employees.** Employees authorized to acquire software should be educated on the requirements of the organization's software acquisition policy.
- **Standardize software acquisition procedures and centralize purchases.** The organization should, to the extent possible, (1) implement standardized software acquisition procedures throughout the organization, and (2) centralize software purchase within a designated department. By implementing standardized acquisition procedures and centralizing software purchases, the organization will be better able to prevent acquisition of pirated software. Moreover, a centralized acquisition program can result in volume purchases, which are often accompanied by discounts.
- **Demand proper licenses and accompanying materials.** Before purchasing software, the employee should research the license and materials that accompany the legitimate product (e.g., an original license agreement, registration card, manual, security features, and diskettes or CD-ROM). Employees should demand and obtain each of these materials and avoid software resellers that refuse to comply.
- **Verify appropriate license.** Before purchasing software, verify that the license authorizes distribution to, and use by, an organization.
- **Purchase software from reputable resellers.** Employees should seek out software resellers with reputations for honesty and customer service within the community.
- **Contact the software publisher.** Particularly for large purchases of software, employees should contact the software publisher or its authorized distributor for information on the product and on authorized resellers within the community. Moreover, the software publisher or authorized distributor should be contacted whenever an employee suspects that software acquired by, or offered to, an organization may be pirated.

(D) Warning Signs of Pirated Software

An organization and any employees authorized to acquire software should be aware of the following "warning signs" that often accompany pirated software:

- The price of the software is significantly below the software publisher's suggested retail price or otherwise appears "too good to be true."
- The software is distributed in a CD jewel case without the packaging and materials that typically accompany a legitimate product.
- The software lacks the software publisher's standard security features, such as a hardware lock or a certificate of authenticity.
- The software lacks an original license or other information from which an organization can verify that the copyright holder validly licenses its use of such software.
- The packaging or materials that accompany the software have been copied or are of inferior print quality.
- The CD contains software from more than one software publisher or programs that are not typically sold as a "suite."

- The software is downloaded via the Internet without the software publisher's authorizations.
- The software is distributed via a mail-order or online reseller that fails to provide appropriate guarantees of legitimate product.
- The software contains markings indicating that distribution to, and use by, the organization would violate the software publisher's license (e.g., "distribute only with new PC hardware," "Academic version," "Upgrade," etc.).
- The software is loaded onto computer hardware without a separate license or invoice indicating a legitimate purchase.

(E) Steps to Take if Pirated Software is Suspected

If an employee suspects that software offered or supplied by a reseller is pirated, the employee should contact the software publisher or an authorized reseller to investigate. If the employee's suspicions are confirmed, an organization should take one or more of the following remedial actions:

- Return the pirated software and request legitimate replacement software or a refund.
- Withhold payment under the software contract until legitimate software is supplied.
- Terminate the contract for the vendor's failure to comply with its terms.
- Suspend and/or debar the reseller for committing an offense that indicates a lack of business integrity, for engagement in fraud, or for willfully failing to comply with contract terms.
- Bring a False Claims Act action against the contractor for payments related to the illegal computer software.

(iii) Sample Software-Management Policy

(A) Purpose

This policy sets forth the steps an organization can take to comply with applicable laws and regulations in managing computer software.

(B) Software Acquisition and Installation Procedures

Where possible, all requests for new software and software upgrades shall be submitted to the CIO or his designee. All new software and software upgrades not acquired by the CIO shall be documented and identified to the CIO or his designee, who will verify that an organization has an appropriate license for the use of such software. All acquisitions of hardware that include bundled software shall be documented and identified to the CIO or his designee, who will verify that the organization has an appropriate license for the use of such bundled software.

(C) Destruction of Unauthorized Software

The CIO or designated employees shall destroy all copies of software for which the organization lacks the appropriate license. Alternatively, the CIO may obtain the license(s) necessary to maintain such software on the organization's computers.

(D) Software Management and Inventory

An organization shall conduct on a periodic basis (i) an assessment of its software management procedures and practices and (ii) an inventory of installed software and related license agreements, purchase invoices, and other documentation evidencing licensed software. The CIO shall supervise such assessment and inventory with assistance, as needed, from the organization's internal audit director, designated employees, and/or outside consultants.

(E) Recordkeeping

An organization, under the supervision of the CIO, shall establish and maintain a recordkeeping system for original software licenses, certificates of authenticity, purchase invoices, completed registration cards, original software media (e.g., diskettes or CD-ROMs), user information, and assessment information.

(F) Software use Policy

All employees should comply with the following software use policy:

a. Prohibitions against Unlicensed Software Use.

No employee shall:

(i) Install, reproduce, distribute, transmit, or otherwise use software for which an organization lacks the appropriate license, unless such software is properly licensed to the employee and used in accordance with organization policy and the applicable license. If an employee becomes aware of the reproduction, distribution, or use of unauthorized software in an organization, he/she should promptly notify his supervisor or the CIO.

(ii) Install, reproduce, or use any software upgrade on a computer that does not already have resident on it the original version of the software.

(iii) Loan, distribute, or transmit organization software to any third party, unless the employee is expressly authorized to do so by his supervisor and the applicable license

b. Authorization to Use an Organization's Software at Home Computers

The licenses for some organization's software permit employees of the organization to make a copy of the software for home use. In such event, employees may make a copy of the organization's software for home use only if they demonstrate a need to conduct business from home and they receive express authorization from their supervisor, the CIO, or the CIO's designee. Under no circumstances, however, may an employee use the organization's software for purposes other than the business of the organization.

c. Downloading of Software from the Internet or Other Sources on to an Organization's Computers

A variety of software is available on the Internet. Some of this software, called "freeware" or "shareware," is available free of charge for limited uses and may be downloaded by an employee with the prior approval of his supervisor. Other software available on the Internet and from other electronic sources, however, requires the user to obtain a license for its use, sometimes for a fee. No employee shall download licensed software to his workstation without the prior approval of his supervisor, the CIO, or the CIO's designee.

d. Enforcement

The CIO shall supervise periodic reviews and assessments to evaluate the effectiveness of the software management policy. As part of this process, the CIO or his designee may ask employees to complete a software user survey. This survey will be used to determine the organization's existing and future use of and need for particular software programs. An employee will be held responsible for the existence of any software at his workstation when the organization lacks the appropriate license.

e. Questions

An employee may direct any questions concerning this policy to his supervisor or the CIO (provide phone numbers, office locations, and e-mail addresses).

(G) Education and Training

An organization shall provide education and training to all existing and new employees in compliance with the policy. As part of such education and training, the organization shall:

- Amend the employee handbook to include the software management policy and distribute the updated handbooks to all employees.
- Provide training to new and existing employees on (i) the software management policy, (ii) how to detect and prevent piracy, (iii) consequences of violating the policy and applicable copyright laws. Such training may be conducted as a separate seminar or as a part of existing training programs.
- Circulate reminders of the policy on a regular basis (at least annually) or remind employees of the policy in other ways (at least annually)—for example, through notices in the organization's newsletters
- Inform employees where they can get additional information on the policy and on software piracy prevention

(H) Performance Measures

The CIO shall develop performance measures to monitor an organization's compliance with the policy.

(iv) Wireless Technology Best Practices

(A) Threats to and Vulnerabilities of Wireless LANs

Wireless communications offer organizations and users many benefits, such as portability and flexibility, increased productivity, and lower installation costs. Wireless technologies cover a broad range of differing capabilities oriented toward different uses and needs. Wireless local area network (WLAN) devices, for instance, allow users to move their laptops from place to place within their offices, without the need for wires and without losing network connectivity. Less wiring means greater flexibility, increased efficiency, and reduced wiring costs. Ad hoc networks, such as those enabled by Bluetooth, allow data synchronization with network systems and application sharing between devices. Bluetooth functionality also eliminates cables for printer and other peripheral-device connection. Handheld devices such as personal digital assistants (PDAs) and cell phones allow remote users to synchronize personal databases and provide access to network services such as wireless e-mail, Web browsing, and Internet access. Moreover, these technologies can offer dramatic cost savings and new capabilities to diverse applications ranging from retail settings to manufacturing shop floors.[19]

Wireless networks include wireless LANs and ad hoc networks. Wireless devices include PDAs, smart phones, universal serial bus (USB), and Bluetooth. Wireless standards include IEEE 802.11 and Bluetooth. WLANs follow the IEEE 802.11 standards, and ad hoc networks (personal area networks) follow the Bluetooth standards.

However, risks are inherent in any wireless technology. Some of these risks are similar to those of wired networks; some are exacerbated by wireless connectivity; some are new. Perhaps the most significant source of risks in wireless networks is that the technology's underlying communications medium, the airwave, is open to intruders, making it the logical equivalent of an Ethernet port in the parking lot.

The loss of confidentiality and integrity and the threat of denial-of- service (DoS) attacks are risks typically associated with wireless communications. Unauthorized users may gain access to organization's systems and information, corrupt the organization's data, consume network bandwidth, degrade network performance, launch attacks that prevent authorized users from accessing the network, or use an organization's resources to launch attacks on other networks.

Specific threats to and vulnerabilities of wireless networks and handheld devices include:

- All the vulnerabilities that exist in a conventional wired network apply to wireless technologies.
- Malicious entities may gain unauthorized access to an organization's computer network through wireless connection, bypassing any firewall protections.
- Sensitive information that is not encrypted (or that is encrypted with poor cryptographic techniques) and that is transmitted between two wireless devices my be intercepted and disclosed.
- Denial of service (DoS) attacks may be directed at wireless connections or devices.
- Malicious entities may steal the identity of legitimate users and masquerade as them on internal or external corporate networks.
- Sensitive data may be corrupted during improper synchronization.
- Malicious entities may be able to violate the privacy of legitimate users and be able to track their movements.
- Malicious entities may deploy unauthorized equipment (e.g., client devices and access points) to surreptitiously gain access to sensitive information.
- Handheld devices are easily stolen and can reveal sensitive information.
- Data may be extracted without detection from improperly configured devices.
- Software viruses and other malicious code may corrupt data on a wireless device and subsequently be introduced to a wired network connection.
- Malicious entities may, through wireless connections, connect to other organizations for the purposes of launching attacks and concealing their activities.
- Interlopers, from inside or out, may be able to gain connectivity to network management controls and thereby disable or disrupt operations.

- Malicious entities may use third-party, untrusted wireless network services to gain access to an organization's network resources.
- Internal attacks may be possible via ad hoc transmissions.

Organizations should be aware that maintaining a secure wireless network is an ongoing process that requires greater effort than is required for other networks and systems. Moreover, it is important that organizations assess risks more frequently and test and evaluate system security controls when wireless technologies are deployed. Maintaining a secure wireless network and associated devices requires significant effort, resources, and vigilance, and involves the following practices:

- Maintaining a full understanding of the topology of the wireless network
- Labeling and keeping inventories of the fielded wireless and handheld devices
- Creating backups of data frequently
- Performing periodic security testing and assessment of the wireless network
- Performing ongoing, randomly timed security audits to monitor and track wireless and handheld devices
- Applying software patches and security enhancements
- Monitoring the wireless industry for changes to standards that enhance security features and for the release of new products
- Vigilantly monitoring wireless technology or new threats and vulnerabilities

Organizations should not undertake wireless deployment of essential operations until they have examined and can acceptably manage and mitigate the risk to their information, system operations, and continuity of essential operations. Organizations should perform a risk assessment and develop a security policy before purchasing wireless technologies, because their unique security requirements will determine which products should be considered for purchase.

The risks related to the use of wireless technologies are considerable. Many current communications protocols and commercial products provide inadequate protection and thus present unacceptable risks. Before deploying wireless technologies, an organization must actively address such risks in order to protect its ability to support essential operations. Furthermore, many organizations poorly administer their wireless technologies. Some examples include deploying equipment with "factory default" settings, failing to control or inventory access points, not implementing the security capabilities provided, and not developing or employing a security architecture suitable to the wireless environment (e.g., one with firewalls between wired and wireless systems, blocking of unneeded services/ports, use of strong cryptography). To a large extent, most of the risks can be mitigated. However, mitigating these risks requires considerable tradeoffs between technical solutions and costs. Today, the vendor and standards community is aggressively working toward more robust, open, and secure solutions for the near future. For these reasons, it may be prudent to simply wait for these solutions to become more mature.

Organizations should be aware of the technical and security implications of wireless and handheld-device technologies. Although these technologies offer significant benefits, they also provide unique security challenges over their wired counterparts. The coupling of the relative immaturity of the technology with poor security standards, flawed implementation, limited user awareness, and lax security and administrative practices forms an especially challenging combination. In a wireless environment, data is

broadcast through the air without the organization being able to exert physical control over the boundaries of transmissions or to use the controls typically available with wired connections. As a result, data may be captured when it is broadcast. Because of differences in building construction, in wireless frequencies and attenuation, and in the capabilities of high-gain antennas, the distances necessary for positive control for wireless technologies to prevent eavesdropping can vary considerably. The safe distance can vary up to kilometers, even when the nominal or claimed operating range of the wireless device is less than a hundred meters.

Organizations should carefully plan the deployment of 802.11, Bluetooth or any other wireless technology. Because it is much more difficult to address security once deployment and implementation have occurred, security should be considered from the initial planning stage. Organizations are more likely to make better security decisions about configuring wireless devices and network infrastructure when they develop and use a detailed, well-designed deployment plan. Developing such a plan will support the inevitable tradeoff decisions between usability, performance, and risk.

(B) Sample Best Practices in Wireless Technology

The following are best practices and recommendations to be implemented to reduce risks in wireless local area network, grouped into management controls, technical controls, and operational controls:

Management Controls

- Develop an organization security policy that addresses the use of wireless technology, including 802.11. A security policy is the foundation on which other countermeasures (operational and technical controls) are rationalized, implemented, and used.
- Ensure that users on the network are fully trained in computer security awareness and the risks associated with wireless technology (e.g., 802.11). A security awareness program helps users to establish good security practices to prevent inadvertent or malicious intrusions into an organization's information systems.
- Perform a risk assessment to understand the value of the assets in the organization that need protection. Understanding the value of organizational assets and the level of protection required is likely to enable more cost-effective wireless solutions that provide an appropriate level of security.
- Ensure that the client's network interface card (NIC) and access point support a firmware upgrade so that security patches may be deployed as they become available prior to purchase. Wireless products should support upgrade and patching of firmware to be able to take advantage of wireless security enhancements and fixes.
- Perform comprehensive security assessments at regular and random intervals (including validating that rogue access points do no exist in the 802.11 WLAN) to fully understand the wireless-network security posture. Security assessments or audits are an essential tool for checking the security posture of a WLAN and for determining corrective action to make sure it stays secure. Random checks ensure that the security posture is maintained beyond periods of assessment.
- Ensure that external boundary protection is in place around the perimeter of the building(s) of the organization. The external boundaries should be secured—as

with a fence or locked doors—to prevent malicious physical access to an organization's information system infrastructure.
- Deploy physical access controls to the building and other secure areas (e.g., photo ID and card badge readers). Identification badges or physical access cards help to ensure that only authorized personnel have access to gain entry to a facility.
- Complete a site survey to measure and establish the access point coverage for the organization. Proper placement of access points will help ensure that there is adequate wireless coverage of the environment while minimizing exposure to external attack. The site survey should result in a report that proposes access point locations, determines coverage areas, and assigns radio channels to each access point and that ensures that the coverage range does not expose access points to potential malicious activities.
- Take a complete inventory of all access points and 802.11 wireless devices, which can be referenced when conducting an audit for unauthorized use of wireless technologies.
- Ensure that wireless networks are not used until they comply with the organization's security policy. Security policy enforcement is vital for ensuring that only authorized access points and 802.11 wireless devices are operating, and that they are in compliance with the organization's wireless security policy.
- Locate access points on the interior of the buildings instead of near exterior walls and windows. Locating access points near exterior walls and windows provides a better range of access for potential external malicious users. Choosing the location wisely to balance security and coverage should be considered.
- Place access points in secured areas to prevent unauthorized physical access and user manipulation. Physically securing the access points, putting them "out of reach," prevents unauthorized access by potential malicious users.

Technical Controls

- Empirically test access-points range boundaries to determine the precise extent of the wireless coverage. By empirically testing the access-point coverage range for an organization, the level of risk associated with the access range afforded potential malicious users can be better understood.
- Make sure that access points are turned off when not being used (e.g., after hours and on weekends). Shutting down access points when not in use minimizes potential exposure to malicious activity.
- Make sure that the reset function on access points is being used only when needed and only by an authorized group of people. The reset function allows an individual to negate any security settings administrators have configured on an access point.
- Restore the access points to the latest security settings after the reset functions have been used. Security settings are lost after a reset function. Therefore, the appropriate personnel should restore the latest security settings after a reset.
- Change the default service set identifier (SSID) in the access points. Many default SSIDs used by vendors are published and well known. Malicious users often try to connect to 802.11 networks using the default SSID.

- Disable the broadcast SSID feature so that the client SSID must match that of the access points. Malicious users can more easily detect and exploit access points that are broadcasting the SSID. Disabling the broadcast SSID feature minimizes exposure of the access points to malicious users.
- Validate that the SSID character string does not reflect the organization's name (e.g., division, department, or street) or products. The SSID should not make it easy for malicious users to determine the organization that owns the access point, and it should be long and difficult to guess.
- Ensure that access point channels are at least five channels different from any other nearby wireless networks to prevent interference. Radio interference between access points can result in a denial of service. As a result, using channels in a different range ensures service availability.
- Understand and make sure that all default parameters are changed. Because default settings are generally known and not secure, these settings should be changed and should comply with organizational security policy.
- Disable all insecure and nonessential management protocols on the access points. Management protocols that are enabled on access points but not used present a potential avenue of attack. Disabling all insecure and nonessential management protocols minimizes potential methods that a hostile entity can use when attempting to compromise an access point.
- Enable all security features of the WLAN product, including the cryptographic authentication and wired equivalent privacy (WEP) feature. Establishing built-in security features provides greater security than the default settings.
- Ensure that encryption key sizes are as large as possible, or at least 128 bits. Brute force attacks on encryption key sizes become more difficult as the key sizes increase. The addition of a single bit doubles the key space. A 128-bit provides an "intractable" key space against cryptanalysis if the algorithm and implementation are sound.
- Make sure that default shared keys are periodically replaced by more secure unique keys. Periodically changing default shared keys decreases the likelihood that a malicious user can exploit a compromised key. A changed key increases the adversary's difficulty.
- Install a properly configured firewall between the wired infrastructure and the wireless network (i.e., access point or hub to access points). A firewall can enforce a security policy on the information flow between the wired network and the wireless network.
- Install anti-virus software on all wireless clients. Anti-virus software helps ensure that the wireless client does not introduce known worms and viruses to the wired network while protecting the wireless client from viruses that originate on the wired network.
- Install personal firewall software on all wireless clients, as it can help to protect against wireless network attacks.
- Disable file sharing on wireless clients (especially in untrusted environments). Malicious users can potentially exploit wireless clients enabled for file sharing.

- Deploy media access control (MAC) access control lists. The use of access control lists based on MAC hardware addresses provides a layer of security that ensures that only authorized wireless devices are allowed to connect to the wired network.
- Consider installation of switches in lieu of hubs for access point connectivity. The use of switches segments network traffic and minimizes potential for a hostile user to monitor traffic by connecting to a hub.
- Deploy Internet Protocol Security–based (IP Sec-based) virtual private network (VPN) technology for wireless communications. The use of IPsec-based VPN provides an overlay protection to the standard link encryption (e.g., WEP) provided by the wireless connecting hosts.
- Ensure that encryption being used is sufficient in regard to the sensitivity of the data on the network and the processor speeds of the computers. Sensitive data transmission should be encrypted. The level of encryption provided must be balanced between data security requirements and the overhead cost related to processor capability.
- Fully test and deploy software patches and upgrades on a regular basis. Newly discovered security vulnerabilities of vendor products should be patched to prevent malicious and inadvertent exploits. Patches should also be fully tested before implementation to ensure that they work.
- Ensure that all access points have strong administrative passwords. Administrator passwords on access points should not be easy to guess. This minimizes the risk of an unauthorized user gaining access by guessing or cracking administrative passwords.
- Ensure that all passwords are being changed regularly. Passwords should be changed regularly to reduce the risk of a compromised password being exploited.
- Deploy user authentication such as biometrics, smart cards, two-factor authentication, and PKI. Implementing strong or two-factor authentication whenever possible minimizes the vulnerabilities associated with simple username and password authentication.
- Ensure that the "ad hoc mode" for 802.11 has been disabled unless the environment is such that the risk is tolerable. Note that some vendor products do not allow disabling this feature; use it with caution or find a different vendor. The ad hoc mode for 802.11 can be exploited. Using hosts with the mode enabled may unintentionally allow outside users to inadvertently or maliciously connect to those systems.
- Use static Internet protocol (IP) addressing on the network to make it more difficult for a hostile user to connect.
- Disable dynamic host control protocol (DHCP). If DHCP is disabled, then hosts are forced to use a static IP address.
- Enable user authentication mechanisms for the management interfaces of the access point. User authentication mechanisms should be enabled to ensure that only authenticated users are allowed access to the management interfaces of an access point.
- Ensure that management traffic destined for access points is on a dedicated wired subnet. Passing management traffic over an "out of band" network or management

subnet protects management traffic, interfaces, and passwords from organizational and outside users.
- Use SNMPv3 and/or secure socket layer/transport layer security (SSL/TLS) protocols for Web-based management of access points. SNMPv3 has enhanced security features relative to its predecessor simple network-management protocol (SNMP) protocol. SNMPv3 and SSL/TLS provide for secure authentication and encryption for Web-based management access of access points.

Operational Controls

- Configure SNMP settings on access points for least privilege (i.e., read only). Disable SNMP if it is not used. SNMPv1 and SNMPv2 are not recommended. Organizations that require SNMP should change the default community string to a strong community string as often as needed. Privileges should be set to "read only" if that is the only access a user requires. SNMPv1 and SNMPv2 message wrappers support only trivial authentication based on plain-text community strings and so are fundamentally insecure and not recommended. Organizations should use SNMPv3.
- Enhance access-point management traffic security by using SNMPv3 or equivalent cryptographically protected protocol. Access-point management traffic should be cryptographically protected. SNMPv3 provides cryptographic mechanisms to provide strong security.
- Use a local serial port interface for access point configuration to minimize the exposure of sensitive management information. Using a local serial port interface for access point configuration ensures that sensitive management information does not traverse the network, and it minimizes the risk of unauthorized users gaining access via a network protocol used to manage the access point.
- Consider other forms of authentication for the wireless network, such as remote authentication dial-in user service (RADIUS) and Kerberos. Use of authentication mechanisms such as RADIUS and Kerberos can improve the security and simplify user management.
- Deploy intrusion detection agents on the wireless part of the network to detect suspicious behavior or unauthorized access and activity. Intrusion detection agents (e.g., host-based or network-based) deployed on the wireless network can detect and respond to potential malicious activities.
- Deploy auditing technology to analyze the records produced by RADIUS for suspicious activity. If RADIUS is used, the audit records should be manually or automatically processed to determine if malicious activity has been directed at the authentication server.
- Deploy an 802.11 security product that offers other security features, such as enhanced cryptographic protection or user authorization features. During product selection, ensure that the product provides enhanced cryptographic protection or user authorization features.
- Enable utilization of crucial mapping keys (802.1X) rather than default keys so that sessions use distinct WEP keys. The use of distinct WEP keys provides more security than default keys and reduces the risk of key compromise.

- Fully understand the impacts of deploying any security feature or product prior to deployment. To ensure a successful deployment, an organization should fully understand the technical, security, operational, and personnel requirements before implementation.
- Designate an individual to track the progress of 802.11 security products and standards, and the threats and vulnerabilities associated with the technology.
- Wait for future releases of 802.11 WLAN technologies that incorporate fixes to the security features or provide enhanced security features. Upgrade to the latest version and avoid purchasing those versions of the 802.11 products with major security vulnerabilities that have not been fixed.
- When disposing access points that will no longer be used by the organization, clear access point configuration to prevent disclosure of network configuration, keys, passwords, and other information.
- If the access point supports logging, turn it on and review the logs on a regular basis. Ensure that the access points are set to perform logging. Review of audit and logging data helps to ensure user accountability and identifies malicious activity.

11.14 COMPUTER OPERATIONS MANAGEMENT

(a) WORKLOAD MANAGEMENT

(i) Overview of Workload Analysis. Organizations should accurately represent the size and composition of their workloads in the performance validation effort. Unfortunately, workload analysis is often the "weak link" in many system acquisitions. Organizations may perform insufficient workload analysis because of ambitious procurement schedules or difficulties in obtaining necessary workload data. Many believe that their current workload is too complex to characterize, or that future requirements are too nebulous to forecast. Incorrect workload analysis leads to wrong capacity planning, which in turn results in grossly inadequate system performance and marked degradation of services.[20]

(ii) Major Issues in Workload Analysis. The following issues merit attention when planning a workload analysis: workload model, workload equivalence, and workload compression.

- **Workload model.** Workload analysis abstracts key characteristics of an operational workload to account for performance of a given system being tested. The analyst builds a model of the workload that preserves some combination of these key characteristics and discards extraneous details. These characteristics, which may be on the physical, logical, or functional level of work, are described below. Selecting appropriate characteristics, measuring them in the operational workload, and summarizing them in the workload model are crucial to workload analysis.
- **Workload equivalence.** Two workloads are equivalent if they result in the same performance when applied to the same computer system. Two equivalent transactions or jobs will have similar average and standard deviation-of-response time, turnaround time, or throughput rate on a given system.

- **Workload compression.** Workload equivalence classes allow compression of the workload from perhaps thousands of transactions and jobs to perhaps a few dozen programs that preserve the essential performance characteristics of the whole. Each equivalence class can be represented by a few of its members (natural benchmark programs) or an abstract entity that reflects its characteristics (synthetic benchmark programs or mathematical models). The total number of programs divided by the number of representative samples is the "compression ratio" of a workload analysis.

(iii) Building the Workload Model for Current Workloads. To build a workload model for an existing workload, the workload analyst selects key characteristics of the workload and measures them on the existing system. The analyst may draw these characteristics from any of three levels: (1) physical workload data, (2) logical workload data, and (3) functional workload data.

Identification of these key characteristics may depend on the analyst's understanding of (1) current hardware or software bottlenecks; (2) crucial system workloads, such as biweekly payroll runs or online transaction-processing systems; and (3) known resource-intensive facilities, such as relational database management systems (DBMSs).

(A) Physical Workload Data

Physical workload means the absorption of resources by a specific physical computing device or component. Examples of devices are central processing units (CPUs), memory, channels, disk controllers, disk and tape drives, and printers. Examples of CPU resources are CPU time, memory space-time, channel and controller percent utilization, disk space utilization, and disk and tape input/output (I/O). Some physical workload data is device- or resource-dependent.

Some examples of physical workload measures include CPU time, memory space-time, disk I/O, channel activity, and network activity. CPU time is the total time a program uses the CPU, often measured in seconds. Operating systems commonly divide the time available on CPUs among competing jobs to avoid idle periods during I/O operations and other inefficiencies. The operating system or an external monitor tallies the total CPU time absorbed by each job. In a multiprocessor system, the monitor measures time on each CPU and reports the total.

Memory space-time is the integral of the amount of memory used by a program over the time it takes to execute the program. It is essentially the average amount of memory multiplied by the execution time. Performance bottlenecks frequently arise in the disk I/O subsystem. Timing components of disk response include seek time, rotational delay, and transfer time. Seek time is the delay in positioning the disk head over the correct track. Rotating magnetic disks are built with movable read/write heads, which must be positioned over the correct track before the data can be read or written. The disk rotates until the sector to be read or written passes under the head. This is called the rotational delay, or latency. In some environments, seek time and rotational delay partially overlap. Transfer time starts when the first part of the data is read from the disk and transferred through the path into system memory, and it ends when it is available to the task that requested it. The CPU will usually be executing other work at the time, and an I/O completion interrupt or other mechanism is used to inform the process that the

data is available. Average disk access time is most often defined as the sum-of-average seek time, average latency, and average transfer time.

Programs require disk I/O to read and write data, for paging and swapping, to fetch library routines, etc. Disk technology is changing; recent developments include solid-state disks and disk caching, multiple disk arrays and disk striping, multiple disk paths for simultaneous access, and optical disks and other novel media.

Physical workload measures of disk activity include counts of reads and writes, percent utilization, device queuing, timing of disk access components, and access time. These measures are available from software monitors.

In channel activity, channels connect CPUs with peripheral devices and device controllers. Because multiple devices may share a channel, contention for its use can delay program execution. Performance monitors often report channel activity in terms of percent utilization.

In network activity, distributed systems may involve networks that attach terminals to CPUs and interprocessor communications, for example. Network activity may be reported as traffic count, response time, percent utilization, or other measures.

In summary, of the available physical workload measures, analysts most frequently select CPU time, memory space-time, and I/O count to build the workload model. The most important of these will vary among workloads. CPU is often a bottleneck in scientific applications, memory in time-sharing systems, and I/O in commercial batch applications. For example, tape I/O may dominate logging and system backup tasks, but it is rarely important within production applications.

Analysts should measure the use of these physical resources by individual jobs or transactions, not in the aggregate. Job-specific measures are necessary to establish workload equivalence classes. Although physical workload forms an important component of workload characterization, it alone is not sufficient. Some logical or functional data should supplement the physical workload analysis. Analysts should divide the workload into gross functional categories such as interactive transaction–processing jobs, office automation jobs, and all batch COBOL-processing jobs.

(B) Logical Workload Data

Logical workload is expressed in terms of software, such as programs written in COBOL, FORTRAN, or C. A single COBOL program can be compiled and executed on many different computers. Each computer might use different physical resources to execute the program, but the logical workload—the COBOL program—remains constant.

Logical workload is less system-dependent than physical workload but still has some system dependencies. A COBOL program constructed to run quickly on one computer may be poorly constructed for a different computer. For example, a vendor may need to access a library of file-handling routines to increase efficiency, and this may require revision of the source program.

Characteristics of logical workload data include (1) the type and extent of numeric and character operations, (2) program structure, (3) data structures, (4) reading and writing to files and terminals, and (5) systems software workloads. Examples of systems software workloads include task priority levels and system services such as system security, performance monitoring, database journaling, and network management. They also include measuring the number of simultaneous active batch jobs and interactive users at

the multiprogramming level. In transaction-processing and database-management environments, the analyst should focus on calls to the teleprocessing monitor and database. Systems software activity is important in environments where contention among multiple jobs or interactive users requires significant supervision by the operating system.

(C) Functional Workload Data

The functional workload is composed of business functions such as number of claim forms processed, number of editing transactions in a word processing document, number of program compiles, number of accounting transactions entered in a journal, and number of inventory part numbers queried.

Analysis of functional workloads is straightforward when the application program already exists. If a claims-processing program exists on the current system, the workload analyst can project the arrival rate of claim transactions during the system's life and size the benchmark arrival rate accordingly. Functional workload analysis is more difficult when the application program is still in the planning stages. This type of analysis may require software performance engineering. A functional workload model is appropriate if the software applications to be proposed and evaluated will be off-the-shelf packages (e.g., word processing, electronic mail, spreadsheets, and database query language) from vendors with dissimilar architectures.

A functional workload characterization is advantageous because it ensures workload equivalence. Vendors are sometimes critical of physical and logical workload models, but they rarely dispute functional workload data. Natural benchmarks are a direct extension of functional workload models. These models are good when vendors propose a diversity of architectures, operating systems, and other systems software. The system-independence of the functional characterization allows all vendors an equal opportunity to show their equipment to its best advantage. This applies to various performance and validation methods based on functional workload analysis, including benchmarks, analytical or simulation performance models, and informal methods.

(iv) Steps of Workload Analysis. After deciding the level of detail for workload characterizations (physical, logical, or functional), the analysis proceeds as follows:

- Workload data collection
- Workload data reduction
- Workload forecasting
- Management review of workload data

(A) Workload Data Collection

Workload data collection requires the cooperation of application system users. Users may resist requests for data that seems excessively detailed or not easily understandable. Strategies to improve the quality of data collected include researching existing reports, such as end-of-run reports from the job entry subsystem, and researching existing internal application documentation for system size.

(B) Workload Data Reduction

Some sources of workload data, particularly software monitors, can produce voluminous data. To make these data useful, the analyst will need to reduce them In data reduction, the

analyst seeks parsimony, preserving the equivalence characteristics of the workload while reducing the volume of data. Examples of data reduction techniques include univariate statistics, factor analysis, and cluster analysis.

(C) Workload Forecasting

Forecasting future workloads is an inexact science at best, but an organization can still conduct a credible analysis for future requirements. The analyst can combine his knowledge of organization missions and goals with the results of quantitative analysis, such as linear regression, multiple regression, and time-series analysis.

(D) Management Review of Workload Data

After the workload analyst has collected input from system users and historical data on the existing system, has reduced the data statistically, and has forecast future requirements with either quantitative or qualitative methods, management should review and approve the analysis. Management review of workload analysis can take into account important factors that dominate other considerations, such as priorities for certain workloads in preference to others, budgets, and changes in the organization's mission.

(v) Workload Analysis Tools. There are four types of tools available for analyzing computer workloads: software monitors and measurement tools, hardware monitors, manual methods, and statistical software packages. These tools are helpful in establishing computer capacity.

(A) Software Monitors and Measurement Tools

Software monitors are programs that execute in a computer system to observe and report on the behavior of the system. They collect much useful data for workload analysis. Software monitors are either event-driven or sampling monitors. Event-driven monitors collect data when a specific event in the computer system occurs (e.g., initiation or completion of a job, or displaying a task from a ready queue). Sampling monitors collect data at regular intervals (e.g., once every millisecond). Sampling monitors produce profiles of resources in the aggregate (e.g., percent CPU utilization at one-hour intervals). Software monitors are intrusive because they place additional work on the processor and the rest of the system. Also, software monitors collect data through the intervention of the systems software, and this cannot detect the most subtle phenomena, e.g., cache hit rates.

Examples of these monitors include operating system monitors and DBMS monitors. Operating system monitors produce job-specific data that is useful for workload characterization. Job- or process-level data is used in cluster analysis to gather jobs with similar characteristics into groups. These clusters become the components used in benchmark or model construction. DBMS monitors provide more detailed data than the operating system monitors due to their built-in software monitors. Some examples of resources measured include: average response time, device utilization, percent channel path busy, total percent CPU utilization, paging rate per second, average queue length, number of physical writes to database, I/O transfer rate, and amount of memory available.

An instruction-counting monitor tabulates the relative frequency of different assembler instructions, such as load, store, or add instructions. Two types of traces exist: static traces and dynamic traces. Static traces work by processing source code or

object code without executing it. Dynamic traces work by observing frequencies as the program executes. Static traces usually do not require altering software. Dynamic traces usually require either modification of the application code or the existence of a trace facility in the operating system.

For natural benchmarks, it is important to measure the frequency of execution of a program or its modules. For example, suppose cluster analysis assigned a program execution to a particular cluster on a given day. If assignment of a program execution to a cluster depends on the size of an input file, then the analyst should know the size of the input file for the interval of the analysis.

(B) Hardware Monitors

Hardware monitors work by attaching probes to processor circuits and detecting and recording events during those probes. The events are detected as changes in voltage levels at the probe points. Hardware monitors are expensive and require an intimate knowledge of the system to be tested. The use of integrated circuits means that probe points may not be available, because probes cannot be inserted into computer chips.

(C) Manual Methods

Manual methods include user surveys, code inspections, and published surveys. The workload analyst will need to gather data from system users or user management by means of a user survey. Trends in use of the existing system and in estimates of requirements for new application systems need to be quantified.

Some significant attributes of program behavior are not easily captured with either hardware or software monitors. When the program attribute is significant enough, visual scanning of samples of the source code is better. One example involves the size of the loops and other iterative program structures. Almost all software will cycle through loops and other repetitive structures, as it tests for conditions, executes numerical algorithms, spins at locks, etc. Loops display the important characteristic of reference locality. Published studies are good for low-cost, low-risk acquisitions such as the common behavior exhibited in regard to online transaction processing.

(D) Statistical Software Packages

Most packages run interactively and have convenient macro or command capabilities for data reduction and regression analysis.

(vi) Performance and Capability Validation. Performance validation is the process of verifying that an offered information system or component can satisfy the performance requirements specified in a solicitation. Performance is often difficult to measure because it results from the interaction of many discrete hardware and systems software components. It is highly dependent on the user workload (e.g., applications software). Capability validation is the process of verifying that an offered information system satisfies the functional specifications in a solicitation. If performance validation answers the question “How fast can the system complete the work?”, then capability validation answers the question “Can the system complete the work?” Performance and capability validation overlap, because any test of performance implicitly tests function as well.

Performance validation techniques include informal and formal decision methods, benchmarking (natural and synthetic), modeling (analytical and simulation), and

rating charts. Examples of informal decision methods are informal decision rules (based on dollar-value thresholds and rules of thumb), prior experience, and consensus methods. Examples of formal decision analysis methods are model building, score sheets, cost-benefit analysis, and rule-based systems using expert systems.

Benchmarks are user-constructed tests that verify the performance of a proposed system by measuring its ability to execute a group of user programs representative of project workload, within certain predetermined user time requirements. Natural workload means that programs and data are in production use. Synthetic workload means that programs and data are specially constructed for use in the benchmark. The benchmark can be partly synthetic and partly natural (e.g., if real programs are used with artificial data).

Modeling uses abstract representations of the behavior of the components and processes of a computer system to predict its performance under varying workloads. Analytical models treat workloads as aggregates, with characteristics described statistically (e.g., average arrival rate for a stream of transactions). Analytical models solve for performance algebraically.

Discrete-event simulation treats workload components as discrete entities (e.g., specific jobs or transactions). Simulation models solve for performance by simulating numerous instances of work being processed and then tabulating the results.

System Monitoring Tools

- Resource utilization statistics
- System uptime data
- System outage analysis
- System response-time analysis
- Service level reporting
- Benchmark data

Rating charts are commercially available computations, often in table form, of comparative information about the performance characteristics of different CPUs, disk devices, etc. Performance is usually measured for a typical workload and may be expressed in a unit of measure such as million instructions per second (MIPS).

There are some risks in using performance validation techniques. Modeling and informal methods may be protested with allegations of inaccuracy. Benchmarks may be protested on the basis of technical contents. It is generally accepted that benchmarks are more accurate than other techniques, discrete event simulation models are the next most accurate, analytical models are the most accurate after that, and informal methods such as rating charts are the least accurate.

Continuing trends reduce the benchmark's cost-effectiveness during procurement of IT resources. Major contributors to the decreasing efficiency of benchmarking include decreasing hardware costs, increasing application complexity, increasing hardware diversity, and increasing system distribution.

Price/performance ratios of computer hardware continue to improve. As the cost of benchmark construction increases, the cost-effectiveness of benchmarking is more frequently challenged. Distributed databases and image processing increase application system complexity, which will drive up the cost of benchmarking. Fair benchmarks

of systems become more complex and costly as equipment diversity increases. Distributed systems with local-area-networks, wide-area networks, intelligent workstations, and tightly and loosely coupled processors are costly to benchmark. Generally, the benchmark test requires interconnecting several systems to measure the performance of the network. Configuring a network of computers is a costly exercise justified only for high-dollar value or high-risk applications.

(b) COMPUTER-OPERATIONS MANAGEMENT BEST PRACTICES. Benchmarking of data centers can provide valuable feedback by using various measurement parameters to compare an individual data center to the "best of breed" centers. This comparison points out areas on which to focus in order to achieve increases in efficiency, quality, and service of data center or computer operations. The efficient data center implements the following six best practices to achieve success:[21]

(i) Best Practice 1: Use economies of scale to reduce costs of hardware and software. The efficient data center can achieve significant savings from large-volume purchases of software and hardware. Software costs are lower for the second CPU and even lower for the third CPU. Also, larger data centers are more likely to negotiate favorable site licenses for software products. Large data centers also tend to obtain better prices for hardware, hardware maintenance, and supplies.

(ii) Best Practice 2: Locate in a low-cost geographic area to reduce operating costs for facility and staff. Large data centers, over 500 installed MIPS and over 100,000 square feet of raised floor, are generally located outside of major metropolitan areas and have a lower occupancy cost than small and medium data centers. Small and medium data centers tend to be located in downtown areas or high-rent industrial parks.

Staffing costs in more rural areas tend to be lower than in major metropolitan areas. The trend toward data center automation means that the level and variety of skills required in the past are no longer required. This contributes to the ability of the data center to relocate to a more rural area with a smaller employee base.

(iii) Best Practice 3: Implement formal capacity planning and increase hardware utilization. Capacity management includes long- and short-term capacity planning as well as everyday utilization management. Large data centers tend to use hardware resources more efficiently and tend not to acquire hardware prematurely. Also, formalized capacity management allows large data centers to lease and/or acquire used hardware to meet short-term capacity requirements rather than acquiring new technology, at list price, at the end of its life cycle. Specific areas to improve include capacity planning and utilization management for CPU, storage, and print resources.

(iv) Best Practice 4: Establish standards and procedures to achieve a high degree of automation. Automation begins in core areas, such as standards and procedures, disk/tape management, security, and data center reporting. The focus then shifts to service areas, such as production job management, output management, and operational controls. The third area focuses on efficiency, including console management and performance management. The fourth and final area focuses on quality, including software configuration management. Automation products are available for advanced print, output (e.g., online viewing) management, input/output balancing and reconciliation, and job scheduling.

(v) Best Practice 5: Optimize workflows. The efficient data center optimizes the workflow by eliminating or reducing physical movements of items into and out of the data center and between workstations within the data center. It focuses on (1) data center inputs (e.g., vendor software, application system changes, data from customers, special job requests, and supplies) and outputs (e.g., reports to users, off-site storage, and data to users and customers) and (2) internal data center station-to-station movements (e.g., job scheduling and setup, console operations, network control, customer service, input and output control, and report printing and distribution).

(vi) Best Practice 6: Implement organizational changes to promote quality and efficiency. The efficient data center overcomes the organizational politics. Several activities are undertaken, including (1) developing quality assurance function within the data center for report design, job setup, data center and user reconciliations, and production job submission by end users, (2) transferring job control language ownership, (3) integrating problem, change, and configuration management, (4) providing tools to help-desk and customer service staff to analyze performance monitors, automated consoles, and automated scheduling, and (5) integrating console operations, network monitoring, and help-desk functions, including local area network (LAN) management, wide area network (WAN) management, and other types of networks. For example, an online performance-monitoring software can measure the response time for an application system, where the response time is defined as execution/cycle time plus data file input and output time plus CPU time plus network time.

11.15 INFORMATION-TECHNOLOGY CONTINGENCY PLANNING

(a) OVERVIEW. IT contingency planning is one modular piece of a larger contingency and continuity of operations (COOP) planning program that encompasses IT, business processes, risk management, financial management, crisis communications, safety and security of personnel and property, and continuity of government. Each piece is operative in its own right, but in concert they create synergy that efficiently and effectively protects the entire organization.[22]

Contingency planning for information systems is a required process for developing general support systems (GSS) and major applications (MA) with appropriate backup methods and procedures for implementing data recovery and reconstitution against IT risks. Risks to information systems may be natural, technological, or human in nature. Contingency planning consists of (1) a process for recovery, and (2) documentation of procedures for conducting recovery.

(b) METHODOLOGY. A seven-step methodology for developing an IT contingency process and plan is presented here. Planning, implementing, and testing the contingency strategy are addressed by six of the seven steps; the final step is documenting the plan and establishing procedures and personnel organization for implementing the strategy.

Step 1: Develop Contingency Planning Policy Statement
Step 2: Conduct Business Impact Analysis
Step 3: Identify Preventive Controls
Step 4: Develop Recovery Strategies

EXHIBIT 11.4 THE SEVEN-STEP IT CONTINGENCY PLANNING PROCESS

Step 5: Develop IT Contingency Plan
Step 6: Plan Testing, Training, and Exercises
Step 7: Plan Maintenance

Exhibit 11.4 highlights contingency planning activities involved in each step that should be addressed during all phases of the system-development life cycle (SDLC).

The capability to recover and reconstitute data should be integral to the information-system design concept during the Initiation phase. Recovery strategies should be built into the general support systems or major application's architecture during the Development phase. The contingency processes should be tested and maintained during the Implementation phase; contingency plans should be exercised and maintained during the Operations/Maintenance phase. When the information system has reached the Disposal phase, the legacy system should remain intact and operational as a contingency to the replaced information system.

(i) Step 1: Develop Contingency Planning Policy Statement. When developing an IT contingency plan, the first step is to establish a contingency planning policy within the organization. This policy may exist at the department, agency, and/or program level of the organization. The statement should define the organization's overall contingency objectives; identify leadership roles and responsibilities, resource requirements, test, training, and exercise schedules; and develop maintenance schedules and determine the minimum required backup frequency.

(ii) Step 2: Conduct Business Impact Analysis. A business impact analysis (BIA) is a critical step to understanding the information system's components, interdependencies, and potential downtime impacts. Contingency-plan strategy and procedures should be designed with the results of the BIA in mind.

A BIA is conducted by identifying the system's critical resources. Each critical resource is then further examined to determine how long functionality of the resource could be withheld from the information system before an unacceptable impact is experienced.

The impact may be something that materializes over time or may be tracked across related resources and dependent systems (e.g., cascading domino effect). The time identified is called a maximum allowable outage (MAO). Based on the potential impacts, the amount of time the information system can go without the critical resource then provides a recourse recovery priority around which an organization can plan recovery activities. The balancing point between the MAO and the cost to recover establishes the information system's recovery time objective (RTO). Recovery strategies must meet the RTO.

The strategy must also address recovering information-system critical components within a priority system, as established by their individual RTOs.

(iii) Step 3: Identify Preventive Controls. In some cases, implementing preventive controls might mitigate outage impacts identified by the BIA. Preventive controls are measures that detect, deter, and/or reduce impacts to the system. When cost-effective, preventing an impact is more desirable than implementing recovery strategies (and therefore risking data loss and impact to the organization). Preventive measures are specific to individual components and the environment in which the components operate. Common controls include:

- Uninterruptible power supply
- Fire suppression systems
- Gasoline- or diesel-powered generators
- Air-conditioning systems with excess capacity to permit failure of certain components
- Heat-resistant and waterproof containers for backup media and vital nonelectronic records
- Frequent, scheduled data backups

(iv) Step 4: Develop Recovery Strategies. When a disruption occurs despite the preventive measures implemented, a recovery strategy must be in place to recover and restore data and system operations within the RTO period. The recovery strategy is designed from a combination of methods, which together address the full spectrum of information system risks. Several options may be evaluated during the Development phase; the most cost-effective, based on potential impact, should be selected and integrated into the information system architecture and operating procedures.

System data must be backed up regularly; therefore, all IT contingency plans should include a method and frequency for conducting data backups. The frequency of backup methods—daily or weekly, incremental or full—should be selected based on system criticality when new information is introduced. The backup method selected should be based on system and data availability and integrity requirements (as defined in the BIA). Data that is backed up may need to be stored off site and rotated frequently, depending upon the criticality of the system.

Major disruptions to system operations may require restoration activities to be implemented at an alternate site. The type of alternate site selected must be based on RTO requirements and budget limitations. Equipment for recovering and/or replacing the information system must be provided as part of the recovery strategy. Cost, delivery time, and compatibility factors must also be considered when determining how to provide the necessary equipment. Agencies must also plan for an alternative site that, at a minimum, provides workspace for all contingency plan personnel, equipment, and the appropriate IT infrastructure necessary to execute IT contingency plan and system recovery activities. In developing a recovery strategy, the alternative site's level of operational readiness is an important characteristic to pin down.

The recovery strategy requires personnel to implement the procedures and test operability. Generally, a member of the organization's senior leadership is selected to activate the plan and lead overall recovery operations. Appropriate teams of personnel (at least two people, to ensure there is a primary and an alternative available to execute procedures) are identified to be responsible for specific aspects of the plan.

Personnel should be chosen to staff the teams based on their normal responsibilities, system knowledge, and availability to recover the system on an on-call basis. A line of succession should be defined to ensure that someone could assume the role of senior leadership if the plan leader is unable to respond.

Having selected choices for each component of the recovery strategy, the final consideration should be given to cost. The recovery strategy must meet criticality, availability, and RTO requirements while remaining within budget. Less obvious costs—such as shipping, awareness programs, tests and exercises, travel, labor hours, and contracted services—must also be incorporated into the evaluation.

(v) Step 5: Develop IT Contingency Plan. Procedures for executing the recovery strategy are outlined in the IT contingency plan. The plan must be written in a format that will provide the users (recovery team leadership and members) the context in which the plan is to be implemented and the direct procedures, based on role, to execute. IT contingency plans are constructed using five components.

The procedures are documented in the Notification/Activation Phase, Recovery Phase, and Reconstitution Phase components of the plan. The Supporting Information and Appendices components provide supplemental information necessary to understand the context in which the plan is to be used and gives additional information that may be necessary to execute procedures (e.g., emergency contact information and the BIA).

(vi) Step 6: Plan Testing, Training, and Exercises. Personnel selected to execute the IT contingency plan must be trained to perform the procedures, the plan must be exercised, and the system strategy must be tested.

Plan testing should include:

- System recovery using platform from backup media
- System performance using alternative equipment
- Coordination among recovery teams
- Restoration of normal operations
- Internal and external connectivity
- Notification procedures

Personnel training should include:

- Purpose of the plan
- Cross-team coordination and communication
- Reporting procedures
- Security requirements
- Team-specific processes
- Individual responsibilities

Plan exercises should be designed to individually and then collectively examine various components of the entire plan. Exercises may be conducted in a classroom setting (discussing specific components of the plan and/or impact issues) or they may be functional exercises (simulating the recovery using actual replacement equipment, data, and alternate sites).

(vii) Step 7: Plan Maintenance. The IT contingency plan must always be maintained in a ready state for use immediately upon notification. Periodic reviews of the plan must be conducted for currency of key personnel and vendor information, system components and dependencies, the recovery strategy, vital records, and operational requirements. While some changes may be obvious (e.g., personnel turnover or vendor changes), others will require analysis. The BIA should be reviewed periodically and updated with new information to identify new contingency requirements and priorities. Changes made to the plan are noted in a record of changes, dated, and signed or initialed by the person making the change. The revised plans, or plan sections, are circulated to those with plan responsibilities. Because of the impact that plan changes may have on interdependent business processes or information systems, the changes must be clearly communicated and properly annotated in the beginning of the document.

(c) CONTINGENCY-PLANNING BEST PRACTICES. Organizations should develop and monitor the following metrics:

- Percentage of critical data files and operations with an established backup frequency. The purpose is to gauge the risk exposure due to insufficient backups.
- Percentage of computer-based application systems that have a contingency plan. The purpose is to determine the percentage of application systems in compliance with the requirement to have a contingency plan. Existence of such a plan indicates a certain level of emergency preparedness if the plan were to be activated.
- Percentage of application systems for which contingency plans have been tested in the past year. The purpose is to determine the number and percentage of contingency plans tested in the past year.

11.16 APPLICABLE LAWS, REGULATIONS, STANDARDS, AND PRINCIPLES

Organizations have a legal and ethical obligation to comply with the various federal, state, and local laws, regulations, circulars and bulletins, directives and executive orders, government orders, and ordinances pertinent to a specific business area. Noncompliance with these laws and regulations can lead to fines, civil and/or criminal penalties, probation, and jail punishments (prison time), thus creating reputation (image) risk. Compliance

with industry and/or organization standards, including professional standards, and national/international standards, can increase the quality of products and services, which, in turn, can enhance an organization's reputation and image in the marketplace.

A brief roundup of information about major laws, regulations, and standards is provided here as a reminder for checklist purposes. Note that these laws and regulations are subject to change as new ones are added and existing ones are amended or repealed. The reader is advised to obtain the original laws, regulations, and standards from the official sources for a better understanding of the provisions, requirements, and conditions of the laws, regulations, and standards (www.regulations.gov). Although some of the following laws, regulations, and standards directly affect public sector organizations (i.e., government agencies), private-sector organizations can read, learn, and apply them to improve their business operations on a proactive basis.

U.S. organizations should comply with the following laws, regulations, standards, and principles pertinent to information technology management:

Sarbanes-Oxley Act of 2002. Although the Sarbanes-Oxley (SOX) Act of 2002 applies primarily to financial and accounting practices, it also encompasses the IT functions that support these practices. SOX can be supported by reviewing logs regularly to look for signs of security violations, including exploitation, as well as retaining logs and records of log reviews for future review by auditors.

Clinger-Cohen Act of 1996. The Clinger-Cohen Act of 1996 is intended to improve the productivity, efficiency, and effectiveness of U.S. federal programs through the improved acquisition, use, and disposal of IT resources. Among other provisions, the law (1) encourages federal agencies to evaluate and adopt best management and acquisition practices used by both private- and public sector organizations; (2) requires agencies to base decisions about IT investments on quantitative and qualitative factors associated with the costs, benefits, and risks of those investments and to use performance data to demonstrate how well the IT expenditures support improvements to agency programs through measurements such as reduced costs, improved employee productivity, and higher customer satisfaction; and (3) requires executive agencies to appoint CIOs to carry out the IT management provisions of the act and the broader information-resources management requirements of the Paperwork Reduction Act. The Clinger-Cohen Act also streamlines the IT acquisition process by eliminating the General Services Administration's central acquisition authority, placing procurement responsibility directly with federal agencies and encouraging the adoption of smaller, modular IT-acquisition projects.

Payment Card Industry Data Security Standard. The Payment Card Industry Data Security Standard (PCI DSS) applies to organizations that store, process, or transmit cardholder data for credit cards. One of the requirements of PCI DSS is to track all access to network resources and cardholder data.

Health Insurance Portability and Accountability Act

Purpose. The U.S. Congress recognized the need for national patient-record privacy standards in 1996 when it enacted the Health Insurance Portability and Accountability Act (HIPAA) of 1996. The law includes provisions designed to save money for health care businesses by encouraging electronic transactions, but it also strengthens safeguards to protect the security and confidentiality of that information.

Covered Entities. As required by HIPAA, the final regulation, which took effect on April 14, 2001, covers health plans, health care clearinghouses, and those health care providers who conduct certain financial and administrative transactions (e.g., electronic billing and funds transfers) electronically.

Consumer Control Over Health Information. Patients will have significant new rights to understand and control how their health information is used. It requires (1) educating patients about their privacy protections, (2) ensuring patients' access to their medical records, (3) receiving patients' consent before information is released, and (4) providing recourse if privacy protections are violated.

Security of Personal Health Information. The final rule establishes the privacy safeguard standards that covered entities must meet, but it gives them the flexibility to design their own policies and procedures to meet those standards. The requirements are flexible and scalable to account for the nature of each entity's business and its size and resources.

Covered entities generally will have to (1) adopt written privacy procedures, (2) train employees, and (3) designate a privacy officer. Written privacy procedures include spelling out who has access to protected information, how it will be used within the entity, and when the information may be disclosed. Covered entities will also need to take steps to ensure that their business associates protect the privacy of health information. Covered entities will need to train their employees in their privacy procedures, and must designate an individual to be responsible for ensuring the procedures are followed (privacy officer).

Accountability for Medical Records Use and Release In HIPAA, Congress provided penalties for covered entities that misuse personal health information.

Civil Penalties Health plans, providers, and clearinghouses that violate these standards will be subject to civil liability. Civil money penalties are $100 per violation, up to $25,000 per person, per year for each requirement or prohibition violated.

Criminal Penalties Criminal penalties are up to $50,000 and one year in prison for obtaining or disclosing protected health information; up to $100,000 and up to five years in prison for obtaining protected health information under "false pretenses"; and up to $250,000 and up to 10 years in prison for obtaining or disclosing protected health information with the intent to sell, transfer, or use it for commercial advantage, personal gain, or malicious harm.

U.S. Computer Security Act. The U.S. Computer Security Act of 1987 requires federal agencies to identify sensitive systems, conduct computer security training, and develop computer security plans. The Act focuses on protecting computer-related assets. This Act:

Requires that federal agencies identify existing systems and new systems under development that contain sensitive information

Requires development of a security plan for each identified sensitive computer system

Requires mandatory periodic training in computer security awareness and accepted computer security practice of all employees involved with the management, use, or operation of federal computer systems within or under the supervision of a federal agency

U.S. Privacy Act. The Privacy Act was enacted in 1974 to provide for the protection of information related to individuals maintained in federal information systems, and to grant individuals access to the information concerning them. The Act establishes (1) criteria for maintaining the confidentiality of sensitive data, and (2) guidelines for determining which data are covered.

The Act imposes numerous requirements upon federal agencies to prevent the misuse of data about individuals, to respect the data's confidentiality, and to preserve its integrity. Federal agencies can meet these requirements by the application of selected managerial, operational, and technical control procedures that, in combination, achieve the objectives of the Act.

The major provisions of the Act (1) limit disclosure of personal information to authorized persons and agencies, (2) require accuracy, relevance, timeliness, and completeness of records, and (3) require the use of safeguards to ensure the confidentiality and security of records.

Although the Act sets up legislative prohibitions against abuses, technical and related procedural safeguards are required in order to establish a reasonable confidence that compliance is indeed achieved. It is thus necessary to provide a reasonable degree of protection against unauthorized disclosure, destruction, or modification of personal data, whether intentionally caused or resulting from accident or carelessness.

U.S. Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources.* The OMB Circular A-130, Appendix III, *Security of Federal Automated Information Systems,* establishes a minimum set of controls to be included in federal automated information-security programs, assigns federal agency responsibilities for the security of automated information, and links agency automated information-security programs and agency management-control systems.

U.S. OMB Circular A-123, *Internal Control Systems.* The OMB Circular A-123 has specific policies and standards for federal agencies for establishing and maintaining internal controls in their programs and administration activities. This includes requirements for vulnerability assessments and internal control reviews. The main provisions of A-123 became law through the enactment of the Federal Managers' Financial Integrity Act of 1982.

U.S. OMB Circular A-127, *Financial Management Systems.* OMB Circular A-127 has specific policies and standards for federal agencies for establishing and maintaining internal controls in financial management systems. This includes requirements for annual reviews of agency financial systems that build on reviews required by OMB Circular A-123.

U.S. Federal Managers' Financial Integrity Act. The Federal Managers' Financial Integrity Act of 1982 enacted the main provisions of OMB Circular A-123. The Act's purpose is to ensure that agencies maintain effective systems of accounting and administrative controls against fraud, waste, and abuse.

U.S. Federal Financial Management Improvement Act. The Federal Financial Management Improvement Act (FFMIA) of 1996 requires agencies to have financial management systems that substantially comply with the federal financial management system's requirements, standards promulgated by the government accounting standards advisory board (GASAB) and the U.S. Standard General Ledger at the transaction level. Financial management systems shall have general and application

controls in place in order to support management decisions by providing timely and reliable data. FFMIA sets the requirements for core financial systems.

U.S. Freedom of Information Act. The Freedom of Information Act (FIA) makes federal information readily available to the public. FIA also establishes the conditions under which information may be withheld from the public to ensure that certain information, such as trade secrets, is protected.

Security and Freedom through Encryption Act. The Security and Freedom through Encryption (SAFE) Act, which was approved in 1997, guarantees the right of all U.S. citizens and residents to use or sell any encryption technology. The purpose is to relax export controls on encryption. The bill specifically makes it legal for any person to use encryption, regardless of encryption algorithm, key length, or implementation technique; makes it legal for any person to sell encryption software, regardless of encryption algorithm, key length, or implementation technique; and prohibits the state and federal governments from requiring anyone to surrender control of an encryption key. Note that the bill specifies legal, not illegal, usage of encryption.

The Act, for example, potentially escalates a minor crime to felony status if the person committing the minor crime used encryption in carrying it out. The Act allows the U.S. software industry to provide the data security features that consumers require to protect their data. In the past, government restrictions on encryption prevented this. The Act gives the American software users the freedom to use software with unlimited encryption strengths, prohibits mandatory key escrow requirements, and allows for export of encryption software.

Electronic Communications Privacy Act. The Electronic Communications Privacy Act (ECPA) governs how investigators can obtain stored account records and contents from network service providers, including Internet service providers (ISPs), telephone companies, cell phone service providers, and satellite services. ECPA issues arise often in cases involving the Internet: anytime investigators seek stored information concerning Internet accounts from providers of Internet service, they must comply with the statute.

Promotion of Commerce Online in the Digital Era Act and Encryption Communications Privacy Act. Both the Promotion of Commerce Online in the Digital Era Act and the Encryption Communications Privacy Act significantly liberalized export restrictions on software with strong encryption and seek to protect both privacy and security on the Internet. Both bills give software users the freedom to use data security software without government intervention.

Economic Espionage and Protection of Proprietary Economic Information Act. The Economic Espionage and Protection of Proprietary Economic Information Act of 1995 addresses the problem of industrial and corporate espionage. The law allows the Federal Bureau of Investigation (FBI) to investigate cases in which a foreign intelligence service attacks U.S. firms to gather proprietary information to benefit companies in their own countries. High technology and defense industries are the primary targets. The Act redefines the definition of stolen property to include proprietary economic information.

The Act supplements state trade secret laws and defines a trade secret to be financial, technical, business, engineering, scientific, or economic information, whether tangible or intangible and without regard to how it is stored. In addition, the Act

specifies that the owner must take "reasonable measures" to keep the information secret.

Penalties under the Act are up to $500,000 and 15 years in prison (10 years if a foreign government's interest is not involved). The Act also gives the government the right to seize any proceeds from the sale of trade secrets or property obtained as a result of espionage.

U.S. Federal Sentencing Guidelines. The U.S. federal sentencing guidelines for organizational defendants became effective in November 1991. These guidelines provide judges with a compacted formula for sentencing business organizations for various white-collar crimes. Included are federal securities, antitrust, and employment and contract laws, as well as the crimes of mail and wire fraud, kickbacks and bribery, and money laundering.

To launder money is to disguise the origin or ownership of illegally gained funds to make them appear legitimate. Hiding legitimately acquired money to avoid taxation also qualifies as money laundering. The crime is not limited to drug trafficking. It is associated with nearly all kinds of "crimes for profit," such as real estate fraud and savings and loan abuses.

The federal sentencing guidelines are equally applicable to the computers-and-information-system security function of a business organization, requiring security plans, policies, procedures, and standards to be developed and implemented. It is important to ensure that these policies and procedures reflect the actual controls and practices being used and enforced.

Racketeer Influenced and Corrupt Organizations Act. In 1970, the U.S. Congress enacted the Racketeer Influenced and Corrupt Organizations Act (RICO) as a weapon against mobsters and racketeers who were influencing legitimate business. The Act defines the term "racketeering activities" to include crimes such as mail fraud and fraud committed in the sale or purchase of securities.

Computers are used as a tool or media for perpetrating fraudulent activities. Information-system security management must develop policies, procedures, and standards to prevent and/or detect these fraudulent activities. To this end, security plans and programs must be effective and efficient.

Computer Fraud and Abuse Act. The Computer Fraud and Abuse Act, as amended in 1996, deals with computers used in interstate commerce and makes it a crime and fraud to alter, damage, or destroy information, steal passwords, or introduce viruses or worms. It covers classified defense and foreign relations information, records of financial institutions and credit-reporting agencies, and government computers. Unauthorized access and access in excess of authorization became felonies for incidents involving classified information and misdemeanors for incidents involving financial information. The Act provides for limited imprisonment for the unintentional damage to one year and civil penalties in terms of compensatory damages.

Foreign Corrupt Practices Act. The Foreign Corrupt Practices Act of 1977 requires, among other things, that a public corporation follow certain procedures in preserving records. A vital records program must be initiated and take into consideration legal, regulatory, and business requirements. Internal accounting controls of a corporation should provide reasonable, cost-effective safeguards against the unauthorized use or disposition of company assets. This requires executives of public companies to

preserve computer records, which in turn requires disaster recovery planning. Hefty penalties can be assessed against executives found to be negligent in this area.

Paperwork Reduction Act. The Paperwork Reduction Act (PRA) of 1980 applied life-cycle management principles to information management and focused on reducing the U.S. government's information collection burden. To this end, PRA designated senior information-resources manager positions in the major departments and agencies and gave the positions responsibility for a wide range of functions. PRA also created the Office of Information and Regulatory Affairs within the OMB to provide central oversight of information management activities across the federal government.

U.S. Computer Software Piracy. The purpose of the U.S. executive order on computer software piracy (intellectual property) is to prevent and combat computer software piracy by observing the relevant provisions of international agreements in effect in the United States, including applicable provisions of the World Trade Organization Agreement on Trade-Related Aspects of Intellectual Property Rights, the Berne Convention for the Protection of Literary and Artistic Works, and relevant provisions of U.S. federal law, including the Copyright Act.

Gramm-Leach-Bliley Act. The Gramm-Leach-Bliley Act (GLBA) requires financial institutions to protect their customers' information against security threats. For example, log management can be helpful in identifying possible security violations and resolving them effectively.

Information Quality Act. The Information Quality Act (IQA) of 2001 requires the U.S. Office of Management and Budget (OMB) to issue government-wide guidelines to ensure the quality of information disseminated by federal agencies. The Act ensures and maximizes the quality, objectivity, utility, and integrity of information, including statistical information, disseminated to the public (www.omb.gov).

Federal Information Security Management Act. The Federal Information Security Management Act (FISMA) of 2002 emphasizes the need for each federal agency to develop, document, and implement an organization-wide program to provide information security for the information systems that support its operations and assets. For example, it describes several controls related to log management, including the generation, review, protection, and retention of audit records, as well as the actions to be taken because of audit failure.

FISMA requires the National Institute of Standards and Technology (NIST) to develop standards and guidelines, including minimum requirements for providing adequate information security for all US Federal agency operations and assets.

Voice of the Customer. "Voice of the customer" (VOC) means organizations should listen to and understand the external customers' needs, wants, and expectations (i.e., customers' voice) and provide products and services that truly meet such needs, wants, and expectations. The same thing applies to internal customers' needs (i.e., departments or functions within an organization).

Voice of the Process. "Voice of the process" means understanding and evaluating the nature of process flows, process variations, and process characteristics and capabilities for both products and services. The goal is to reduce process variations in order to make the process stable and predictable and to reduce cycle time.

New work processes must be designed to reduce the cycle time by eliminating stop points, chokepoints, pain points, or fault points in a process that enjoys

the support and availability of resources such as tools, technology, people, equipment, and information. Existing work processes must be (1) streamlined by reviewing the upstream and downstream work steps, (2) simplified by removing unnecessary handoffs, stop points, chokepoints, pain points, or fault points, (3) standardized based on "lessons learned," and (4) institutionalized by being rolled out to the entire organization.

IT Governance Institute. The IT Governance Institute (ITGI) developed and promotes Control Objectives for Information and related Technology (COBIT), which starts from the premise that IT must deliver whatever information a given enterprise needs to achieve its objectives. (www.itgi.org)

In addition to promoting process focus and process ownership, COBIT looks at the fiduciary, quality, and security needs of enterprises and provides seven information criteria that can be used to generally define what a given business requires from IT: effectiveness, efficiency, availability, integrity, confidentiality, reliability, and compliance.

American Institute of Certified Public Accountants. The American Institute of Certified Public Accountants (AICPA) is a professional organization and the voice of the accounting profession. It establishes professional certification (CITP), professional standards, and code of ethics for information technology practitioners to follow. CITP is Certified Information Technology Professional (www.aicpa.org).

Information Systems Audit and Control Association. The Information Systems Audit and Control Association (ISACA) is a professional organization and the voice of the information-security management profession. It establishes professional certification (CISM), professional standards, and a code of ethics for information security managers to follow. CISM is Certified Information Security Manager (www.isaca.org).

International Information Systems Security Certification Consortium Institute. The International Information Systems Security Certification Consortium (ISC2) Institute is a professional organization and the voice of the information security profession. It establishes professional certification (CISSP), professional standards, and a code of ethics for information security practitioners to follow. CISSP is Certified Information Systems Security Professional (www.isc2.org).

American Institute of Certified Public Accountants and Canadian Institute of Chartered Accountants. The American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) offer trust services such as SysTrust and WebTrust. The SysTrust is an assurance service designed to increase the comfort of management, customers, and business partners. Under the SysTrust, an accountant provides an assurance service in which he evaluates and tests whether a system is reliable when measured against four essential principles: availability, security, integrity, and maintainability.

Information Security Forum. The Information Security Forum's (ISF's) *Standard of Good Practice for Information Security* is based on research and the practical experience of forum members. The standard divides security into five component areas: security management, critical business applications, computer installations, networks, and system development.

US Department of Homeland Security. The U.S. Department of Homeland Security cohosted a National Cyber Security Summit in 2003 and formed five task forces,

including the Corporate Governance Task Force. In its report, the task force called upon all organizations to make information security governance a corporate board–level priority. The report requires the Committee of Sponsoring Organizations of the Treadway Commission to revise its document entitled *Internal Control: An Integrated Framework* so that it explicitly addresses information security governance.

Organization for Economic Co-operation and Development. The Organization for Economic Co-operation and Development (OECD) issued Guidelines for the Security of Information Systems in 1980 covering data collection limitations, quality of data, limitations on data use, IT security safeguards, and accountability of the data controller (www.oecd.org).

ISO Standard 17799. The International Standards Organization (ISO) Standard 17799 (formerly known as the British Standard (BS) 7799) is a comprehensive set of controls addressing information security. It is intended to serve as a single reference point for identifying controls needed for most situations where information systems are used in industry and commerce for large, medium, and small organizations. The standard has three major components: confidentiality, integrity, and availability (www.iso.org).

The ISO Standard 17799 points out how organizations are dependent on information systems and technologies, and the need to comply with laws and contractual terms. It makes the point that use of and advances in information technology have increased the range of possible threats to information security, including such things as fraud, unauthorized access, damage, and system failure.

The standard recommends the following controls at the system specification and design stages:

- Information-security policy document
- Allocation of security responsibilities
- Information-security education and training
- Reporting of security incidents
- Virus controls (prevention, detection, and correction)
- Business-continuity planning process
- Control of intellectual property
- Safeguarding of company records and equipment
- Compliance with data protection laws and regulations
- Compliance with organization's security policy

Additional Resources

Malik, Shadan. *Enterprise Dashboards: Design and Best Practices for IT*. Hoboken, NJ: John Wiley & Sons, 2005.

Stenzel, Joe, ed. *CIO Best Practices: Enabling Strategic Value with Information Technology*. Hoboken, NJ: John Wiley & Sons, 2007.

Notes

1. U.S. General Accounting Office, *Improving Mission Performance through Strategic Information Management and Technology: Learning from Leading Organizations* (GAO/AIMD-94-115), Washington, DC: May 1994.
2. GAO, *Maximizing the Success of Chief Information Officers: Learning from Leading Organizations* (GAO/AIMD-00-83), Washington, DC: March 2000.
3. This section is reprinted with permission. Source: COBIT 4.0 © 1996, 1998, 2000, 2004 IT governance Institute. All rights reserved. Used by permission. COBIT is a registered trademark of the Information Systems Audit Control and Association and the IT Governance Institute.
4. This section is reprinted with permission. Source: COBIT 4.0 © 1996, 1998, 2000, 2004 IT governance Institute. All rights reserved. Used by permission. COBIT is a registered trademark of the Information Systems Audit Control and Association and the IT Governance Institute.
5. This section is reprinted with permission. Source: COBIT 4.0 © 1996, 1998, 2000, 2004 IT governance Institute. All rights reserved. Used by permission. COBIT is a registered trademark of the Information Systems Audit Control and Association and the IT Governance Institute.
6. Lynne Rosenthal, *Guidance on Planning and Implementing Computer System Reliability*, NIST Special Publication 500-121, January 1985, Gaithersburg, MD: U.S. Department of Commerce).
7. GAO, *Measuring Performance and Demonstrating Results of Information Technology Investments* (GAO/AIMD-98-89), Washington, DC: March 1998.
8. Federal Acquisition Regulation (FAR), FAC 97-02, FAC 97-10, FAC 97-12, FAC 97-14, 1997–1999, Washington, DC: U.S. Government.
9. GAO, *Assessing Risks and Returns: A Guide for Evaluating Federal Agencies' IT Investment Decision Making*, Version 1 (GAO/AIMD-10.1.13), Washington, DC: Feb. 1997.
10. *Information Security Handbook: A Guide for Managers*, NIST Special Publication 800-100, Chapter 3, June 2006, (Gaithersburg, MD: U.S. Department of Commerce).
11. GAO, *Information Security Risk Assessment: Practices of Leading Organizations* (GAO/AIMD-99-139), Washington, DC: Aug. 1999.
12. GAO, *Information Security Management: Learning from Leading Organizations* (GAO/AIMD-98-68), Washington, DC: May 1998.
13. *Engineering Principles for Information Technology Security*, NIST SP 800-27RA, National Institute of Standards and Technology (NIST), June 2004, Gaithersburg: MD: U.S. Department of Commerce.
14. *Information Security Handbook: A Guide for Managers*, NIST Special Publication 800-100, chap. 13, June 2006, (Gaithersburg, MD: U.S. Department of Commerce).
15. *Information Security Handbook,* chap. 6.
16. *Guidelines on Electronic Mail Security*, NIST SP 800-45, Version 2, National Institute of Standards and Technology (NIST), February 2007, Gaithersburg, MD.
17. This section is reprinted with permission. Source: *E-Commerce Security: Enterprise Best Practices*, ©2000 Information Systems Audit and Control Foundation,. All rights reserved.
18. *Implementing the Executive Order on Computer Software Piracy*, Tool Kit 2000, January 2000, (Washington, DC: The CIO Council, http://www.cio.gov.
19. *Wireless Network Security: 802.11, Bluetooth and Handheld Devices*, NIST SP 800-48, National Institute of Standards and Technology (NIST), November 2002, (Gaithersburg, MD: U.S. Department of Commerce).
20. U.S. General Services Administration, *A Guide for Performance and Capability Validation* (KMP-94-2-P), Washington, DC: Dec. 1993.
21. *Best Data Center Practices*, December 1994, (Washington, DC: Defense Information Systems Agency [DISA], U.S. Department of Defense).
22. *Information Security Handbook*, chap. 9.

CHAPTER 12

INTERNATIONAL-BUSINESS MANAGEMENT BEST PRACTICES

12.1 OVERVIEW

This chapter focuses more on major issues confronting international business managers and executives, and less on best practices, because best practices in the international arena are dependent on at least two countries' (i.e., Country A's and Country B's) business methods, cultures, and political, social, and economic environments. Therefore, this chapter focuses on the U.S. side of the international business equation (i.e., Country A). One of the major issues facing the U.S.-based international business managers and executives when doing business outside the United States is dealing with U.S. trade laws and regulations, which are confusing, duplicative, and time-consuming because their enforcement mechanism is spread among several agencies with different strategies and priorities.

12.2 ROLES AND RESPONSIBILITIES OF CHIEF GLOBALIZATION OFFICER

The Chief Globalization Officer is a key person in the C-level executive suite and has the following roles and responsibilities.

- Developing global business strategies in harmony with corporate business strategies
- Understanding the risks involved in conducting international business
- Establishing proper organization structure and control at the global level
- Understanding U.S. trade laws and regulations and the inner workings of international trade, economics, investment, banking, and payment methods, including the laws and regulations of the country in which the business is conducted
- Promoting harmony with international cultures and workforce diversity
- Applying ethical principles and values to international business, including in the matter of bribes and gifts
- Lowering total manufacturing and service costs in order to lower selling prices, increase sales volume, and increase profits
- Linking production and service costs to cash flows and gross profits
- Increasing faster product and service deliveries to customers to achieve their total satisfaction
- Innovating new production and service techniques and processes by leveraging technology to improve quality and to reduce costs

- Eliminating non-value-added activities in production and service to trim waste and to lower costs
- Focusing more on value-added activities in production and services to provide a solid value to the customers and to the organization
- Identifying key drivers of cost, quality, risks, expenses, revenues, profits, business growth, competition, and performance. Focus on the root causes of these drivers and understand why these drivers go up and down
- Seamlessly integrating the back-end systems with the front-end systems for (1) maximum data consistency, completeness, and accuracy, (2) better customer service and satisfaction, and (3) stronger connection of disparate business processes
- Building standardized, transparent, and repeatable production and service processes to provide the stable, consistent, and quality products and services that customers expect. First, streamline both upstream and downstream business processes involved in international licensing and franchising arrangements, and other operations; second, simplify; third, standardize; and then institutionalize.
- Understanding that increases in sales velocity increase inventory velocity, which, in turn, increases production or service velocity, finance velocity, human capital velocity, and systems velocity. The goal is to synchronize these velocities in a cohesive manner.
- Implementing the goal congruence concept by linking individual employee goals with those of the department/division and the organization. He must remove or reduce the competing or conflicting goals.
- Implementing crosscutting best practices across business units, divisions, departments, functions, and countries through busting silos and building bridges
- Linking employee rewards, bonuses, and promotions to employees' true performance and tangible results, and empower employees
- Building solid working relationships with C-level executives in manufacturing, marketing, finance, human resources, IT, and other functions through formal and informal approaches at the workplace
- Encouraging employees to continuously acquire and improve their knowledge, skills, and abilities (KSAs) through targeted training courses, management development programs, and professional certifications
- Establishing a solid and sustainable chain of knowledge linked through the entire management hierarchy to ensure adequate core knowledge competencies for all levels of employees in the organization
- Inviting global audits, special management reviews, and self-assessments periodically and proactively to ensure continuous improvement in international business
- Encouraging employees at all levels of the organization to think differently and radically (i.e., out-of-the-box thinking) at all times, which can lead to new perspectives providing best-of-breed solutions
- Participating in the succession-planning process for key positions
- Analyzing outside-in views (i.e., views of stakeholders about company management) and inside-out views (i.e., views of company management about stakeholders) to identify disconnections between these views and to integrate them in a coherent manner

12.3 INTERNATIONAL TRADE MANAGEMENT

(a) OVERVIEW. International trade has become an increasingly critical part of the U.S. economy. Exports account for more than 10% of the U.S. gross domestic product (GDP) and are an important source of job creation. Nevertheless, and despite the country's rising exports, many experts believe that the United States is losing ground in the new global competition.[1]

The U.S. economy has become increasingly intertwined with those of other nations in a new international marketplace; many of these nations have gained considerable economic power. As a result, the United States must better balance its domestic economic goals and policies with the constraints imposed by the realities of the interdependent global economy.

(b) MAJOR ISSUES IN INTERNATIONAL TRADE. There are several major issues confronting the international business manager or executive. Understanding these issues will facilitate a better appreciation of the problems to be encountered so appropriate solutions can be developed in advance. The issues include (1) U.S. trade deficits and competitiveness; (2) promoting U.S. exports; (3) combating unfair foreign trade practices; (4) protection of intellectual property rights; (5) foreign industrial targeting, dumping, and export subsidies; (6) international finance; (7) trade in telecommunications services and equipment; and (8) globalizing the U.S. supplier base.

(i) Issue 1: U.S. Trade Deficits and Competitiveness. A major priority for the United States is the need to address the macroeconomic imbalances resulting from the very large federal budget deficits. These trade deficits, and the borrowing to finance the U.S. budget deficit, have made the United States the world's largest debtor nation. There is a need to develop and implement a comprehensive, government-wide strategy tackling management problems in the country's export promotion programs, which are spread among several agencies. As international competition sharpens and foreign firms show interest in acquiring high-technology firms and other national security–related firms, continued attention needs to be paid to the way foreign investments in U.S. industries affect this nation's defense capabilities and competitive position.

The new economic environment will require a careful examination of how government programs and policies affect the competitive position of the U.S. economy. For example, at the macroeconomic level, the U.S. government will need to adopt policies that support private-sector investment by keeping the cost of capital at reasonable levels. At the government program level, it must develop efforts that support rising productivity in the private sector, such as an improved infrastructure and a better-educated and -trained labor force. Finally, it must encourage private-sector firms to improve their own goals, policies, and management systems as their critical contribution to enhancing U.S. competitiveness. Such a comprehensive effort is needed to help ensure that citizens of the United States enjoy a rising standard of living as their country continues to sell its goods and services on world markets.

(ii) Issue 2: Promoting U.S. Exports. The U.S. government spends significant amounts on export promotion programs, export loans, credit guarantees, and insurance. The export

promotion programs are spread over many different agencies, causing duplication and confusion, and funds are not allocated on the basis of any specific government-wide strategy. Consequently, the federal government does not have any reasonable assurance that its export promotion funds are being channeled into areas with the greatest potential returns. A government-wide strategy or set of priorities is needed to apportion export promotion funds.

(iii) Issue 3: Combating Unfair Foreign Trade Practices. Section 301 of the U.S. Trade Act of 1974 is the primary provision in U.S. trade law authorizing the U.S. government to act against unfair trade practices that restrict U.S. export access to foreign markets. Furthermore, Section 301 creates a unique relationship between U.S. and international trade law by allowing private parties to enlist the aid of the U.S. government when combating an unfair foreign trade practice through the World Trade Organization (WTO) dispute settlement mechanism. Concerns have grown that the Section 301 process is too lengthy, too uncertain, and too seldom used. Complaints have arisen that the "political will" to force the resolution of trade disputes has been lacking.[2]

(iv) Issue 4: Protection of Intellectual Property Rights. Protection of intellectual property (IP) rights (i.e., patents, trademarks, and copyrights) from foreign infringement has emerged as one of the most important trade issues. Foreign firms, often operating in counties that provide no or inadequate legal protection for IP rights, mass-produce protected goods for distribution in the United States and elsewhere. This activity reportedly costs U.S. business millions of dollars annually and certainly undermines the United States. IP rights protection system. The U.S. government needs to strengthen its ability to stop counterfeit and infringing goods from entering the country. Section 337 of the Tariff Act of 1930 provides relief to the affected U.S. firms from foreign infringement; however, these firms must first obtain exclusion orders from the International Trade Commission (ITC) through yearlong proceedings. The Section 337 process is too cumbersome, complicated, time-consuming, and ineffective, which hurts U.S firms needing protection.

(v) Issue 5: Foreign Industrial Targeting, Dumping, and Export Subsidies. Industrial targeting involves coordinated government assistance to a domestic industry with the goal of increasing exports of a country's products. The assistance may include explicit export subsidies, research and development subsidies, or relaxed regulatory or tax rules for export industries. There is a concern (1) that other nations, seeing the size and potential markets of the U.S. economy, have consciously targeted U.S. markets for increased exports and have conducted policy with this goal in mind, and (2) that current U.S. trade laws are not adequate to prevent the ensuing damage to U.S. industries. The problem is compounded by delays between government action and actual market impact, which may take several years. What is needed is an automatic response to foreign industrial targeting under U.S. trade law provisions, such as Section 301 of the Trade Act of 1974.

Other concerns include the effectiveness of the countervailing duty and anti-dumping laws in preventing or remedying the effects of foreign subsidies or dumping practices. The U.S. countervailing duty and antidumping laws are designed only to

offset the injury of the unfair foreign subsidy or dumping practice, not to insulate the petitioning industry from foreign competition.

(vi) Issue 6: International Finance. The long-lasting period of the strong U.S. dollar, its rapid depreciation, and large daily fluctuations in exchange rates have raised concerns that the current international monetary system based on floating exchange rates is ill-suited to the job of facilitating international trade. The concern about exchange rates and their behavior joins other persistent problems of international finance, such as high levels of debt owed by developing nations and the implications facing U.S. and other developed-nation banks that hold the debt. Predicting exchange rate behavior is difficult because the exchange rate is the price of a financial asset, much like the price of a stock or bond, and asset prices have always proven all but unpredictable. The system of floating exchange rates has not performed as well as was hoped at its onset, but there is no simple solution that will address all of the problems of the international monetary system. Exchange rate movements and many other problems are actually attributable to the greater integration of national economies rather than to the exchange rate system. Even if it were possible to fix exchange rates, divergent national economic policies would have to be accommodated in some manner.

(vii) Issue 7: Trade in Telecommunications Services and Equipment. As part of the information industry, telecommunications trade is assuming an increased importance. The telecommunications industry is one in which governments have long exerted significant influence, ranging from regulatory control to outright state ownership. There are relatively few restrictions on foreign firms selling telecommunications equipment and services in the United States. Many nations retain "buy-national" rules for their state-owned or controlled industries, with telecommunications being one such industry. The U.S. government is discussing with foreign nations limiting market access and to push for greater market access, including reciprocal treatment. If other nations do not open their markets to U.S. firms, the United States should deny firms from those nations full access to the U.S. market.

(viii) Issue 8: Globalizing the U.S. Supplier Base. The U.S. government has not struck an appropriate balance between the globalizing U.S. supplier base and protection of U.S.-based companies and technologies. Complaints against the U.S. government include (1) its supplier policy is fragmented, confusing, and often takes a default position, (2) it has not clearly identified industries and technologies to protect, (3) it has not determined the effectiveness of existing protectionist legislation in maintaining the industrial base, (4) it overly restricts technology transfers to allies and discourages global suppliers from participating in the U.S. supplier base, (5) it does not distinguish between purchasing goods and purchasing services, and (6) it does not provide clear requirements to suppliers and does not maintain competition in the supplier base.

The U.S. government has a responsibility to define a supplier management policy that provides suppliers with a roadmap for future needs. As regulator, buyer, and financier for suppliers, the U.S. government needs to set out a framework for supply chain management. It should formulate innovative ways to expand the supplier base rather than focusing on restricting manufacturing industry profits.

(c) U.S. EXPORT PROMOTION PROGRAMS. International trade can permit a higher U.S. standard of living if the country (1) makes and exports those goods and services that it can produce with relative efficiency, and (2) imports those goods and services that it can produced only with relative inefficiency. Supporters of export promotion programs view increased exports as a way to enhance the benefits gained from international trade and, thereby, further improve the economic well-being of the U.S. public. Opponents of such programs view them as an unnecessary interference in the workings of the market.[3]

There are several arguments for and against the U.S. government's export promotion programs, all of which rely heavily on economic analysis. The conceptual bases include macroeconomic considerations, microeconomic considerations, and trade policy objectives.

(i) Macroeconomic Considerations. Some supporters of export promotion programs point to jobs created by exports as an important reason for such government backing. Similarly, others have supported export promotion programs as a way to reduce the U.S. trade deficit. However, these programs cannot produce a substantial change in the U.S. trade balance, nor can they produce a substantial change in employment levels. The levels of these variables are largely determined by the underlying competitiveness of the U.S. economy and by the macroeconomic policies of the United States and its trading partners.

WHAT ARE MACRO- AND MICROECONOMIC CONSIDERATIONS?

- Macroeconomic considerations look at the impact on jobs and the trade deficit.
- Microeconomic considerations look at the extent to which the U.S. government enhances or detracts from the efficiency of markets.

(ii) Microeconomic Considerations. Economists, as a general proposition, oppose government intervention in private markets because markets typically produce more efficient outcomes. Government intervention tends to distort resource allocation and create inefficiencies. However, for markets to be able to achieve the anticipated level of economic efficiency, key conditions need to be met. For example, all costs and benefits are to be "internalized" to firms and consumers, market participants are to have perfect information regarding all market variables and the future, and no market participants may hold monopoly power. When such key conditions are not satisfied, the outcome that the market generates may not be the most efficient. It is under such circumstances, referred to as "market failures," that the economics literature discusses how government intervention can improve economic efficiency.

Arguments both for and against export promotion programs can be tied to the concept of market failure. Supporters of government assistance for exporters hold that real world deviations from the conditions necessary to make markets work efficiently provide a strong justification for such programs. Correction of these market failures can improve economic efficiency and overall economic well-being. On the other hand, opponents of government assistance hold that the government cannot do better than the market and that government intervention can even make a bad situation worse.

Technological spillover is an example of a market failure that could be used to argue for government assistance to increase exports. Proponents argue that such government intervention would help the U.S. maximize the benefits from technological innovation, such as increasing the number of high-wage jobs and increasing the financial returns to innovation. Opponents argue that this type of assistance involves the government's being able to pick winning companies, which is not an easy task. Furthermore, in today's integrated world market, it is not possible for one country to secure all the gains from a technological innovation.

(iii) Trade Policy Objectives. Other reasons offered in support of export promotion programs relate to the use of trade promotion to achieve broader trade policy objectives. Trade policy objectives include helping U.S. firms overcome foreign trade barriers, leveling the playing field for U.S. companies competing against foreign companies that receive government support, and countering foreign subsidies as a trade policy strategy so that foreign governments will negotiate to reduce and eliminate such subsidies.

Several different rationales may provide the justification for a specific example of government support for exporting. There are at least four types of export promotion activities: subsidizing export prices, providing foreign market information, advocating for U.S. businesses, and assisting with export finance.

12.4 INTELLECTUAL PROPERTY MANAGEMENT

(a) OVERVIEW. The scope of intellectual property (IP) includes trademarks, copyrights, patents, common law (i.e., unregistered) trademarks, trade secrets, mask works (i.e., the pattern on the surface of a semiconductor chip), and others.

Trademarks protect words, names, symbols, devices, or a combination thereof, used by a manufacturer or merchant to identify its goods and distinguish them from others.

Copyrights protect literary and artistic expression, granting a given author, composer, playwright, publisher, or distributor the exclusive right to publish, produce, sell, or distribute a literary, musical, dramatic, or artistic work.

Patents, which protect functional and design inventions, give inventors the right to exclude others from making, using, or selling their inventions.

Trademarks can be registered with the U.S. Patent and Trademark Office of the Department of Commerce. Copyrights can be registered with the U.S. Copyright Office of the Library of Congress. Unregistered claims to copyrights in works are entitled to protection under the Universal Copyright Convention if the claims have been recorded with the U.S. Customs. Regardless of registration, trademarks can be counterfeited and infringed and copyrights and patents can be infringed.

Trademark counterfeiting generally involves the deliberate, unauthorized duplication of another's trademark or packaging. Trademark infringement generally involves the unauthorized use of a trademark that is so similar to another existing trademark that, considering the products involved, consumers are likely to become confused.

Copyright infringement generally involves the unauthorized use or copying of a copyrighted work.

Patent infringement generally involves the unauthorized manufacture, use, or sale in the United States of any device that embodies a patented invention, whether copied from an authorized device or resulting from independent development.

(b) SURVEY OF U.S. FIRMS' VIEW ON U.S. CUSTOMS' PROTECTION OF INTELLECTUAL PROPERTY RIGHTS. U.S. firms responding to General Accounting Office (GAO) surveys reported that trademark-counterfeit goods and copyright-infringing goods continued to enter the country, often in large quantities, after these firms had obtained U.S. Customs Service assistance in protecting their IP rights (e.g., patents, trademarks, and copyrights). The surveyed firms indicated that Customs' efforts were limited foremost by the availability of staff, and they reported that the counterfeit and infringing imports continued to cause lost sales and loss of consumer confidence in the legitimate products. Survey respondents supported several proposals to enhance the ability of the Customs Service's staff to protect IP rights, despite staff shortage.[4]

There are two methods for obtaining U.S. Customs Service assistance in protecting IP rights.

1. *Recordation:* Owners of trademarks and copyrights that have previously been registered with the federal government can record such property rights with the Customs Service. Upon receipt of the fee, certain information on the IP rights, and proof of registration, Customs prints notices containing the needed information and mails them to the ports. In protecting trademarks and copyrights, Customs can exclude shipment of counterfeit or infringing goods from the country and, in certain instances, can seize such shipments, which may be forfeited to the government.
2. *Section 337 of the Tariff Act of 1930 Exclusion Orders:* Owners of other types of IP rights, most notably patents, must first obtain exclusion orders from the U.S. International Trade Commission (ITC). To obtain such an order, the owner must participate in a long adversarial proceeding in which it must demonstrate that a valid and enforceable IP right has been infringed by imports. Should the ITC find in favor of the firm bringing the complaint, it can instruct the Customs Service to exclude counterfeit and/or infringing goods from entering the country. An exclusion order from ITC gives Customs the authority to exclude, but not to seize, shipments of goods that counterfeit or infringe the IP rights covered by the ITC orders.

(c) INTERNATIONAL PERSPECTIVES ON INTELLECTUAL PROPERTY. Rights in property can be rendered useless if law cannot protect such rights. Most developed countries, such as the United States, Canada, Japan, and the nations of Western Europe, have laws that protect the owners of IP, and they enforce those laws. However, copyrights, patents, and trademarks are widely pirated in the developing countries of Asia, Latin America, Africa, Russia, Eastern Europe, and the Middle East, whose protection laws are either nonexistent or not enforced at all.

In this section, we present a brief discussion of the U.S. trade-secret laws, patents, and copyrights, as they relate to computer software and hardware, followed by views of the international scene from the standpoints of the Pacific Rim, Western Europe, and Latin America.[5]

(i) U.S. Trade-Secret Law. Trade-secret law protects certain types of confidential technical or business information against unauthorized use or disclosure. In order to qualify as a trade secret, information must possess certain characteristics. First, information that

is the subject of trade-secret protection must be of some minimal competitive value or advantage to the owner or his business. Trade secrets can include technical information, customer lists, suppliers, or accumulated business wisdom. The information must also be the result of some minimal investment or expense and must not be generally known to the public. Courts also consider the amount of effort invested in creating a program when determining whether a trade secret exists. Finally, the trade-secret owner must affirmatively maintain the secret. In summary, the basic elements of a trade secret are value, secrecy, and use.

Trade-secret law is one of the most widely used forms of legal protection for IP interests in computer software. Numerous courts in a variety of U.S. jurisdictions have ruled that trade-secret law properly protects computer software.

Developers of computer software have attempted to address the more difficult problem of maintaining trade secrecy in the face of mass-marketed software, extensive distribution of which might otherwise destroy requisite secrecy, by use of what is known as a "shrink-wrap" license. Theoretically, such a license is used in conjunction with the practice of publishing program code in object code form. Object code is understandable to people only after extensive effort and ordinarily requires intermediate steps to recover a higher-level language representation of the program. Distributing the code in such a form is intended to maintain the secret nature of the information. In addition, it invokes the provisions of the copyright law, since recovering a high-level language version may involve the making of a copy or derivative work of the object code program. The making of such a copy or derivative work is a violation of the copyright law.

The shrink-wrap license further signals secrecy and is established by marketing software in a sealed package with a notice and a license agreement visible on the package's exterior. The agreement generally provides that the user, by opening the package, is deemed to have accepted the license terms and conditions. The terms of such a license generally prohibit decompilation, disassembly, or copying of a program for any reason except for use and backup purposes. Some shrink-wrap agreements contain an express prohibition on "reverse engineering," decompilation, or disassembly.

(ii) U.S. Patents. Patents grant inventors a limited property right to exclude others from practicing (i.e., making, using, or selling) the claimed invention for 17 years. A patent should have characteristics such as novelty, utility, and nonobviousness. The inventor must make an application for a patent. It must be in writing and contain a specification and, where necessary, a drawing. The application must include claims and an oath or declaration that the inventor believes himself to be the original and first inventor of that for which the protection is sought.

Some courts asserted that a general-purpose digital computer programmed with a claimed process becomes a special-purpose digital computer and could qualify as a patentable invention, assuming the requirements of novelty, utility, and nonobviousness are met.

(iii) U.S. Copyrights. Copyright law in the United States protects the right of an author to control the reproduction, adaptation, public distribution, public display, and public performance of original works of authorship. Copyright protection is expressly provided for eight categories of works: literary; musical; dramatic; pantomime and choreographic; pictorial, graphic, and sculptural; audiovisual (including film and television);

sound recording; and architectural. Computer programs are copyrightable as "literary works." Source code, microcode, and object code, whether the code is an operating system or an application program, are copyrightable. The copyright protection of computer programs may extend beyond a program's literal code to its structure, sequence, and organization. Databases are protected under copyright law as compilations.

SOFTWARE COPYRIGHTS

- The user interface is viewed as part of the ''structure, sequence, and organization'' of the underlying program.
- The screen displays are considered a separate work from the program code.
- Command languages, menu-based dialogs, graphical user interfaces, and newer interactive techniques such as icons have expanded the design choices available for user interface design.

Copyright does not protect ideas but rather the expression of ideas. Copyright protection does not extend to any procedure, process, system, method of operations, concept, principle, or discovery, regardless of the form in which it is described, explained, illustrated, or embodied. Copyright protects the writing of an author against unauthorized copying and distribution, but it protects the form of expression rather than the subject matter of the writing. Unlike patents, it does not protect against independent creation.

Owners of copyrighted software are awarded exclusive rights to their works for varying periods, but typically with a 75-year maximum. Procedurally, copyright is an automatic protection, conferred as soon as an expression is fixed in a tangible medium, even if the work is never published. Registration with the Copyright Office is not required, nor is full disclosure necessary. To secure a registered copyright, the creator of a program need only submit materials describing the first and last 25 written pages of the work.

Copyright grants the owner the exclusive right to do and to authorize others to do the following:

- Reproduce copies of the copyrighted work.
- Prepare derivative works based on the copyrighted work.
- Distribute copies of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending.
- Perform the copyrighted work publicly.
- Display the copyrighted work publicly.

A single and effective control procedure to detect illegal use of copyrighted software is to develop a software-inventory management system and periodically compare the software inventory list to company purchase orders.

(iv) International Perspectives. In this section, focus is on the computer software and hardware from patent, copyright, and trade secret viewpoints. The international nature of the software industry and market is mirrored in the global significance of national intellectual property laws and international treaties and agreements. This globalization of the law reflects the reality that the laws of a country are affected by, and in turn affect, the laws of other countries. There is an increased tendency for countries to make at least

somewhat similar policy choices. The following is a presentation of comparisons of laws in major foreign countries.

(A) Pacific Rim

Patent law. Patent laws of Japan, Taiwan, South Korea, and Thailand are all silent on the issue of patentability of computer programs. In theory, patent law does not provide protection for a computer program itself. However, Japan and Taiwan have granted patents for certain computer programs, especially if the computer program is described in conjunction with a method or computer in which the program is used in the specification of an application.

Copyright law. Under Japanese law, both source code and object code are copyrightable. Translation from source code to object code constitutes a reproduction of the source code. Japanese copyright law further provides that the author shall have the exclusive right to reproduce, translate, arrange, transform, dramatize, cinematize, or adapt his work. The period of protection for computer software in Japan is the life of the creator plus 50 years. For unpublished software, the copyright endures 50 years after the creation of the work.

The scope of protection afforded software by South Korean law is similar to that granted to software in Japan. The term of protection for software in South Korea is 50 years from the time at which the program is created. In Taiwan, the copyright law covers software. Taiwanese copyright law provides protection for the life of the author plus 30 years. If an employee creates the work, 30 years of protection are provided.

Trade-secret law. Japan is the only Pacific Rim nation whose law provides for trade-secret protection. Under the law, if a computer program properly qualifies as a trade secret, the computer program owner who is damaged or is likely to suffer damage by unauthorized use or disclosure of his program may require the offending party to stop the unauthorized use or disclosure of the program. The trade secret owner may request that the media on where the program is stored be destroyed.

South Korea has committed itself to the future adoption of a trade-secret law. There is no specific law protecting trade secrets in Taiwan. Thailand has no specific law covering, nor a clear definition of, trade secrets.

(B) Western Europe

Patent law. The European Community has agreed in its Software Directive that the prescribed protection of computer programs under copyright law does not prejudice the application of other forms of protection where appropriate. Computer software may be protected under patent law in addition to copyright in European Community member nations.

French patent law provides that computer programs are not patentable. The patent protects the process but not the software; the software can be used independently or in another process. Hardware may be patented. Swiss patent law does not provide patent protection for computer software.

Copyright law. The European Community follows the directive requiring software is protected by copyright as a literary work within the meaning of the Berne Convention. The French term of protection under copyright is 25 years from the creation date of the software. In Switzerland, protection extends for the life of the author plus 50 years.

Trade secret law. Computer software is properly protected by trade-secret and copyright laws in European Community member nations.

(C) Latin America

Patent law. In Argentina, software was not known or considered when the patent law was enacted, so it is not specifically mentioned in the law. The Patent Office may allow patent protection when it is part of the essence of an invention.

Under Brazilian law, while hardware is subject to patent protection, software is not considered patentable and is expressly excluded from patentable subject matter by the Industrial Property Code.

Copyright law. Mexican law now includes computer programs as a category of protected works under the copyright law. Mexican law includes no private use or "fair use" type of limitation. In Brazil, software programs are not included in an enumerated list of creations subject to protection. Argentine law protects all traditional forms of creative expression. Source code programs may have copyright protection. Draft laws grant protection to both source code and object code programs, as well as to the operating systems software and application programs.

Trade secret law. Brazil has no specific law for trade-secret protection. There is no Argentine law directed specifically toward protection of trade secrets. Mexican law generally protects industrial secrets. No specific provisions are made for trade secrets in computer software.

12.5 INTERNATIONAL LICENSING AND FRANCHISING MANAGEMENT

(a) OVERVIEW. As valuable assets, IP can be sold or licensed for use to others through a licensing agreement. International licensing agreements are contracts by which the holder of IP will grant certain rights in that property to a foreign firm under specified conditions and for a specified time. Licensing agreements represent an important foreign-market entry method for firms with marketable IP. For example, a firm might license the right to manufacture and distribute a certain type of computer chip or the right to use a trademark on apparel such as blue jeans or designer clothing. It might license the right to distribute movies or to reproduce and market word-processing software in a foreign market, or it might license its patent rights to produce and sell a high-tech product or pharmaceutical drug. U.S. firms have extensively licensed their property around the world, and in recent years have purchased the technology rights of Japanese and other foreign firms.[6]

Problems with U.S. Exports

Many exporters view U.S. export-licensing requirements as stricter than those of other countries and as increasingly less effective because of the growing availability of comparable products from newly industrializing countries.

U.S. exporters are particularly concerned over the large volume of exports that require licenses, the complexity of the regulations and the time required, licensing requirements for reexport of U.S.-source parts and components, and foreign availability of goods and technologies subject to U.S. export controls. They fear that sales may be lost and the incentive for U.S. companies to develop new products and technology lessened.

(b) NEED FOR INTERNATIONAL LICENSING. A firm may choose licensing as its market entry method to the foreign market than is possible through exporting. A firm may realize many advantages in having a foreign company produce and sell products based on its IP instead of simply shipping finished goods to that market. When exporting to a foreign market, the firm must overcome obstacles such as long-distance shipping and the resulting delay in filling orders. Exporting requires a familiarity with the local culture. Redesign of products or technology for the foreign market may be necessary. Importantly, an exporter may have to overcome trade restrictions, such as quotas or tariffs, set by the foreign government. Licensing to a foreign firm allows the licensor to circumvent trade restrictions by having the products produced locally, and it allows entrance to the foreign market with minimal initial start-up costs. In return, the licensor might choose to receive a guaranteed return based on a percentage of gross revenues. This arrangement ensures payments to the licensor whether or not the licensee earns a profit. Even though licensing agreements give the licensor some control over how the licensee utilizes its IP, problems can arise. For instance, the licensor may find that it cannot police the licensee's manufacturing or quality control process. Protecting itself from the unauthorized use or "piracy" of its copyrights, patents, or trademarks by unscrupulous persons not party to the licensing agreement is also a serious concern for the licensor.

(c) NEED FOR TECHNOLOGY TRANSFER. The exchange of technology and manufacturing know-how between firms in different countries through arrangements such as licensing agreements is known as technology transfer. Transfers of technology and know-how are regulated by government control in some countries. This control is common when the licensor is from a highly industrialized country, such as the United States, and the licensee is located in a developing country, such as those in Latin America, the Middle East, or Asia. In their efforts to industrialize, modernize, and develop a self-sufficiency in technology and production methods, these countries often restrict the terms of licensing agreements in a manner benefiting their own country. For instance, government regulation might require that the licensor introduce its most modern technology to the developing countries or train workers in its use.

Foreign ownership of U.S. assets is a concern to many U.S. experts as it could affect the nation's defense capabilities and security. Transferring U.S. technology to other countries through foreign purchases of and joint ventures with U.S. firms raises a number of potential issues, such as increased foreign political influence and effects on domestic employment.

(d) NEED FOR INTERNATIONAL FRANCHISING. Franchising is a form of licensing that is gaining in popularity worldwide. The most common form of franchising is known as a business operations franchise, which is most often used in retailing. Under a typical franchising agreement, the franchisee is allowed to use a trade name or trademark in

offering goods or services to the public in return for a royalty based on a percentage of sales or other fee structure. The franchisee will usually obtain the franchiser's know-how in operating and managing a profitable business and its other "secrets of success" (ranging from a "secret recipe" to store design to accounting methods). Franchising accounts for a large proportion of total retail sales in the United States. In foreign markets as well, franchising has proven successful in fast-food retailing, hotels, video rentals, convenience stores, photocopying services, and real estate services, to name but a few. U.S. firms have excelled in franchising overseas, making up the majority of new franchise operations worldwide.

Franchising is a good vehicle for entering a foreign market because the local franchisee provides capital investment, entrepreneurial commitment, and on-site management to deal with local customs and labor problems. However, many legal requirements affect franchising. In the United States, the Federal Trade Commission (FTC) regulates the franchise business. The FTC requires the filing of extensive disclosure statements to protect prospective investors. Other countries have also enacted new franchise disclosure laws. Some developing countries have restrictions on the amount of money that can be removed from the country by the franchiser, some require government approval for franchise operations, and some restrict imports of supplies. But now more and more developing countries are relaxing restrictions in order to invite franchise business into their countries.

(e) NEED FOR AUDITING LICENSE AND FRANCHISE AGREEMENTS. Mutual trust and ongoing communications can help in establishing long-term working relationships between licensor and licensee, between franchisor and franchisee, and between other business partners. Auditing or reviewing of licensing agreements and royalty calculations is a good business practice that can protect both parties' rights. A person independent of the parties involved in a licensing or franchising agreement should conduct the auditing work to eliminate conflict-of-interest situations.

The auditor who is reviewing the international licensing and franchising agreement should do the following:

- Understand the business purpose of the international license or franchise arrangement. Become familiar with the business partners and their backgrounds and business methods.
- Review the agreement for confidentiality and nondisclosure requirements.
- Review the agreement for exclusivity or nonexclusivity of the rights granted, including their assignment.
- Understand the schedules for submission of operating and technical reports by the licensee to the licensor or by the franchisee to the franchisor. Review a sample of such reports and understand how and what interest rate is attached to late payments, the basis for currency conversion, and the royalty payment methods.
- Review the agreement for such clauses as the right to audit for royalties, the right to inspect financial and technical records, and the right to inspect the physical production facilities of the licensee or the franchisee. Determine how long the financial and technical records must be maintained by the licensee or the franchisee.

- Understand the basis for calculating the royalty payments or remuneration (i.e., one-time flat fee, or staggered flat fees, or a fixed percentage of net sales). Take a sample of such payments and retrace the calculations for correctness and completeness. Determine whether business deductions taken by the licensee or the franchisee during royalty calculations are in line with the agreement.
- Determine whether the agreement has a provision that gives the licensor or the franchisor the right to terminate the contract in case the licensee or the franchisee is involved in fraudulent activities.

12.6 INTERNATIONAL RISK MANAGEMENT

(a) OVERVIEW. International risks are many because of the complexities involved in dealing with several nations' economic, political, and cultural systems. Yet many companies choose to do business in risky markets because of the risk-versus-return tradeoff. With appropriate rewards (returns), many risks become more tolerable.

Usually, international risks stem from a host government's laws and regulations. Adverse governmental actions are the result of nationalism, the deterioration of political relations between home and host country, and the desire for independence. If a host country's citizens feel exploited by foreign investors, the host government officials are more likely to take antiforeign action. Major international risks such as political risks, economic risks, and lending risks are discussed next.[7]

(b) POLITICAL RISKS. The politics and laws of a host country affect international business operations in a variety of ways. Organizations usually prefer to conduct business in a country with a stable and friendly government, but such governments are not always easy to find. International business managers and executives must constantly monitor a given government, its policies, and its stability to determine the potential for political change that could adversely affect corporate business operations.

Political risks can be divided into transfer risks, operating risk, and ownership risks. Examples of transfer risks include tariffs on exports and imports, restrictions on exports, dividend remittance, and capital repatriation. Examples of operating risk include price controls, financing restrictions, export commitments, taxes, and local-sourcing and local-content requirements. Examples of ownership risks include pressure for local participation, confiscation, expropriation, domestication, and abrogation of property rights.

Foreign organizations should do the following to reduce political risks in a local (host) country:

- Increase hiring and training of local employees.
- Provide better pay to local employees.
- Give contributions to local charities.
- Make investments useful to local society.
- Form joint ventures with local partners to demonstrate that the company is willing to share its gains with local nationals.
- Closely monitor political developments in the host country to discover trouble spots as early as possible and to react quickly to prevent major losses.

(c) ECONOMIC RISKS. A host government's political situation or desires may lead it to impose economic regulations or laws to restrict or control the international activities of firms. Examples of economic risks include controls on the movement of capital into and out of the country, exchange controls against certain products or companies, tax policy to control foreign investors, and price controls on imported products or services.

Foreign organizations should do the following to reduce both political and economic risks in a local (host) country:

- Obtain currency inconvertibility insurance, which covers the ability to convert profits, debt service, and other remittances from local currency to the home country's currency.
- Obtain expropriation insurance, which covers the loss of an investment due to expropriation, nationalization, or confiscation by a foreign government.
- Obtain political violence insurance, which covers the loss of assets or income due to war, revolution, insurrection, or politically motivated civil strife, terrorism, or sabotage.

(d) LENDING RISKS. The level of international lending by U.S. banks has created a two-sided problem. On the one hand, a high level of lending is needed to support international economic growth and to expand U.S. exports. On the other hand, increased foreign lending has intensified the U.S. banking system's exposure to country risk—the possibility that adverse economic, social, or political circumstances may prevent a country's borrowers from making timely repayment of the interest or principal of a loan.[8]

For major U.S. banks, foreign assets account for one-third or more of total assets. As part of the broader examination process, the U.S. bank regulatory agencies have adopted uniform examination procedures for evaluating and commenting on country risk to U.S. banks with relatively large foreign lending. The country-risk examination system is advisory. Its overall objective is to help bring about adequate diversification of bank exposures (international loans) among countries. Diversification is viewed as the primary means of moderating country risk in a bank's portfolio of international loans.

International lending risk is of three types: credit risk, country risk, and currency risk. Credit risk is financial and centers on the probability that part or all of the interest or principal of a loan will not be repaid. The larger the potential for default on a loan, the higher the interest rates that the bank must charge the borrower. Country risk is political and centers on political developments in a country, especially the government's views concerning international investments and loans. Currency risk is economic and centers on exchange controls and currency depreciation and appreciation. For example, exchange controls restrict the movement of funds across national borders or limit a currency's convertibility into dollars for repayment, thus adding to the risk of international lenders.

12.7 MANAGING OFFSHORE BUSINESS ACTIVITIES

(a) OVERVIEW. Although offshoring has existed for decades in the manufacturing sector, recently concerns have been raised about the emergence of services offshoring. Offshoring is the practice, by either U.S. companies or government entities, of replacing goods or services previously produced domestically with goods or services produced abroad. A company may offshore services either by purchasing services from a company

based overseas or by obtaining services in-house through an affiliate located overseas. For example, a U.S.-based company might stop producing parts of its accounting and payroll services in-house and instead outsource them to a foreign-based company. A U.S.-based multinational company might offshore by moving parts of its accounting and payroll services from its domestic operations to its foreign affiliate, thus keeping the services in-house. Relocating services to foreign affiliates and importing services that had previously been acquired domestically can both result in the displacement of U.S. service production and employment, with ripple effects on productivity and consumer prices likely to follow.[9]

However, other business activities that do not directly result in the displacement of U.S. workers are sometimes included in a broader definition of offshoring. This definition could include other business activities that might result in forgone job creation domestically but would not result in job losses. For example, a U.S.-based company might expand its accounting and payroll services through a foreign company or affiliate, but do so without affecting its U.S. workforce.

Broader definitions of offshoring sometimes include the movement of production offshore. This definition of offshoring focuses on U.S. companies' investing in overseas affiliates. Offshoring defined in this way would not necessarily result in the displacement of U.S. service production or employment. For example, a U.S.-based company investing in an overseas affiliate in order to produce accounting and payroll services to sell to other companies abroad might do so without affecting its production and employment levels in the United States.

(b) ENABLING FACTORS AND INCENTIVES FOR OFFSHORING. Firms have been offshoring manufacturing since long before the recent trend in services offshoring. In previous decades, U.S. manufacturing companies were motivated to offshore because of the low costs and the availability of skilled labor, production and supply networks in some developing countries, and because of reductions in the cost of transporting goods. At the same time, U.S. companies divided their production processes into discrete pieces, which allowed them to offshore some of the components. As a result, some businesses offshored total production and others offshored parts of the production process. Firms generally retained higher-end, higher-skilled service functions in the United States, such as management, finance, marketing, and research and development.

Offshoring has recently expanded into services due to three key factors. First, technological advances, such as advances in telecommunications and the emergence of the Internet, have enabled workers in different locations in the world to communicate and be connected electronically and have also facilitated the digitization and standardization of activities needed to complete business processes. These changes in turn have allowed business processes to be divided into smaller components, some of which can be done in different locations. For example, standardized software has made it possible for firms to offshore financial or human resources activities to separate overseas companies that handle such functions for a variety of clients. Thus, in many cases, the offshoring of services constitutes an outgrowth of outsourcing business functions. Second, countries such as India, China, Russia, and much of Eastern Europe have increasingly opened their borders to the global economy. Third, other countries have highly educated populations with the technical skills for performing services and technology-related work.

According to several business studies, a primary reason that organizations engage in offshoring is to reduce costs. The cost savings from offshoring are primarily the result of differences between the United States and developing counties in the unit cost of labor—the worker compensation (wages and benefits) that must be paid to produce one unit of goods or services. Unit labor costs are lower for certain services in developing countries primarily because workers' wages in those countries are lower than in the United States. However, unit labor costs also depend upon the productivity levels of workers. The U.S. worker can produce many more or higher-quality products within a certain time frame than a worker in the country the United States is being compared with. Differences in unit labor costs can also result from differences in costs of employee benefits, such as health care and pension benefits. In addition, cost savings can be affected by currency exchange rates, countries' tax policies, and government-provided incentives such as tax rebates.

Aside from cost savings, firms may have other incentives to offshore. Access to a workforce in different time zones across the globe may enable companies to conduct work around the clock and consequently meet worldwide customer needs. Establishing a presence in foreign countries can provide companies access to overseas markets. In addition, offshoring noncore services can enable companies to focus their resources on their core functions. By outsourcing noncore functions to overseas firms that specialize in them, businesses may also experience improvements in the quality of these functions.

Although firms may have many incentives to offshore, they may also face disincentives. Offshoring has several costs associated with it, including costs to start up an offshore operation and to manage and train an offshore workforce. In addition, some experts have noted that wages of workers in developing countries are rising more rapidly than U.S. wages, thereby shrinking the cost savings of offshoring over time. Furthermore, offshoring carries potential risks, such as possible political instability in overseas locations, less reliable civil infrastructure, currency exchange-rate volatility, less developed legal and regulatory systems, and risks to intellectual property rights.

(c) TYPES OF SERVICES ASSOCIATED WITH OFFSHORING. Types of services associated with offshoring tend to be those that are capable of being performed at a distance and whose product can be delivered through relatively new forms of advanced telecommunications. Examples of these business functions include software design and programming, call center operations, accounting and payroll operations, medical records transcription, paralegal services, statistical analysis, stock market research reports, client/vendor proposal presentations, and software research and testing.

(d) MAJOR ISSUES OF OFFSHORING. While traditional economic theory predicts that offshoring is likely to benefit the overall economy, concerns have been raised about four areas of potential impact: the average U.S. standard of living, employment and job loss, income distribution, and national security. Observers of offshoring have expressed a range of views about the likely impact of offshoring on each of these areas.

Major Issues of Offshoring

Services offshoring raises issues involving a wide array of topics, including the economy, the workforce, consumer privacy, and national security.

(i) Issue 1: Potential Impacts on the Average U.S. Standard of Living. Traditional economic theory on international trade predicts that in the long run, offshoring is likely to be beneficial for the average U.S. standard of living; however, some economists have argued that offshoring could harm U.S. living standards if it contributes to the erosion of important U.S. industries, undermines U.S. technological leadership, or leads to a decrease in average U.S. wages. Underlying this debate are different predictions about what new areas of comparative advantage the United States will develop as globalization intensifies—that is, what new goods and services will be developed that can be produced most efficiently in the United States—and different assessments about whether offshoring is contributing to downward pressure on U.S. wages.

(ii) Issue 2: Potential Impacts on Employment and Job Displacement. Many economists agree that offshoring is not likely to affect aggregate U.S. employment in the long run but acknowledge that in the short run some workers will lose their jobs when employers relocate production abroad. In addition, some economists argue that an important effect of offshoring and increased trade are structural changes that will generate permanent shifts in the types of work conducted by the U.S. labor force. However, there is debate about the expected magnitude of job losses related to offshoring, the implications of job displacement for those workers who are directly affected by it, and the expected direction of any structural changes in the labor market caused by offshoring.

(iii) Issue 3: Potential Impacts on Distribution of Income. There is disagreement among economists about whether offshoring is likely to significantly affect the distribution of income in the United States. Some economists have expressed concern that offshoring could accelerate U.S. income inequality. But others argue that changes in the income distribution are driven primarily by factors unrelated to offshoring, such as technological developments, and still others point out that offshoring could potentially decrease income inequality. Underlying these disagreements are debates about the extent to which, in the long run, offshoring will change the demand for U.S. workers at various income and skill levels.

(iv) Issue 4: Potential Impacts on National Security and Consumer Privacy. Experts express varying degrees of concern about the impact of services offshoring on the security of U.S. defense system and critical infrastructure—systems and structures that are essential to the nation, such as utilities and communication networks—as well as the privacy and security of consumers' financial and medical information. Underlying these debates are unresolved questions about the extent to which offshore operations, such as software development or medical records processing, pose increased security risks and the extent to which current laws and practices mitigate these risks.

(e) PROPOSED POLICIES IN OFFSHORING. Analysts of the offshoring phenomenon have proposed a broad range of policies in response to offshoring, proposals that represent a diverse set of potential directions for public policy in this area.

(i) Policy 1: Proposals to Improve U.S. Global Competitiveness. Many observers view offshoring as one aspect of a much broader process of increasing global interdependence. They propose policies that seek to improve the ability of U.S. firms and workers to compete in the global economy. Proponents of these policies contend that

increased foreign competition signals a need for policies to help the U.S. economy strategically develop new areas of comparative advantage. Examples of these proposals include increasing government support for research and development and improving education and training of U.S. workers.

(ii) Policy 2: Proposals to Address Effects on the Workforce. In response to concerns about job displacements due to offshoring, many have proposed policies to assist displaced workers who bear the immediate costs of offshoring. Some proposals would build on existing programs, such as extending the Trade Adjustment Assistance program to dislocated service workers. (Currently, the program covers only workers in the manufacturing sector, providing extended unemployment benefits and subsidized retraining to those who are dislocated because of foreign trade.) Other proposals would involve broader and more extensive reforms, such as establishing universal or portable health insurance or a wage insurance program under which reemployed workers' pay would not fall too far below what they had been paid before displacement.

(iii) Policy 3: Proposals to Enhance Security. Some proposals seek to address concerns that offshoring could pose risks to U.S. security, critical infrastructure, or the privacy of personal data. These proposals can be broadly categorized into two types—those that would restrict the type of work that can be sent to foreign locations, and those that would strengthen requirements governing security and data protection.

(iv) Policy 4: Proposals to Reduce the Extent of Offshoring. Some policy proposals address concerns about offshoring by U.S. government agencies or the private sector by seeking to reduce the extent of offshoring's occurrence. For example, some proposals would prohibit or constrain offshoring in government procurement. Other proposals seek to modify firms' incentives to offshore by altering tax provisions or enhancing incentives for firms to locate work in the United States.

12.8 APPLICABLE LAWS, REGULATIONS, STANDARDS, AND PRINCIPLES

Organizations have a legal and ethical obligation to comply with the various federal, state, and local laws, regulations, circulars and bulletins, directives and executive orders, government orders, and ordinances pertinent to a specific business area. Noncompliance with these laws and regulations can lead to fines, civil and/or criminal penalties, probation, and jail punishments (prison time), thus creating reputation (image) risk. Compliance with industry and/or organization standards, including professional standards, can increase the quality of products and services, which, in turn, can enhance an organization's reputation and image in the marketplace. Adherence to generally accepted business principles and practices could have similar effect as complying with standards.

A brief roundup of information about major laws, regulations, and standards is provided here as a reminder for checklist purposes. Note that these laws and regulations are subject to change as new ones are added and existing ones are amended or repealed. The reader is advised to obtain the original laws, regulations, and standards from the official sources for a better understanding of the provisions, requirements, and conditions of the laws, regulations, and standards (www.regulations.gov). Although some of the following laws, regulations, and standards directly affect public sector organizations

(i.e., government agencies), private-sector organizations can read, learn, and apply them to improve their business operations on a proactive basis.

U.S. organizations should comply with the following laws, regulations, standards, and principles pertinent to international business management:

U.S. Export Enhancement Act. The Export Enhancement Act of 1992 was established to devise a government-wide strategic plan for promoting exports and for creating a unified federal budget for export promotion that would be consistent with priorities established in the plan.

Omnibus Trade and Competitiveness Act. The Omnibus Trade and Competitiveness Act of 1988 provides authority for a unilateral response to unfair trade practices when established processes prove ineffective or untimely.

Export Trading Company Act. The Export Trading Company Act of 1982 was passed so that U.S. export-trading companies, like those in foreign countries, would have a means of reducing or eliminating perceived foreign barriers to their exports.

Export Administration Act. Under the Export Administration Act of 1979, the U.S. government controls exports of commercial goods and technology that can be diverted from civilian or nonnuclear purposes to military or nuclear purposes. Under the Act, the Secretary of Commerce administers the control system and issues export licenses.

U.S. Trade Act. The Trade Act of 1974 contains several sections. Some major sections are discussed next.

Section 201 of the act provides domestic industries with a period of relief from import competition when imports are a "substantial cause of serious injury." Temporary import relief is intended to provide the industry with an opportunity to adjust to import competition. The relief is granted if (1) the International Trade Commission (ITC) determines that the industry has been seriously injured, and (2) the U.S. President decides that temporary protection of the injured industry is in the national economic interest.

Section 301 of the act gives the U.S. President broad powers to enforce U.S. rights granted by trade agreements and to attempt to eliminate acts, policies, or practices of a foreign government that are unjustifiable, discriminatory, or unreasonable and that restrict U.S. trade or violate international trade agreements.

The Trade Act of 1974 expanded the types of remedies available to the ITC and made proceedings under Section 337 of the Tariff Act of 1930 subject to certain provisions of the Administrative Procedure Act and judicial review. The Trade Act also amended Section 337 to correct some deficiencies.

U.S. Tariff Act. Section 337 of the U.S. Tariff Act of 1930 deals with protecting intellectual property rights from counterfeit and infringing imports.

World Trade Organization. In 1995, the Geneva-based World Trade Organization (WTO) was created to administer the trade rules and to assist in settling trade disputes between its member nations. All WTO nations are entitled to normal trade relations with one another. This is referred to as most favored nation (MFN) trading status. This means that a member country cannot subject imports from a fellow member to tariffs that are higher than those the first country imposes on the same goods when imported from other WTO member countries. General Agreement on Tariffs and Trade (GATT)

was the previous name for the WTO. WTO established antidumping measures, protection of IP rights, trade in service measures, and trade-related investment measures (www.wto.org).

Patent Cooperation Treaty. The Patent Cooperation Treaty provides procedures for filing a single international application designating countries in which a patent is sought, a move that has the same effect as filing national applications in each of those countries.

International Court of Justice. The International Court of Justice (ICJ) is a judicial branch of the United Nations (UN) having voluntary jurisdiction over nations. Because the ICJ cannot enforce its rulings, countries displeased with an ICJ decision may simply ignore it. Consequently, few nations submit their disputes to the ICJ.

European Union. In 1993, the European Union (EU) was formed to promote common trade policies among member nations. There are several other regional trade communities in the world similar to EU. The EU's objectives are to (1) promote economic and social progress by creating an area without internal borders and by establishing an economic and monetary union, (2) assert its identity on the international scene by implementing a common foreign and security policy, (3) strengthen the protection of the rights and interests of citizens of its member states, and (4) develop close cooperation on justice and home affairs.

North American Free Trade Agreement. The North American Free Trade Agreement (NAFTA), which took effect in 1994, established a free trade area among the United States, Canada, and Mexico. NAFTA's objectives are to (1) eliminate trade barriers to the movement of goods and services across the borders, (2) promote conditions of fair competition in the free trade area, (3) increase investment opportunities in the area, and (4) provide adequate and effective enforcement of intellectual property rights.

Contracts for the International Sales of Goods. The United Nations (UN) Convention on Contracts for the International Sales of Goods (CISG) governs all contracts for international sales of goods between parties located in different nations that have ratified the CISG.

U.S. Antitrust Laws. U.S. antitrust laws apply to unfair methods of competition that have a direct, substantial, and reasonably foreseeable effect on the domestic, import, or export commerce of the United States.

U.S. Securities Regulations. Foreign issuers who issue securities or whose securities are sold in the secondary market in the United States must register them with the U.S. Securities and Exchange Commission (SEC) unless an exemption is available. The Securities Act of 1933 applies to primary market transactions, while the Securities Exchange Act of 1934 applies to secondary market transactions (www.sec.gov).

Organization for Economic Co-operation and Development. The Organization for Economic Co-operation and Development (OECD), located in Paris, France, issues codes and guidelines to member countries on topics including corporate governance principles, information security, bribery, and competition that affect international business (www.oecd.org).

U.S. Foreign Corrupt Practices Act. In 1977, the U.S. Congress enacted the Foreign Corrupt Practices Act (FCPA), prohibiting all U.S. domestic concerns from bribing foreign governmental or political officials.

International Anti-Bribery and Fair Competition Act. In 1998, the U.S. Congress enacted the International Anti-Bribery and Fair Competition Act to conform the FCPA to the OECD Convention against corruption. In essence, the 1998 act expands the scope of the FCPA.

U.S. Employment Discrimination Laws. Title VII of the U.S. Civil Rights Act of 1964, the Americans with Disabilities Act (ADA), and the Age Discrimination in Employment Act (ADEA) apply to U.S. citizens working for U.S. employers or for foreign companies controlled by U.S. employers. Employers, however, are not required to comply with these employment discrimination laws if compliance would violate the law of the foreign country in which the workplace is located.

International Chamber of Commerce. The International Chamber of Commerce (ICC), which is a nongovernmental organization, founded the International Court of Arbitration in 1923 to handle international commercial disputes. Arbitration usually is faster and less expensive than litigation in the courts.

Intellectual Property Laws. The U.S. laws protecting IP do not apply to transactions in other countries. Generally, the owner of an IP right must comply with each country's requirements to obtain from that country whatever protection is available. The requirements vary substantially from country to country, as does the degree of protection. There are several principal treaties with the United States such as the Paris Convention for the Protection of Intellectual Property, the Universal Copyright Convention, and the Berne Convention to protect IP rights.

Additional Resources

Berry, John. *Offshoring Opportunities: Strategies and Tactics for Global Competitiveness*. Hoboken, NJ: John Wiley & Sons, 2006.

Goldscheider, Robert, and Alan H. Gordon, eds. *Licensing Best Practices: Strategic, Territorial, and Technology Issues*. Hoboken, NJ: John Wiley & Sons, 2006.

Razgaitis, Richard. *Valuation and Pricing of Technology-Based Intellectual Property*. Hoboken, NJ: John Wiley & Sons, 2003.

Notes

1. *International Trade Issues* (GAO/OCG-93-11TR), December 1992, (Washington, DC: U.S. General Accounting Office).
2. *International Trade* (GAO/NSIAD-87-103BR), March 1987, (Washington, DC: U.S. General Accounting Office).
3. *Export Promotion: Rationales for and Against Government Programs and Expenditures* (GAO/T-GGD-95-169), May 1995, (Washington, DC: U.S. General Accounting Office).
4. *International Trade: U.S. Firms' Views on Customs' Protection of Intellectual Property Rights* (GAO/NSIAD-86-96), May 1986, (Washington, DC: U.S. General Accounting Office).
5. *Finding a Balance: Computer Software, Intellectual Property, and the Challenge of Technological Change* (OTA-TCT-527), May 1992, (Washington, D.C.: U.S. Congress, Office of Technology Assessment).

6. *Certified Business Manager (CBM) Examination Preparation Guide*, Part 2, Volume Three, Thomson Learning, 2004, 826–827.
7. *Certified Business Manager (CBM) Examination Preparation Guide*, Part 2, Volume Three, Thomson Learning, 2004, 835–838, 905–906.
8. *Bank Examination for Country Risk and International Lending* (GAO/ID-82-52), September 1982, (Washington, DC: U.S. General Accounting Office).
9. *Offshoring of Services: An Overview of the Issues* (GAO-06-5), November 2005, (Washington, DC: U.S. Government Accountability Office).

CHAPTER 13

PROJECT-MANAGEMENT BEST PRACTICES

13.1 OVERVIEW

(a) WHAT IS A PROJECT? A project is a *temporary* endeavor undertaken to create a unique product, service, or result. Temporary means that every project has a definite beginning and a definite end. The end is reached when the project's objectives have been achieved, or it becomes clear that the project objectives will not or cannot be met, or the need for the project no longer exists and the project is terminated. Temporary does not mean short in duration; many projects last for several years. In every case, however, the duration of a project is finite. Projects are not ongoing efforts.

A project creates unique deliverables, which are products, services, or results. *Uniqueness* is an important characteristic of project deliverables. The presence of repetitive elements in a specific project does not change the fundamental uniqueness of the project work.

Progressive elaboration is another characteristic of projects, one that accompanies the concepts of temporary and uniqueness. Progressive elaboration means developing in steps and continuing by increments.

(b) WHAT IS PROJECT MANAGEMENT? Project management is the application of knowledge, skills, tools, and techniques to project activities to meet project requirements. Project management is accomplished through the application and integration of the project management processes of initiating, planning, executing, monitoring, controlling, and closing. The project manager is the person responsible for accomplishing the project activities.

Managing a project includes:

- Identifying requirements
- Establishing clear and achievable objectives
- Balancing the competing demands for quality, scope, time, and cost
- Adapting the specifications, plans, and approach to the different concerns and expectations of the various stakeholders

13.2 PROJECT INTEGRATION MANAGEMENT

Project integration management includes the processes and activities needed to identify, define, combine, unify, and coordinate the various processes and activities. In the project management context, integration includes characteristics of unification, consolidation,

articulation, and integrative actions that are crucial to project completion, successfully meeting customer and other stakeholder requirements, and managing expectations. Integration, in the context of managing a project, is making choices about where to concentrate resources and efforts on any given day, anticipating potential issues, dealing with these issues before they become critical, and coordinating work for the overall project good. The integration effort also involves making tradeoffs among competing objectives and alternatives.

The need for integration in project management becomes evident in situations where individual processes interact. For example, a cost estimate needed for a contingency plan involves integration of the planning processes in project cost management, project time management, and project risk management. When additional risks associated with various staffing alternatives are identified, then one or more of those processes must be revisited. The project deliverables also need to be integrated with ongoing operations of either the performing organization or the customer's organization, or with the long-term strategic planning that takes future problems and opportunities into consideration.

Most experienced project management practitioners know there is no single way to manage a project. They apply project management knowledge, skills, and processes in different orders and degrees of rigor to achieve the desired project performance. However, the perception that a particular process is not required does not mean that it should not be addressed. The project manager and project team must address every process, and the level of implementation for each process must be determined for each specific project.

Organizations should do the following:

- **Develop Project Charter.** Develop a project charter formally authorizing the project or project phase.
- **Develop Preliminary Project Scope Statement.** Develop the preliminary project-scope statement, which presents a high-level scope narrative.
- **Develop Project Management Plan.** Document the actions necessary to define, prepare, integrate, and coordinate all subsidiary plans into a project management plan.
- **Direct and Manage Project Execution.** Execute the work defined in the project management plan to achieve the project's requirements as defined in the project scope statement.
- **Monitor and Control Project Work.** Monitor and control the processes used to initiate, plan, execute, and close a project to meet the performance objectives defined in the project management plan.
- **Integrated Change Control.** Review all change requests, approve changes, and control changes to the deliverables and organizational process assets.
- **Close Project.** Finalize all activities across all of the project management processes to formally close the project or project phase.

13.3 PROJECT SCOPE MANAGEMENT

Project scope management includes the processes required to ensure that the project includes all the work required, and only the work required, to complete the project successfully. Project scope management is primarily concerned with defining and controlling

what is and is not included in the project. The term "project scope" can refer to product scope as well as to project scope. "Product scope" is the features and functions that characterize a product, service, or result. "Project scope" is the work that needs to be accomplished to deliver a product, service, or result with the specified features and functions.

Organizations should do the following:

- **Scope Planning.** Create a project scope management plan that documents how the project scope will be defined, verified, and controlled, and how the work breakdown structure (WBS) will be created and defined.
- **Scope Definition.** Develop a detailed project scope statement as the basis for future project decisions.
- **Create WBS.** Subdivide the major project deliverables and project work into smaller, more manageable components.
- **Scope Verification.** Formalize acceptance of the completed project deliverables.
- **Scope Control.** Control changes to the project scope.

13.4 PROJECT TIME MANAGEMENT

Project time management includes the processes required to accomplish timely completion of the project.

Organizations should do the following:

- **Activity Definition.** Identify the specific schedule activities that need to be performed to produce the various project deliverables.
- **Activity Sequencing.** Identify and document dependencies among schedule activities.
- **Activity Resource Estimating.** Estimate the type and quantities of resources required to perform each schedule activity.
- **Activity Duration Estimating.** Estimate the number of work periods that will be needed to complete individual schedule activities.
- **Schedule Development.** Analyze activity sequences, durations, resource requirements, and schedule constraints to create the project schedule.
- **Schedule Control.** Control changes to the project schedule.

13.5 PROJECT COST MANAGEMENT

Project cost management includes the processes involved in planning, estimating, budgeting, and controlling costs so that the project can be completed within the approved budget.

Organizations should do the following:

- **Cost Estimating.** Develop an approximation of the costs of the resources needed to complete project activities.
- **Cost Budgeting.** Aggregate the estimated costs of individual activities or work packages to establish a cost baseline.
- **Cost Control.** Influence the factors that create cost variances (i.e., cost variance drivers) and control changes to the project budget.

- **Cost Management Plan.** Establish cost precision level, units of measure, organizational procedures links, control thresholds, earned value rules, reporting formats, and process descriptions.

13.6 PROJECT QUALITY MANAGEMENT

Project-quality management processes include all the activities of the performing organization that determine quality policies, objectives, and responsibilities so that the project will satisfy the needs for which it was undertaken. It implements the quality management system through the policies, procedures, and processes of quality planning, quality assurance, and quality control, with continuous process improvement activities conducted throughout, as appropriate.

Organizations should do the following:

- **Quality Planning.** Identify which quality standards are relevant to the project and determine how to satisfy them.
- **Perform Quality Assurance.** Apply the planned, systematic quality activities to ensure that the project employs all processes needed to meet requirements.
- **Perform Quality Control.** Monitor specific project results to determine whether they comply with relevant quality standards and identify ways to eliminate causes of unsatisfactory performance.
- **Quality Management System.** Select proprietary approaches to quality management systems, such as those recommended by Deming, Juran, Crosby, and others. Or select nonproprietary approaches, such as total quality management (TQM), Six Sigma, failure mode and effect analysis, design reviews, voice of the customer, cost of quality, and continuous improvement.
- **Quality Management and Project Management**. Understand that quality management complements project management. Emphasize customer satisfaction, prevention over inspection, management responsibility for resources, and continuous improvement with the plan-do-check-act (PDCA) cycle.

13.7 PROJECT HUMAN-RESOURCES MANAGEMENT

Project human-resources management includes the processes that organize and manage the project team. The project team is composed of the people who have been assigned roles and responsibilities for completing the project. Team members should be involved in much of the project's planning and decision making. Early involvement of team members adds expertise during the planning process and strengthens commitment to the project. The type and number of project team members can often change as the project progresses. Project team members can be referred to as the project's staff.

Organizations should do the following:

- **Human Resources Planning.** Identify and document project roles, responsibilities, and reporting relationships, as well as creating the staffing management plan.
- **Acquire Project Team.** Obtain the human resources needed to complete the project.

- **Develop Project Team.** Improve the competencies and interaction of team members to enhance project performance.
- **Manage Project Team.** Track team member performance, provide feedback, resolve issues, and coordinate changes to enhance project performance.

13.8 PROJECT COMMUNICATIONS MANAGEMENT

Project communications management employs the processes required to ensure timely and appropriate generation, collection, distribution, storage, retrieval, and ultimate disposition of project information. It provides the critical links among people and information that are necessary for successful communications. Project managers can spend an inordinate amount of time communicating with the project team, stakeholders, customers, and sponsors. Everyone involved in the project should understand how communications affect the project as a whole.

Organizations should do the following:

- **Communications Planning.** Determine the information and communications needs of the project stakeholders.
- **Information Distribution.** Make needed information available to project stakeholders in a timely manner.
- **Performance Reporting.** Collect and distribute performance information, including status reporting, progress measurement, and forecasting.
- **Manage Stakeholders.** Manage communications to satisfy the requirements of and resolve issues with project stakeholders.

13.9 PROJECT RISK MANAGEMENT

Project risk management includes the processes concerned with conducting risk management planning, identification, analysis, responses, monitoring, and control on a project, where most of these processes are updated throughout the project. The objectives are to increase the probability and impact of positive events, and decrease the probability and impact of events adverse to the project.

Organizations should do the following:

- **Risk Management Planning.** Decide how to approach, plan, and execute the risk management activities involved in a project.
- **Risk Identification.** Determine which risks might affect the project and document their characteristics.
- **Qualitative Risk Analysis.** Prioritize risks for subsequent further analysis or action by assessing and combining their probability of occurrence and impact.
- **Quantitative Risk Analysis.** Numerically analyze the effect on overall project objectives of identified risks.
- **Risk Response Planning.** Develop options and actions to enhance opportunities, and to reduce threats to project objectives.
- **Risk Monitoring and Control.** Track identified risks, monitor residual risks, identify new risks, execute risk response plans, and evaluate their effectiveness throughout the project life cycle.

13.10 PROJECT PROCUREMENT MANAGEMENT

Project procurement management includes the processes to purchase or acquire the products, services, or results needed from outside the project team to perform the work. The project organization can be either the buyer or seller of the product, service, or results under a contract.

Project procurement management includes the contract management and change control processes required to administer contracts or purchase orders issued by authorized project team members. It also includes administering any contract issued by an outside organization (the buyer) that is acquiring the project from the performing organization (the seller), and it includes administering contractual obligations placed on the project team by the contract.

Organizations should do the following:

- **Plan Purchases and Acquisitions.** Determine what to purchase or acquire and determine when and how.
- **Plan Contracting.** Document products, services, and results requirements and identify potential sellers.
- **Request Seller Responses.** Obtain information, quotations, bids, offers, or proposals, as appropriate.
- **Select Sellers.** Review offers, choose among potential sellers, and negotiate a written contract with each seller.
- **Contract Administration.** Manage the contract and relationship between buyer and seller, review and document how a seller is performing or has performed to establish required corrective actions and provide a basis for future relationships with the seller, mange contract-related changes, and manage the contractual relationship with the outside buyer of the project.
- **Contract Closure.** Complete and settle each contract, including the resolution of any open items, and close each contract applicable to the project or a project phase.

13.11 APPLICABLE LAWS, REGULATIONS, STANDARDS, AND PRINCIPLES

Organizations have a legal and ethical obligation to comply with the various federal, state, and local laws, regulations, circulars and bulletins, directives and executive orders, government orders, and ordinances pertinent to a specific business area. Noncompliance with these laws and regulations can lead to fines, civil and/or criminal penalties, probation, and jail punishments (prison time), thus creating reputation (image) risk. Compliance with industry and/or organization standards, including professional standards, and national/international standards, can increase the quality of products and services, which, in turn, can enhance an organization's reputation and image in the marketplace.

A brief roundup of information about major laws, regulations, standards is provided here as a reminder for checklist purposes. Note that these laws and regulations are subject to change as new ones are added and existing ones are amended or repealed. The reader is advised to obtain the original laws, regulations, and standards from the official sources for a better understanding of the provisions, requirements, and conditions of the laws, regulations, and standards (www.regulations.gov). Although some of the following laws, regulations, and national/international standards, and principles directly affect

public sector organizations (i.e., government agencies), private-sector organizations can read, learn, and apply them to improve their business operations on a proactive basis.

U.S. organizations should comply with the following laws, regulations, standards, and principles pertinent to project management:

Affirmative Action Plans. Executive Orders 11246, 11375, and 11478 address affirmative action plans requiring federal government contractors to develop and implement a formal, written plan for an employer with at least 50 employees and over $50,000 government contracts. The U.S. Secretary of Labor was given the power to cancel the contract of a noncomplying contractor or blacklist a noncomplying employer from future government contracts.

Age Discrimination in Employment Act. The Age Discrimination in Employment Act (ADEA) of 1967, amended in 1978, 1986, and 1991, makes it illegal for an employer to discriminate in compensation, terms, conditions, or privileges of employment because of an individual's age. There is no mandatory retirement age. The Act applies to all individuals above age of 40 working for employers having 20 or more workers. However, the Act does not apply if age is a job-related occupational qualification.

Americans with Disabilities Act. The Americans with Disabilities Act (ADA), enforced by the Equal Employment Opportunity Commission (EEOC), was passed in 1990 to stop discrimination against individuals with disabilities. The Act applies to all employers (i.e., private employers, employment agencies, labor unions, and state and local governments) with 15 or more employees. Major requirements of the ADA include the following:

- Discrimination is prohibited against individuals with disabilities who can perform the essential job functions.
- A covered employer must have reasonable accommodation for persons with disabilities so that they can function as employees, unless undue hardship would be placed on the employer.
- Preemployment medical examinations are prohibited except after an employment offer is made, conditional upon individuals passing a physical examination.
- Federal contractors and subcontractors with contracts valued at more than $2,500 must take affirmative action to hire qualified disabled individuals.

Consolidated Omnibus Budget Reconciliation Act. The Consolidated Omnibus Budget Reconciliation Act (COBRA) requires that most employers (except churches and the federal government) with 20 or more employees offer extended health care coverage to (1) employees who voluntarily quit, (2) widowed or divorced spouses and dependent children of former or current employees, and (3) retirees and their spouses whose health care coverage ends.

Davis-Bacon Act. The Davis-Bacon Act of 1931 affects compensation paid by firms engaged in federal construction projects valued in excess of $2,000 and requires that the prevailing wage rate be paid on all federal construction projects.

Foreign Corrupt Practices Act. The Foreign Corrupt Practices Act (FCPA) of 1977 prohibits U.S. firms from engaging in bribery in foreign countries. A fine line exists between paying agent-fees and gifts, which are legal, and bribery, which is illegal.

Health Insurance Portability and Accountability Act. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 allows employees to switch their health insurance plan from one employer to another to get the new health coverage, regardless of preexisting health conditions. The Act prohibits group insurance plans from dropping coverage for a sick employee and requires them to make individual coverage available to employees who leave group plans.

Immigration Reform and Control Act. The Immigration and Reform and Control Act (IRCA) of 1986 makes it illegal for an employer to discriminate in recruiting, hiring, or terminating based on an individual's national origin or citizenship. The Act penalizes employers who knowingly hire illegal aliens, and it establishes minimum documentation requirements for all new employees.

Occupational Safety and Health Act. The Occupational Safety and Health Act (OSHA) of 1970 was passed to assure every working man or woman safe and healthful working conditions. Every employer engaged in commerce who has one or more employees is covered by the Act. Farmers having fewer than ten employees are exempt. Federal, state, and local government employees and coal-mining employees are covered under different provisions or statutes.

Privacy Act. The Privacy Act of 1974 intended to protect the privacy of personal information applies to both private and sector organizations. The Act requires an organization to have a signed release from a person before it can give information about that person to someone else.

McNamara-O'Hara Service Contract Act. Like the Davis-Bacon Act, the McNamara-O'Hara Service Contract Act of 1965 applies to government contractors. The Service Contract Act requires firms with federal supply or service contracts exceeding $10,000 to pay a prevailing wage rate.

Walsh-Healy Public Contracts Act. The Walsh-Healy Public Contracts Act applies to government contractors, as do the Davis-Bacon Act and the McNamara-O'Hara Service Contract Act. The Walsh-Healy Public Contracts Act requires firms with federal supply or service contracts exceeding $10,000 to pay a prevailing-wage rate.

Vietnam-Era Veterans Readjustment Act. The Vietnam-Era Veterans Readjustment Act of 1974 requires that affirmative action in hiring and advancing Vietnam-era veterans be undertaken by federal contractors and subcontractors having contracts of $10,000 or more.

Goal Congruence Principle. The goal congruence principle states that the actions, wills, and needs of employees should be subordinated to the greater good of the organization they work for. An employee should ask himself whether his goals are consistent with the organization's goals.

Industry Standards. For example, contractors working with the U.S. Department of Defense must comply with its cost accounting standards when estimating costs during contract bidding.

Project Management Institute. The Project Management Institute (PMI) is a professional organization and the voice of the project management profession. It establishes professional certification (Project Management Professional, PMP), professional standards, and a code of ethics for project managers to follow (www.pmi.org).

Additional Resources

Kerzner, Harold. *Advanced Project Management: Best Practices on Implementation*, second edition. Hoboken, NJ: John Wiley & Sons, 2003.

Kerzner, Harold. *Project Management: A Systems Approach to Planning, Scheduling, and Controlling*, ninth edition. Hoboken, NJ: John Wiley & Sons, 2005.

McGhee, Pamela, and Peter McAliney. *Painless Project Management: A Step-by-Step Guide for Planning, Executing, and Managing Projects*. Hoboken, NJ: John Wiley & Sons, 2007.

Note

1. Sections 13.1 through 13.10 are excerpted with permission. *A Guide to the Project Management Body of Knowledge* (PMBOK® Guide), third edition (Newtown Square, Pennsylvania: Project Management Institute Inc., 2004). Copyright and all rights reserved. Material from this publication has been reproduced with the permission of PMI.

INDEX