Wiley Finance Series

Operational Risk Management

A Complete Guide to a Successful Operational Risk Framework

+ website

PHILIPPA X. GIRLING

WILEY

Operational Risk Management

Founded in 1807, John Wiley & Sons is the oldest independent publishing company in the United States. With offices in North America, Europe, Australia, and Asia, Wiley is globally committed to developing and marketing print and electronic products and services for our customers' professional and personal knowledge and understanding.

The Wiley Finance series contains books written specifically for finance and investment professionals as well as sophisticated individual investors and their financial advisors. Book topics range from portfolio management to e-commerce, risk management, financial engineering, valuation and financial instrument analysis, as well as much more.

For a list of available titles, visit our Web site at www.WileyFinance.com.

Operational Risk Management

A Complete Guide to a Successful Operational Risk Framework

PHILIPPA GIRLING

WILEY

Cover design: Wiley

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

Library of Congress Cataloging-in-Publication Data:

ISBN 9781118532454 (Hardcover)
ISBN 9781118744642 (ePDF)
ISBN 9781118744789 (ePub)

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

For my husband, Joe; my daughters, Leah, Holly, and Tegwen;
and my step-daughters, Hayley and Allison.
Thank you all for helping me to balance risk and reward every day.

Contents

Preface

The evolution of operational risk over the past 10 years has given rise to a new profession: the operational risk manager. This book equips the student or practitioner of operational risk with all of the framework elements that are needed in order to establish a successful operational risk framework.

While best practices and regulatory guidelines are readily available for both the qualitative and the quantitative elements of operational risk, many firms are still struggling with the practical implementation of operational risk frameworks. This book provides real-life examples of successful methods and tools while facing head-on the cultural challenges that are prevalent in this field.

Today, chief risk officers are finding themselves facing the daunting task of providing assurances to senior management and to board members that operational risks are being effectively managed and mitigated. Traditional market and credit risk approaches offer only partial effectiveness in the operational risk field, and this book explores the unique qualitative aspects of operational risk management.

This book also provides insight into some of the (often notorious) operational risk events that have occurred in the past 10 years, with analysis of the JPMorgan Whale event, the UBS and Société Générale unauthorized trading scandals, the Knight Capital technology misstep and the management of operational risk at the 2012 London Olympics.

The author explores how the regulatory framework has evolved over the past few years in response to these events and in response to the recent economic crises and proposes effective approaches to meet both global regulatory expectations and the industry's risk management goals.

The framework proposed provides practical steps to ensure effective identification, assessment, monitoring, and mitigation of operational risks. In starker terms, how can you find it, size it, watch it, and kill it (or choose to accept it)?

Operational risk is an elusive risk category, but it can be managed using best practices that have grown up in the industry in the past few years. This book provides both the new and the experienced operational risk professional with tools and best practices to implement a successful operational risk framework and to embed operational risk management more deeply in their firms.

Acknowledgments

Thank you to my agent, John Wright, for his engagement, support, and encouragement, and to Bill Falloon at Wiley & Sons for taking me on as a new author and for welcoming me into the Wiley community. Thank you to the whole Wiley & Sons team, especially my editors, Meg Freeborn and Stacey Fischkelta for their careful and diligent shepherding of the manuscript and Tiffany Charbonier for her book design.

Thank you to Cathy Hampson, Jon Holland, Nicole Hubert, Lorinda Opsahl-Ong, Ilya Rozenfeld, David Silverman, Mark Taylor, Jedediah Turner, and Jan Voigts—my friends, colleagues, and peers, who generously agreed to review portions of this book and to provide their thoughts and suggestions. This is a much stronger work as a result of your excellent insight and in-depth knowledge of the field of operational risk. I am grateful to you all for taking time to review and improve the manuscript when you are very busy managing operational risk on a daily basis. Any remaining weaknesses and errors in the book are entirely my own doing.

Thank you to both ORX and IBM Algo FIRST for providing external loss data for analysis with a generous spirit and remarkable efficiency.

Thank you to Penelope Vance for coaching me through the entire process and for asking all of the right questions at the right time.

Thank you to GARP for generously allowing the reuse of content that I wrote for one of their course textbooks.

Finally, a special thank you to my children, Leah, Holly, Tegwen, Hayley, and Allison for their patience with me as I wrote, and to my husband, Joe, for his constant encouragement that I could, and should, write this book.

Operational Risk Management

CHAPTER 1

Definition and Drivers of Operational Risk

This chapter examines the definition of operational risk and its formal adoption in Basel II. The requirements to identify, assess, control, and mitigate operational risk are introduced, along with the four causes of operational risk—people, process, systems, and external events—and the seven risk types. The definition is tested against the 2012 London Olympics. The different roles of operational risk management and measurement are introduced, as well as the role of operational risk in an enterprise risk management framework.

THE DEFINITION OF OPERATIONAL RISK

What do we mean by operational risk?

Operational risk management had been defined in the past as all risk that is not captured in market and credit risk management programs. Early operational risk programs, therefore, took the view that if it was not market risk, and it was not credit risk, then it must be operational risk. However, today a more concrete definition has been established, and the most commonly used of the definitions can be found in the Basel II regulations. The Basel II definition of operational risk is:

> *. . . the risk of loss resulting from inadequate or failed processes, people and systems or from external events.*
>
> *This definition includes legal risk, but excludes strategic and reputational risk.*[1]

Let us break this definition down into its components. First, there must be a risk of loss. So for an operational risk to exist there must be an

associated loss anticipated. The definition of "loss" will be considered more fully when we look at internal loss data in Chapter 7, but for now we will simply assume that this means a financial loss.

Next, let us look at the defined causes of this loss. The preceding definition provides four causes that might give rise to operational risk losses. These four causes are (1) inadequate or failed processes, (2) inadequate or failed people (the regulators do not get top marks for their grammar, but we know what they are getting at), (3) inadequate or failed systems, or (4) external events.

While the language is a little awkward (what exactly are "failed people," for example), the meaning is clear. There are four main causes of operational risk events: the person doing the activity makes an error, the process that supports the activity is flawed, the system that facilitated the activity is broken, or an external event occurs that disrupts the activity.

With this definition in our hands, we can simply look at today's newspaper or at the latest online headlines to find a good sample of operational risk events. Failed processes, inadequate people, broken systems, and violent external events are the mainstay of the news. Operational risk surrounds us in our day-to-day life.

Examples of operational risk in the headlines in the past few years include egregious fraud (Madoff, Stanford), breathtaking unauthorized trading (Société Générale and UBS), shameless insider trading (Raj Rajaratnam, Nomura, SAC Capital), stunning technological failings (Knight Capital, Nasdaq Facebook IPO, anonymous cyber-attacks), and heartbreaking external events (hurricanes, tsunamis, earthquakes, terrorist attacks). We will take a deeper look at several of these cases throughout the book.

All of these events cost firms hundreds of millions, and often billions, of dollars. In addition to these headline-grabbing large operational risk events, firms constantly bleed money due to frequent and less severe events. Broken processes and poorly trained staff can result in many small errors that add up to serious downward pressure on the profits of a firm.

The importance of these types of risks, both to the robustness of a firm and to the systemic soundness of the industry, has led regulators to push for strong operational risk frameworks, and has driven executive managers to fund and support such frameworks.

The Basel II definition of operational risk has been adopted or adapted by many firms and is now generally accepted as the standard. It has been incorporated into national regulations across the globe with only minor adaptations and is consistently referred to by regulators and operational risk managers.

Basel II is the common name used to refer to the "International Convergence of Capital Measurement and Capital Standards: A Revised Framework," which was published by the Bank for International Settlements in Europe in 2004.

The Basel II framework set out new risk rules for internationally active financial institutions that wished to continue to do business in Europe. These rules related to the management and capital measurement of market and credit risk, and introduced a new capital requirement for operational risk. In addition to the capital requirement for operational risk, Basel II laid out qualitative requirements for operational risk management, and so a new era of operational risk management development was born.

JPMorgan Chase has adapted the definition very simply as follows:

> *Operational risk is the risk of loss resulting from inadequate or failed processes or systems, human factors or external events.*[2]

Deutsche Bank has a more creative interpretation:

> *Operational risk is the potential for failure (incl. the legal component) in relation to employees, contractual specifications and documentation, technology, infrastructure and disasters, external influences and customer relationships.*
>
> *Operational risk excludes business and reputational risk.*[3]

Under the Basel II definition, legal events are specifically included in the definition of operational risk, and a footnote is added to further clarify this.

> *Legal risk includes, but is not limited to, exposure to fines, penalties, or punitive damages resulting from supervisory actions, as well as private settlements.*[4]

This is a helpful clarification, as there is often some tension with the legal department when the operational risk function first requests information on legally related events. This is something that will be considered in more detail later in the section on loss data collection.

The Basel II definition also specifically *excludes* several items from operational risk:

> *This definition includes legal risk, but excludes strategic and reputational risk.*[5]

These nuances in the Basel II definition are often reflected in the definition adopted by a firm, whether or not they are governed by that regulation. However, these exclusions are not always applied in operational risk frameworks.

For example, some firms have adopted definitions of operational risk that include reputational risk. For example, Citi's definition includes reputational risk:

> *Operational risk is the risk of loss resulting from inadequate or failed internal processes, systems or human factors, or from external events. It includes the reputation and franchise risk associated with business practices or market conduct in which Citi is involved.*[6]

We will be looking at ways that operational risk management and measurement can meet the underlying need to accomplish five tasks:

1. **Identifying** operational risks.
2. **Assessing** the size of operational risks.
3. **Monitoring and controlling** operational risks.
4. **Mitigating** operational risks.
5. **Calculating capital** to protect you from operational risk losses.

These five requirements occur again and again in global and national regulations and are the bedrock of successful operational risk management.

In addition to putting these tools in place, a robust operational risk framework must look at all *types* of operational risk. There are seven main categories of operational risk as defined by Basel II.

Before we dive into how operational risk impacts the financial services industry, let's take a step back and see how other business have been addressing operational risk.

The 2012 Summer Olympics and Paralympics in London, England, provide an interesting case study in how operational risk is managed outside financial services and a practical view into how the basic elements of operational risk management have been applied.

2012 LONDON OLYMPICS: A CASE STUDY[7]

At the end of the summer of 2012 the Paralympic flame was extinguished in London, bringing the Summer Olympics and Paralympics to a triumphant close. By all accounts both Games were a resounding success, and there has been much proud puffing of British chests and declaring of "Happy and Glorious!"

Before the opening ceremony, London mayor Boris Johnson had admitted that there would be "imperfections and things going wrong" as the capital coped with the Olympics.[8]

However, at the opening ceremony, London 2012 Olympic Chairman Lord Sebastian Coe confidently declared: "One day we will tell our children and our grandchildren that when our time came we did it right."[9]

It is unlikely that Lord Coe and his team turned to banking regulations to assist them in this task, but the Games do offer us an interesting opportunity to assess whether the Basel II operational risk requirements stand up to a "real world" test. Is Lord Coe an excellent operational risk manager? Will we see him as a headline speaker at a future risk conference? (Spoiler alert: He has my vote.)

The Basel requirements are designed to ensure that there is an adequate framework in place to manage any risks resulting from failed or inadequate processes, people, and systems or from external events. These were exactly the risks that faced the London 2012 team as they prepared to unleash a global event on the crowded city of London. The four main causes of operational risk were there in abundance.

People: Nervous athletes, opinionated officials, aggressive press, terrorists, disgruntled Londoners, (missing) security guards, confused volunteers, crazed fans, lost children, heads of state, visiting dignitaries, and the list goes on.

Processes and systems: Stadium building and preparation, ticket sales, transportation, opening ceremonies, closing ceremonies, Olympic village management, cleaning, feeding, running races, organizing matches, safety checks of the parallel bars, awarding medals, playing anthems, global broadcasting, keeping that darned flame alight, and the list goes on.

External events: Two words—London weather.

In the most recent Bank of International Settlements Sound Practices document the rules require risk management activities that identify and assess, monitor and report, and control and mitigate operational risks. Was this how Lord Coe pulled it off? Did he ensure that the London 2012 team excelled in all of those practices?

The Basel rules also provide seven categories of risk for us to fit any operational risk events into.[10] The risk categories certainly seem comprehensive to those of us in the banking industry, but do they truly capture all operational risks? The categories we are given to work with are:

- **Internal Fraud:** Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law, or company policy, excluding diversity/discrimination events, which involves at least one internal party.

- **External Fraud:** Losses due to acts of a type intended to defraud, misappropriate property, or circumvent the law, by a third party.
- **Employment Practices and Workplace Safety:** Losses arising from acts inconsistent with employment, health, or safety laws or agreements; from payment of personal injury claims; or from diversity/discrimination events.
- **Clients, Products, and Business Practices:** Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product.
- **Damage to Physical Assets:** Losses arising from loss or damage to physical assets from natural disaster or other events.
- **Business Disruption and System Failures:** Losses arising from disruption of business or system failures.
- **Execution, Delivery, and Process Management:** Losses from failed transaction processing or process management, from relations with trade counterparties and vendors.

We will learn more about these categories later, but first we will test them out in the real world.

Test One: Do the Seven Basel Operational Risk Categories Work in the Real World?

Let's take a look at the categories and see if they match up with those salacious Olympics headlines that popped up over the summer:

- **Internal Fraud:** "Olympic Badminton Players Disqualified for Trying to Lose"[11]
- **External Fraud:** "London Olympics Fake Tickets Create 'Honeypot' for Criminals"[12]
- **Clients, Products, and Business Practices:** "Empty Seats at Olympic Venues Prompt Investigation"[13]
- **Employment Practice and Workplace Safety:** "Dispute Between London Olympics and Musicians Union Heats Up"[14]
- **Execution, Delivery, and Process Management:** "NATB Calls London Olympics Ticket Distribution a Failure"[15]
- **Damage to Physical Assets:** "Olympic Security Shortfall Called 'Absolute Chaos'"[16]
- **Business Disruption and System Failure:** "London 2012: Traffic Jams and Impact of Games Lanes"[17]

Certainly, the Olympics raised risks in each of the categories. Indeed, over eight years of working in operational risk with clients ranging from banks to commodities shipping firms and from law firms to tourism and hospitality conglomerates, I have found the Basel seven categories have proven remarkably resilient and comprehensive.

Test Two: The Risk Management Tools

Managing the Olympic Games and Paralympic Games was without doubt an enormous challenge in operational risk management. So the next test, and surely the more important one, is whether the recent Sound Practices requirements cover the bases? (*Note:* We will not be discussing why baseball is not an Olympic sport).

Risks did materialize, and the headlines were at times brutal, but the final wrap-up headlines were consistently positive. Did the London 2012 team avert disaster by applying the tenets of good operational risk management? Did they identify and assess, monitor and report, and control and mitigate the risks?

Yes, they did. In the Annual Report of the London Organising Committee of the Olympic Games and Paralympic Games Ltd. (LOCOG),[18] the team outline the "principal risks and uncertainties" that they face and describe their methodology for managing these risks as follows:

> *Management use a common model to* ***identify*** *and* ***assess*** *the impact of risks to their business. For each risk, the likelihood and consequence are identified, management* ***controls*** *and the frequency of* ***monitoring*** *are confirmed and results reported. (emphasis added, p. 33)*

To be a stickler for accuracy, I will concede that the word *mitigation* is referenced only for budget risks and security risks, but it is clear in the report that mitigation of the risks identified was the key purpose of the risk management activities. In addition, according to their own website,[19] the London Prepares series, the official London 2012 sports testing program, helped to test vital areas of operations ahead of the London 2012 Games.

The Basel rules were first published in 2004 and have not changed fundamentally since that time. It is interesting, and somewhat comforting, to see that the language of operational risk management has become remarkably consistent—the same risk categories and the same tenets of best practices apply whether you are a bank or an Olympic Games.

London Mayor Boris Johnson admitted that there would be "imperfections and things going wrong"[20] as the capital coped with the Olympics.

For the record, I like this as a new definition for operational risk. Operational risk management does not ensure that nothing will go wrong, but instead focuses on identifying and assessing what can go wrong, on monitoring and reporting changes in risk, and mitigating and controlling the impact of any events that are threatening to occur, or that have occurred and need speedy and effective cleanup.

It's real-world risk management, and that is why operational risk managers get so passionate about their discipline. Operational risk exists in every industry and in every endeavor. It exists in massive global multimedia extravaganzas and in small local events. It does appear that the Basel operational risk management rules are applicable across the board. Job well done, Bank for International Settlements.

Now whether we need to have all of these rules and also hold bucket loads of capital in case something happens anyway—well, that's a different discussion for a different chapter (Chapter 12, "Capital Modeling").

For now, we can agree that an excellent motto for an operational risk department would be Lord Coe's confident declaration that "one day we will tell our children and our grandchildren that when our time came we did it right."[21]

Operational risk has some similarities to market and credit risk. Most important, it should be actively managed because failure to do so can result in a misstatement of an institution's risk profile and expose it to significant losses.

However, operational risk has some fundamental differences to market and credit risk. Operational risk, unlike market and credit risk, is typically not directly taken in return for an expected reward. Market risk arises when a firm decides to take on certain products or activities. Credit risk arises when a firm decides to do business with a particular counterparty. In contrast, operational risk exists in the natural course of corporate activity. As soon as a firm has a single employee, a single computer system, a single office, or a single process, operational risk arises.

While operational risk is not taken on voluntarily, the level of that risk can certainly be impacted by business decisions. Operational risk is inherent in any enterprise, but strong operational risk management and measurement allows for that risk to be understood and either mitigated or accepted.

OPERATIONAL RISK MANAGEMENT AND OPERATIONAL RISK MEASUREMENT

There are two sides to operational risk: operational risk management and operational risk measurement. There is often tension between these two activities, as well as overlap. Basel II requires capital to be held for operational risk and offers several possible calculation methods for that capital, which will be discussed

later in this chapter. This capital requirement is the heart of the operational risk measurement activities and requires quantitative approaches.

In contrast, firms must also demonstrate that they are effectively managing their operational risk, and this requires qualitative approaches. A successful operational risk program combines qualitative and quantitative approaches to ensure that operational risk is both appropriately measured and effectively managed.

Operational Risk Management

Helpful guidelines for appropriate operational risk management activities in a firm can be found in Pillar 2 of Basel II:

> *736.* **Operational risk:** *The Committee believes that similar rigour should be applied to the management of operational risk, as is done for the management of other significant banking risks. …*
>
> *737. A bank should develop a framework for managing operational risk and evaluate the adequacy of capital given this framework. The framework should cover the bank's appetite and tolerance for operational risk, as specified through the policies for managing this risk, including the extent and manner in which operational risk is transferred outside the bank. It should also include policies outlining the bank's approach to identifying, assessing, monitoring and controlling/mitigating the risk.*[22]

There are several important things to note in these sections. First, operational risk should be managed with the same rigor as market and credit risk. This is an important concept that has many implications when considering how to embed an operational risk management culture in a firm, as will be explored later in this chapter.

Second, policies regarding risk appetite are required. This is no easy task, as articulating a risk appetite for operational risk can be very challenging. Most firms would prefer to have no operational risk, and yet these risks are inherent in their day-to-day activities and cannot be completely avoided. Recently, regulators have been very interested in how firms are responding to this challenge, and there is much debate about how to express operational risk appetite or tolerance and how to manage against it. This will be explored further in each of the framework sections later in the chapter.

Finally, policies must be written that outline the bank's approach to "identifying, assessing, monitoring, and controlling/mitigating" operational risk. This is the heart of the definition of operational risk management, and the elements of an operational risk framework need to address these

challenges. Does each element contribute to the identification of operational risks, the assessment of those risks, the monitoring of those risks, and the control or mitigation of those risks? To be successful, an operational risk framework must be designed to meet these four criteria for all operational risk exposures, and it takes a toolbox of activities to achieve this.

In the operational risk management toolbox are loss data collection programs, risk and control self-assessments, scenario analysis activities, key risk indicators, and powerful reporting. (See www.wiley.com/go/girling for access to sample toolbox templates.) Each of these elements will be considered in turn in this book.

Operational Risk Measurement

Operational risk measurement focuses on the calculation of capital for operational risk, and Basel II provides for three possible methods for calculating operational risk capital, which will be discussed later. Some firms choose to calculate operational risk capital, even if they are not subject to a regulatory requirement, as they wish to include the operational risk capital in their strategic planning and capital allocation for strategic and business reasons.

The Relationship between Operational Risk Management and Other Risk Types

Operational risk often arises in the presence of other risk types, and the size of an operational risk event may be dramatically impacted by market or credit risk forces.

EXAMPLE

One of Gamma Bank's business lines offers retail customers the ability to trade bonds. One of the customers calls the broker at Gamma Bank and instructs the broker to buy Andromeda Corporation bonds for the customer's account. The trade is executed, but it is mistakenly booked as a sell, instead of a buy; this will result in a significantly larger loss if the market moves up.

The cost of making the customer whole will now be much higher than if the market had remained stable. In fact, there could be a gain if the market drops. It is clear, then, that market risk can magnify operational risk.

There are also events that include both credit and operational risk elements. If a counterparty fails, and there was an operational error in securing adequate collateral, then the credit risk event is magnified by operational risk.

While market risk, credit risk, and operational risk functions are usually run separately, there are benefits in integrating these functions where possible. The overall risk profile of a firm depends not on the individual market, credit, and operational risks, but also on elusive strategic and reputational risks (or impacts) and the relationships among all of these risk categories.

Additional risk categories also exist—for example, geopolitical risk and liquidity risk. For these reasons, some firms adopt an enterprise risk management (ERM) view of their risk exposure. It is important to consider the role of operational risk management as an element in ERM and to appreciate its relationship with all other risk types. The relationship among risks can be illustrated in Figure 1.1.

This ERM wheel illustrates that all risk types are interrelated and that central risk types can have an impact on risk types on the outer spokes of the wheel. For example a geopolitical risk event might result in risks arising in market risk, credit risk, strategic risk, liquidity risk, and operational risk.

Similarly, reputational risk or reputational impact can occur as a result of any risk event and so is at the center of the ERM wheel. This is just one possible model for the relationship between risk types and simply illustrates the complexity of effective ERM. Operational risk sits on the ERM wheel and is best managed and measured with that in mind.

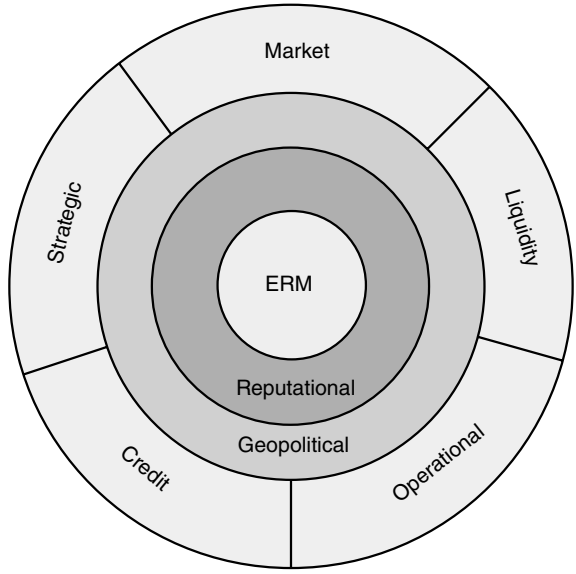

FIGURE 1.1 Enterprise Risk Management Wheel

EXAMPLE

A country's government banned trades in a particular type of derivative. This ban could result in market risk (the value of the derivatives plummets), credit risk (counterparties who are concentrated in this product might fail), strategic risk (the business model might rely on growth in that product), and operational risk (certain activities might now be illegal).

DRIVERS OF OPERATIONAL RISK MANAGEMENT

Operational risk management has arisen as a discipline as a result of drivers from three main sources: regulators, senior management, and third parties.

In addition to Basel II, there are other regulatory drivers for operational risk management including Solvency II, which imposes Basel-like requirements on insurance firms, and a host of local regulations such as the Markets in Financial Instruments Directive (MiFID) legislation in Europe and the Sarbanes-Oxley Act (which includes risk and control requirements for financial statements) in the United States. The regulatory evolution of operational risk is discussed in Chapter 2.

Additional business drivers from within the banks and from third parties complement the many regulatory drivers of operational risk management. One of the most important of these additional drivers is that senior management and the board both want to be fully informed of the risks that face the firm, including operational risk exposures. They are fully aware that operational risk events can have catastrophic financial and reputational impact. An effective operational risk program should provide transparency of operational risk exposure to allow senior management to make strategic business decisions fully informed of the operational risk implications.

A strong operational risk framework provides transparency into the risks in the firm, therefore allowing for informed business decision making. With a strong operational risk framework, a firm can avoid bad surprises and equip itself with tools and contingency planning to be able to respond swiftly when an event does occur.

Furthermore, external third parties have started to ask about the operational robustness of a firm.

Ratings agencies, investors, and research analysts are now aware of the importance of operational risk management and often ask for evidence that

an effective operational risk framework is in place, and whether sufficient capital is being held to protect a firm from a catastrophic operational risk event.

KEY POINTS

- Operational risk is defined in Basel II as the risk of loss resulting from inadequate or failed processes, people and systems or from external events. This definition includes legal risk but excludes strategic and reputational risk.
- Firms adapt the Basel II definition to their own needs.
- Both qualitative and quantitative approaches are needed to effectively manage and measure operational risk.
- Operational risk is a key element in an enterprise risk management (ERM) approach.

REVIEW QUESTIONS

1. Which of the following best meets the Basel II definition of operational risk?
   a. A basket of options expires with a value of zero.
   b. A client refuses to pay his invoice.
   c. A wire transfer is sent to the wrong account.
   d. A government expropriates all foreign-owned assets.
2. The main causes of operational risk are generally accepted to be:
   a. People, processes, systems, external events
   b. People, processes, systems, internal events
   c. Processes, systems, events
   d. People, events

NOTES

1. S644, International Convergence of Capital Measurement and Capital Standards: A Revised Framework, Bank for International Settlements, 2004.
2. JPMorgan Chase & Co. Annual Report, 2008, p. 117.
3. Deutsche Bank Financial Report, 2011, p. 110.
4. Footnote 90, supra.
5. See note 1.

6. Citi Annual Report 2011, p. 106
7. As featured in issue 9 of *Risk Universe* and reproduced with their permission.
8. www.independent.co.uk/news/uk/home-news/things-will-go-wrong-as-london-holds-olympics-says-boris-johnson-7952706.html.
9. www.bbc.co.uk/sport/0/olympics/18906710#TWEET179228.
10. Annex 9, International Convergence of Capital Measurement and Capital Standards: A Revised Framework, Bank for International Settlements, 2004.
11. http://edition.cnn.com/2012/08/01/sport/olympics-badminton-scandal/index.html.
12. www.bloomberg.com/news/2012-07-26/london-olympics-fake-tickets-create-honeypot-for-criminals.html.
13. http://sports.yahoo.com/blogs/olympics-fourth-place-medal/empty-seats-olympic-venues-prompt-investigation-224320331–oly.html.
14. www.billboard.biz/bbbiz/industry/legal-and-management/dispute-between-london-olympics-and-musicians-1007687952.story#I1ptQC1VdfjCF9xS.99.
15. www.ticketnews.com/news/natb-calls-london-olympics-ticket-distribution-a-failure081213258.
16. www.cbsnews.com/8301-33747_162-57473130/olympic-security-shortfall-called-absolute-chaos/.
17. www.bbc.co.uk/news/uk-england-london-18962856.
18. www.london2012.com/mm/Document/Publications/Annualreports/01/24/09/33/locog-annual-report-2010-11.pdf.
19. www.london2012.com/about-us/london-prepares-series/.
20. See note 8.
21. www.bbc.co.uk/sport/0/olympics/19023771.
22. S644, International Convergence of Capital Measurement and Capital Standards: A Revised Framework, Bank for International Settlements, 2004.

CHAPTER 2

The Regulatory Push

The regulation of operational risk is globally founded on Basel II. This chapter discusses the regulatory response to the Basel Capital Accords (commonly known as Basel I and Basel II) that were presented by the Basel Banking Committee of the Bank of International Settlements in 1988 and 2004, which were intended to provide a robust capital framework and risk management approach for internationally active banks.

The focus of this chapter is on (1) the history of the Basel Accords; (2) the rules of the Basel Accords; (3) the adoption of Basel II in Europe and (4) in the United States; (5) the impact of the financial crisis and resulting European and U.S. regulatory changes, including the Dodd-Frank regulation in the United States; and, finally, (6) the future of Basel regulation and the role of operational risk management.

HISTORY OF THE BASEL ACCORDS

The Basel Accords were developed by the Bank of International Settlements (BIS), which is headquartered in Basel, Switzerland. The BIS describes its mission and activities as follows:

> *BIS is an international organization which fosters international monetary and financial cooperation and serves as a bank for central banks.*
>
> *The BIS fulfills this mandate by acting as:*
>
> - *a forum to promote discussion and policy analysis among central banks and within the international financial community*
> - *a center for economic and monetary research*
> - *a prime counterparty for central banks in their financial transactions*
> - *agent or trustee in connection with international financial operations*[1]

The BIS was originally established in 1930 to assist with the management of reparation loans post World War I, but it soon transitioned into a body that addressed monetary and financial stability through statistical analysis, economic research, and regular meetings between central bank governors and other global financial experts.

The following central banks or monetary authorities participate in BIS meetings: Algeria, Argentina, Australia, Austria, Belgium, Bosnia and Herzegovina, Brazil, Bulgaria, Canada, Chile, China, Croatia, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hong Kong SAR, Hungary, Iceland, India, Indonesia, Ireland, Israel, Italy, Japan, Korea, Latvia, Lithuania, Macedonia (FYR), Malaysia, Mexico, the Netherlands, New Zealand, Norway, the Philippines, Poland, Portugal, Romania, Russia, Saudi Arabia, Serbia, Singapore, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Thailand, Turkey, the United Kingdom, and the United States, plus the European Central Bank.[2] Over the years, the BIS has established several standing committees to take on the important financial topics of the day. It was heavily involved in supporting the Bretton Woods System in the early 1970s, and tackled the challenges of cross-border capital flows and the importance of financial regulation in the late 1970s and 1980s. In 1974, the G10 nations[3] formed the BIS Basel Committee on Banking Supervision to address shortcomings in the regulation of internationally active banks. The committee membership has now grown to include 27 countries.[4]

In 1988, the Basel Committee on Banking Supervision published the Basel Capital Accord[5] (commonly known today as Basel I) to provide a framework for the consistent and appropriate regulation of capital adequacy and risk management in internationally active banks. In 2004, the Basel Committee published a revised framework, which came to be known as Basel II.[6] Today, the Basel Committee has four subcommittees: the Standards Implementation Group, the Policy Development Group, the Accounting Task Force, and the Basel Consultative Group, each of which also has its own subcommittees and working groups.

By its own admission, the Basel Committee has no legal authority over member central banks:

> *The Committee does not possess any formal supranational supervisory authority, and its conclusions do not, and were never intended to, have legal force. Rather, it formulates broad supervisory standards and guidelines and recommends statements of best practice in the expectation that individual authorities will take steps to implement them through detailed arrangements—statutory or otherwise—which are best suited to their own national systems. In this way, the Committee encourages convergence*

> *towards common approaches and common standards without attempting detailed harmonization of member countries' supervisory techniques.*[7]

However, the U.S. Federal Reserve, along with the majority of member central banks, moved forward with national regulatory implementation of most of the Basel Committee recommendations.

RULES OF THE ACCORDS

The Basel Accords outline rules for financial institutions and for the national regulators who supervise those institutions.

Basel I

In 1988, the BIS Basel Committee on Banking Supervision published the International Convergence of Capital Measurement and Capital Standards (commonly known then as the Basel Capital Accord and today as Basel I). The report aimed to "secure international convergence of supervisory regulations governing the capital adequacy of international banks" (1988, p. 1). Balin outlined the four "pillars" of Basel I as the Constituents of Capital, the Risk Weights, a Target Standard Ratio, and Transitional and Implementing Agreements.[8]

Basel I focused on credit risk and assigned different weightings (0 percent, 10 percent, 20 percent, 50 percent, and 100 percent) for capital requirements, depending on the level of credit risk associated with the asset. Later amendments to Basel I added further weightings to accommodate more sophisticated instruments. The Target Standard Ratio set a minimum standard whereby 8 percent of a bank's risk-weighted assets had to be covered by Tier 1 and Tier 2 capital reserves.

There were no requirements to either manage or measure operational risk under the Basel Accord.

The Basel Accord was adopted with relative ease by the G10 nations who were members of the Basel Banking Committee at that time, including the United States. In the United States, the Basel recommendations were codified in Title 12 of the United States Code and Title 12 of the Code of Federal Regulations.

The Basel Accord (Basel I) was seen as a safety and soundness standard that would protect banks from insolvency and the minimum capital requirements provided a standard below which regulators would not permit a bank to continue to conduct business. However, regulators soon began to

question whether Basel I adequately captured the risks of the increasingly complex and changing financial markets. In addition, banks were able to "game" the system by moving assets off balance sheet and by manipulating their portfolios to minimize their required capital, while not necessarily minimizing their actual risk exposure.

Basel II

As pressure mounted for a revised approach, the Basel Committee responded by proposing a revised Capital Adequacy Framework in June 1999. They described the new proposed capital framework as consisting of three pillars: "minimum capital requirements; … supervisory review of an institution's internal assessment process and capital adequacy; and effective use of disclosure to strengthen market discipline as a complement to supervisory efforts."[9]

Comments and discussions were held over the next few years, with the newly broadened membership of the Committee providing a global perspective on the proposed changes. The International Convergence of Capital Measurement and Capital Standards, a Revised Framework was issued on June 26, 2004, and served as a basis for national rule-making to reflect the Basel II approaches. The Basel Committee outlined the goal of the revised framework as follows:

> *The Basel II Framework describes a more comprehensive measure and minimum standard for capital adequacy that national supervisory authorities are now working to implement through domestic rule-making and adoption procedures. It seeks to improve on the existing rules by aligning regulatory capital requirements more closely to the underlying risks that banks face. In addition, the Basel II Framework is intended to promote a more forward-looking approach to capital supervision, one that encourages banks to identify the risks they may face, today and in the future, and to develop or improve their ability to manage those risks. As a result, it is intended to be more flexible and better able to evolve with advances in markets and risk management practices.*[10]

On July 4, 2006, the Committee issued an updated version of the revised framework incorporating additional guidance and including those sections of Basel I that had not been revised. The revised framework is almost 10 times the length of Basel I, running to over 300 pages. For the first time, operational risk management and measurement were required.

Basel II consists of three pillars: Pillar 1—Minimum Capital Requirements, Pillar 2—Supervisory Review Process, and Pillar 3—Market Discipline.

Pillar 1 The major changes to the capital adequacy rules are outlined in detail in Pillar 1. Basel II requires banks to hold capital for assets in the holding company, so as to prevent banks from avoiding capital by moving assets around within its corporate structure.

Credit Risk Pillar 1 offers three possible approaches to calculating credit risk: the standardized approach, the foundation internal ratings based (F-IRB) approach, and, finally, the advanced IRB approach.

Under the standardized approach a bank uses "authorized" rating institution ratings in order to assign risk weightings and to calculate capital.

Under the IRB approaches, the banks may take advantage of capital improvements on the standardized approach by applying their own internal credit rating models. Under F-IRB, a bank may develop their own model to estimate the probability of default (PD) for individual clients or groups of clients, subject to approval from their local regulators. F-IRB banks are required to use their regulator's prescribed loss given default (LGD) and to calculate the risk-weighted asset (RWA) and the final required capital.

Under advanced IRB (A-IRB), banks may use their own estimates for PD, LGD, and exposure at default (EAD) to calculate RWA and the final required capital.

Market Risk Pillar 1 also provides market risk capital requirements, based mainly on a value at risk (VaR) approach.

Operational Risk Finally, Pillar 1 introduces a new risk category: operational risk. As discussed in Chapter 1, operational risk is defined in Basel II as the "risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk."[11]

Pillar 1 offers three possible methods to calculate capital for operational risk: the basic indicator approach (BIA), the standardized approach (TSA), or the advanced measurement approach (AMA).[12]

Under BIA, capital is simply calculated from a percentage (currently set at 15 percent) of the average of the last three years' revenue. TSA offers different percentage weightings depending on the business line—ranging from 12 percent for retail banking to 18 percent for sales and trading. AMA offers banks the opportunity to develop their own risk-based model for calculating operational risk capital. AMA requires that the model include

BASIC INDICATOR APPROACH

$\sum avg\ 3yr\ gross\ revenue\ x\ \alpha$

α is 15%

THE STANDARDIZED APPROACH

$\sum avg\ 3yr\ gross\ revenue\ x\ \beta$

β for each business line is:

Corporate Finance	18%
Trading and Sales	
Payment and Settlement	
Commercial Banking	15%
Agency Services	
Retail Banking	12%
Retail Brokerage	
Asset Management	

ADVANCED MEASUREMENT APPROACH

Regulator approved, internal risk model which includes the following inputs:

- Internal Loss Data
- External Loss Data
- Scenario Analysis
- Business Environment Internal Control Factors

FIGURE 2.1 Three Capital Calculation Approaches for the Treatment of Operational Risk under Pillar 1 of Basel II

four elements: internal loss data, external loss data, scenario analysis, and business environment and internal control factors. These three methods are summarized in Figure 2.1.

While Pillar 1 offers three possible methods to calculate operational risk capital, most large banks have found that their local regulator requires them to pursue an AMA approach. In addition, even where a bank is not required to take an AMA approach to calculating capital, their regulator often advises them that they should adopt best practices and that best practices require them to ensure they have fully developed all four elements of AMA.

Therefore, the standard for a strong operational risk framework is based on the effective development of internal and external loss data systems, appropriate use of scenario analysis, and effective development of business environment and internal control factors. Whether or not these are used as direct inputs into a capital model, they are considered vital elements of a sound operational risk management framework.

Capital Reserves Finally, under Pillar 1, a bank must hold capital reserves of at least 8 percent of their total credit, market, and operational risk-weighted assets:

$$\frac{capital}{market\ risk + credit\ risk + operational\ risk} \geq 8\%$$

Pillar 2 Basel II introduces the Pillar 2 requirements as follows:

> *This section discusses the key principles of supervisory review, risk management guidance and supervisory transparency and accountability produced by the Committee with respect to banking risks, including guidance relating to, among other things, the treatment of interest rate risk in the banking book, credit risk (stress testing, definition of default, residual risk, and credit concentration risk), operational risk, enhanced cross-border communication and cooperation, and securitization.*[13]

Pillar 2 outlines how the regulators are expected to enforce soundness standards and provides a mechanism for additional capital requirements to cover any material risks that have not been effectively captured in Pillar 1.

Pillar 3 Pillar 3 provides methods for disclosure of risk management practices and capital calculation methods to the public. The purpose of Pillar 3 is to increase transparency and to allow investors and shareholders a view into the inner risk practices of the bank.

ADOPTION OF BASEL II IN EUROPE

In the European Union, Basel II was codified through the European Parliament through the Capital Requirements Directive,[14] which required member states to enact appropriate local regulations by January 1, 2007, with advanced approaches available by January 1, 2008.

ADOPTION OF BASEL II IN THE UNITED STATES

In the United States, the plethora of regulators added to the complexities of implementation.

Securities and Exchange Commission Amendments to the Net Capital Rule

U.S. investment banks needed to select a global Basel II regulator, and the Securities and Exchange Commission (SEC) looked for ways for them to be able to select the SEC as that regulator. To support this, the SEC adopted rules that allowed for consolidated supervised entities (CSEs) to apply to the SEC for regulatory supervision for Basel II. The five large U.S.

investment banks took this opportunity: Goldman Sachs, Morgan Stanley, Bear Stearns, Merrill Lynch, and Lehman Brothers successfully applied for CSE status.

The SEC moved swiftly to make changes to its net capital rules to reflect Basel II standards,[15] and the five investment banks were quickly approved for Basel II supervision by the SEC.

U.S. Regulators' Adoption of New Regulations to Apply Basel II

Meanwhile, the remaining United States banks were waiting to see whether U.S. banking regulations would be amended to apply the Basel II rules to them. Questions were raised on the appropriateness of the rules, and the audacity of the European Union in driving these global standards was hotly debated in Congress. Pressure was mounting from the regulators and the banks, and international political tensions were increasing as banks waited for the United States to move forward with Basel II rules.

On September 25, 2006, the Federal Banking Agencies (the Office of the Comptroller of the Currency [OCC], the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation [FDIC], and the Office of Thrift Supervision [OTS]), came together to collect comments on the adoption of Basel II rules in the United States through two Notices of Proposed Rulemaking relating to capital requirements: New Risk-Based Capital Rules for Large or Internationally Active U.S. Banks in accordance with Basel II, and Market Risk Rule.

On November 2, 2007, the Federal Reserve Board approved final rules to implement new risk-based capital requirements in the United States for large, internationally active banking organizations, stating:

> *The new advanced capital adequacy framework, known as Basel II, more closely aligns regulatory capital requirements with actual risks and should further strengthen banking organizations' risk-management practices.*
>
> *'Basel II is a modern, risk-sensitive capital standard that will protect the safety and soundness of our large, complex, internationally active banking organizations. The new framework is designed to evolve over time and adapt to innovations in banking and financial markets, a significant improvement from the current system,' said Federal Reserve Board Chairman Ben S. Bernanke.*[16]

On July 20, 2008, the Federal Reserve, OCC, OTS, and FDIC reached agreement regarding implementation of Basel II in the United States. There

would be mandatory Basel II rules for large banks, and opt-in provisions for noncore banks as had been proposed in the Notices of Proposed Rulemaking (NPRs).

The new standards were to be transitioned into over a parallel run period, with Basel I based capital floors being set for the first three years.

Pillar 2 guidance was provided later, resulting in supervisory guidance being published on December 7, 2007.[17] The Pillar 2 guidance provided for an Internal Capital Adequacy Assessment Process (ICAAP) for the implementation of Pillar 2 standards in a bank. The final rules were published in the Federal Register, mostly through amendments to Title 12.

IMPACT OF THE FINANCIAL CRISIS

The global economic crisis that began in 2007 led to much soul-searching by governments, regulators, and the BIS as they sought to understand how the Basel frameworks had failed to protect the global economy.

The Promise of Basel III

Global political pressure has resulted in the BIS Basel Committee on Banking Supervision revisiting Basel II to consider what further regulatory and capital enhancements are needed in order to ensure global financial stability. Christopher Cox himself has been vocal about the need for regulatory reform, recently stating that "in March 2008, I formally requested that the Basel Committee address the inadequacy of the Basel capital and liquidity standards."[18]

The Group of Twenty (G20) has also been meeting regularly to address concerns regarding global regulatory requirements and capital adequacy. They established a Financial Stability Board (FSB) to address these concerns and to make recommendations for change, and the BIS has been working closely with the FSB and the International Monetary Fund (IMF) to develop new recommendations to enhance the Basel framework. In April 2010, the G20 met to review a report prepared by IMF and FSB and "the main message coming through this document from central banks and regulators is that priority number one is Basel III," two sources involved in the G20 process said.[19]

Indeed, the G20 agreed to introduce Basel III by the end of 2012. Proposals for an updating of Basel II were put forward by the Basel Committee on Banking Supervision in December 2009 in two documents: "Strengthening the Resilience of the Banking Sector"[20] and "International

Framework for Liquidity Risk Measurement, Standards and Monitoring."[21] The Committee gathered comments and feedback, and the main recommendations are:

- An increase in Tier One capital.
- Additional capital for derivatives, securities financing, and repo markets.
- Tighter leverage ratios.
- Setting aside revenue during upturns to protect against cyclicality of markets.
- Minimum 30-day liquidity standards.
- Enhanced corporate governance, risk management, compensation practices, disclosure, and board supervision practices.

European Response to the Crisis

The Committee of European Banking Supervisors (CEBS) produced the "Guidelines on the Management of Operational Risk in Market Related Activities"[22] in October 2010. They placed a heavy emphasis on the importance of strong corporate governance, an area that many saw as one of the key causes of the financial crisis. This document supplemented the earlier "Guidelines on the Scope of Operational Risk and Operational Risk Loss"[23] and rounded out the European detailed guidance on the implementation of a robust operational risk framework under Basel II.

This guidance is now used by European regulators as a measure against which to assess the operational risk frameworks of European banks.

U.S. Response to the Crisis

The financial turmoil of 2007–2009 resulted in a quick and fundamental change in the way that Basel II was applied to large financial institutions in the United States. Of the original five investment banks that had opted for CSE status with the SEC, three no longer existed by 2009: Bear Stearns, Lehman Brothers, and Merrill Lynch. The remaining two, Goldman Sachs and Morgan Stanley, changed their structures to Bank Holding Companies, and they were now under the regulatory auspices of the Federal Reserve. As a result, the SEC Basel II framework was simply no longer relevant and was formally ended by then chairman Christopher Cox on September 26, 2008.[24] Chairman Cox maintained that the economic turmoil was not a result of SEC Basel II implementation, but instead that the voluntary opt-in nature of the regulations was to blame.

> *As I have reported to the Congress multiple times in recent months, the CSE program was fundamentally flawed from the beginning, because investment banks could opt in or out of supervision voluntarily.*[25]

However, there was some speculation and criticism that the SEC had taken a light touch approach to the application of Basel II rules for its five CSEs and that it had, in fact, thereby contributed to the economic crisis. In particular, the high levels of leverage that were permitted by the investments banks were strongly debated, with suggestions that the SEC's CSE rules allowed them to lever up to levels of 30-to-1.[26] The operational risk requirements of Basel II did not seem to receive strong enforcement by the SEC, and operational risk frameworks were put under intense scrutiny once the Federal Reserve moved in as the new regulator for the original CSEs.

Morgan Stanley and Goldman Sachs are currently operating their new bank status under the Basel I framework while they seek to be readmitted to the Basel II club under the Federal Reserve's Basel II regulations. The time taken to meet the Federal Reserve standards does suggest that there may be some truth to the suggestion that their previous Basel II framework under the SEC, including the operational risk requirements, may have been relatively, and inappropriately, light.

Banks that were operating under the Federal Reserve's Basel II framework before the economic crisis are continuing to pursue their Basel II approval with no major changes. However, they too may have noticed an increased vigilance from their regulator as the current emphasis on regulatory stringency is on the upswing.

U.S. Interagency Guidance on Advanced Measurement Approach In June 2011, the United States regulators issued the "Interagency Guidance on the Advanced Measurement Approaches for Operational Risk."[27] This guidance was agreed by the Board of Governors of the Federal Reserve System, the FDIC, the OCC, and the OTS.

The guidance had been long awaited and addressed several areas where the range of practices in operational risk had been broad among U.S. banks. While some of the conclusions may have been unpopular, the written guidance pointed toward a clearer path to Basel II AMA approval in the United States. However, as of the time of writing, there has still not been an approval in the United States.

The Guidance will be referred to in later chapters, as it contains important interpretation of how governance and validation should be

implemented and the use of the four required data elements in the capital calculation.

Dodd-Frank Act In the United States, regulatory reform has been progressing along similar lines to those that were proposed by G20. President Barack Obama introduced a guidance document, "A New Foundation: Rebuilding Financial Supervision and Regulation," on June 17, 2009, and 2009 saw many bills introduced that addressed specific aspects of regulatory reform, often overlapping with existing Basel II rules. Davis Polk[28] summarized these as follows:

- The Financial Stability Improvement Act as amended by the House Financial Services Committee through November 6, 2009, or the "House Interim Version."
- The Investor Protection Act, passed by the House Financial Services Committee on November 4, 2009, or the "House Investor Protection bill."
- The Consumer Financial Protection Agency Act, passed by the House Financial Services Committee on October 29, 2009, or the "House CFPA bill."
- The Accountability and Transparency in Rating Agencies Act, passed by the House Financial Services Committee on October 28, 2009, or the "House Rating Agencies bill."
- The Private Fund Investment Advisers Registration Act, passed by the House Financial Services Committee on October 27, 2009, or the "House Private Fund Investment Advisers bill."
- The Derivatives Markets Transparency and Accountability Act, passed by the House Committee on Agriculture on October 21, 2009, or the "Peterson bill."
- The Over-the-Counter Derivatives Markets Act, passed by the House Financial Services Committee on October 15, 2009, or the "Frank OTC bill."
- The Federal Insurance Office Act, introduced by Representative Paul Kanjorski (D-PA) on October 1, 2009, or the "House Insurance bill."
- The Liability for Aiding and Abetting Securities Violations Act, introduced by Senator Arlen Specter (D-PA) on July 30, 2009, or the "Specter bill."
- Treasury Proposals released in the summer of 2009, or the "Treasury proposals."
- The Shareholder Bill of Rights Act, introduced by Senator Charles Schumer (D-NY) on May 19, 2009, or the "Schumer bill."

These all finally culminated in a catch-all bill, the Restoring American Financial Stability Act of 2009, which was introduced into the Senate by Senator Christopher Dodd (D-CT) and into the House of Representatives

by Representative Barney Frank (D-MA). It was subsequently renamed the "Dodd-Frank Wall Street Reform and Consumer Protection Act," and President Obama signed the bill into law on July 21, 2010.

The full title of the Act is rather emotive:

> *An Act to promote the financial stability of the United States by improving accountability and transparency in the financial system, to end "too big to fail," to protect the American taxpayer by ending bailouts, to protect consumers from abusive financial services practices, and for other purposes.*

Dodd-Frank addresses some of the Basel III issues and will result in United States regulatory changes that meet many of the Financial Stability Board recommendations. The main elements of Dodd-Frank are outlined in the summary released by the Senate Committee on Banking, Housing, and Urban Affairs[29] under the following categories:

- **Consumer Protections with Authority and Independence:** The bill creates "a new independent watchdog, Consumer Financial Protection Bureau, housed at the Federal Reserve, with the authority to ensure American consumers get the clear, accurate information they need to shop for mortgages, credit cards, and other financial products, and protect them from hidden fees, abusive terms, and deceptive practices."
- **Ends Too Big to Fail:** The bill "ends the possibility that taxpayers will be asked to write a check to bail out financial firms that threaten the economy by: creating a safe way to liquidate failed financial firms; imposing tough new capital and leverage requirements that make it undesirable to get too big; updating the Fed's authority to allow system-wide support but no longer prop up individual firms; and establishing rigorous standards and supervision to protect the economy and American consumers, investors and businesses."
- **Advanced Warning System:** The bill "creates a council to identify and address systemic risks posed by large, complex companies, products, and activities before they threaten the stability of the economy."
- **Transparency and Accountability for Exotic Instruments:** The bill "eliminates loopholes that allow risky and abusive practices to go on unnoticed and unregulated—including loopholes for over-the-counter derivatives, asset-backed securities, hedge funds, mortgage brokers and payday lenders."
- **Federal Bank Supervision:** The bill "streamlines bank supervision to create clarity and accountability and protects the dual banking system that supports community banks."

- **Executive Compensation and Corporate Governance:** The bill "provides shareholders with a say on pay and corporate affairs with a non-binding vote on executive compensation"
- **Protects Investors:** The bill "provides tough new rules for transparency and accountability for credit rating agencies to protect investors and businesses."
- **Enforces Regulations on the Books:** The bill "strengthens oversight and empowers regulators to aggressively pursue financial fraud, conflicts of interest and manipulation of the system that benefit special interests at the expense of American families and businesses."[30]

With President Obama having successfully entered his second term, any hopes of a full-scale repeal of Dodd-Frank have been put to rest. While there may be changes made to some of the elements of the Act, much of the main content will move forward into regulation, albeit at a lower pace than had been originally planned.

THE FUTURE

The Basel Accords have resulted in global regulatory changes that have reached beyond G10, beyond G20, and into the far reaches of the global financial regulatory environment. Basel I introduced credit risk capital measures, and Basel II provided enhanced risk capital calculation for credit, market, and operational risk. The United States has played a key role on the Basel Committee for Banking Supervision that designed these accords and so it is not surprising to find that U.S. regulators have consistently adopted these measures.

The recent economic crisis has highlighted the need for further refinements in the way that banks calculate and hold capital for all risk types, and the importance of sound operational risk management and measurement. In addition, it has drawn close scrutiny of the methods used to ensure there is robust risk management and healthy liquidity in the bank. Basel III was scheduled for adoption in January 2013, but at the time of writing, this deadline had been missed by both the EU and the United States, and a delayed and phased implementation was being crafted for implementation over the next few years.

Meanwhile, the writing and implementation of rules under Dodd-Frank and similar nation specific rules across the globe continues at a fast pace. While the operational risk framework has remained mostly unchanged since Basel II, the plethora of new regulatory requirements and governance enhancements has led to increasing complexity in managing the operational risks faced by a bank on a day-to-day basis.

KEY POINTS

- The Basel Accords were developed by the Bank of International Settlements (BIS) to ensure capital adequacy.
- Basel II was first published in 2004, and its full title is "International Convergence of Capital Measurement and Capital Standards: A Revised Framework."
- Basel II required operational risk management and measurement for the first time.
- There are three approaches to calculating capital for operational risk under Basel II: the basic approach, the standardized approach, and the advanced measurement approach.
- In 2008, the Federal Reserve, OCC, FDIC, and OTS issued a joint requirement for mandatory Basel II rules for large United States banks and opt-in provisions for noncore banks.
- In 2009 and 2010, the CEBS issued guidance on operational risk management and measurement.
- In 2011, U.S. regulators issued the Interagency Guidance on the Advanced Measurement Approaches for Operational Risk.
- The United States enacted the Dodd-Frank Wall Street Reform and Consumer Protection Act in July 2010.
- The areas addressed by the act are:
  - Consumer Protections with Authority and Independence
  - Ends Too Big to Fail
  - Advanced Warning System
  - Transparency and Accountability for Exotic Instruments
  - Federal Bank Supervision
  - Executive Compensation and Corporate Governance
  - Protects Investors
  - Enforces Regulations on the Books

REVIEW QUESTIONS

1. The full title of Basel II is
   a. "International Convergence of Capital Measurement and Capital Standards: A Revised Framework"
   b. "International Convergence of Capital Accords"
   c. "Accord of the Bank of International Settlements"
   d. "International Convergence of Capital Measurement and Capital Standards"

2. Pillar 1 provides guidance for
   - **I.** Three approaches to credit risk
   - **II.** Three approaches to operational risk
   - **III.** Market risk VaR
   - **IV.** A minimum capital ratio of 8 percent
   - **V.** Liquidity risk ratios
     - **a.** I only
     - **b.** I and II only
     - **c.** I, II, and III only
     - **d.** I, II, III, and IV only
     - **e.** All of the above

NOTES

1. "About BIS" (n.d.). Retrieved from www.bis.org/about/index.htm.
2. "BIS Activities" (n.d.). Retrieved from www.bis.org/about/functions.htm.
3. Central bank and lead financial regulatory representatives from France, Germany, Italy, Japan, the Netherlands, Sweden, Switzerland, the United Kingdom, the United States, and Luxembourg.
4. Argentina, Australia, Belgium, Brazil, Canada, China, France, Germany, Hong Kong SAR, India, Indonesia, Italy, Japan, Korea, Luxembourg, Mexico, Netherlands, Russia, Saudi Arabia, Singapore, South Africa, Spain, Sweden, Switzerland, Turkey, United Kingdom, United States. "Fact Sheet—Basel Committee on Banking Supervision" (n.d.). Retrieved from www.bis.org/about/factbcbs.htm.
5. "International Convergence of Capital Measurement and Capital Standards." Bank of International Settlements, Basel Committee, 1988.
6. Bank of International Settlements, "International Convergence of Capital Measurement and Capital Standard: A Revised Framework," 2004.
7. "History of the Basel Committee and its Membership" (n.d.). Retrieved from www.bis.org/bcbs/history.htm.
8. B. J. Balin, "Basel I, Basel II, and Emerging Markets: A Non-Technical Analysis." Washington DC: The Johns Hopkins University School of Advanced International Studies (SAIS), 2008, pp. 3–4.
9. See note 7.
10. "Basel II: Revised International Capital Framework" (n.d.). Retrieved from www.bis.org/publ/bcbsca.htm.
11. "International Convergence of Capital Measurement and Capital Standards: A Revised Framework," Comprehensive Version. Bank of International Settlements, Basel Committee on Banking Supervision, 2006, section 644.

12. Ibid., p. 144.
13. Ibid., p. 204.
14. Comprising Directive 2006/48/EC and Directive 2006/49/EC.
15. Net Capital Rule Amendments. Securities and Exchange Commission, Release No. 34-49830, 69 Fed. Reg. 34427, June 21, 2004.
16. "Risk-Based Capital Standards: Advanced Capital Adequacy," November 2, 2007. Retrieved from www.federalreserve.gov/newsevents/press/bcreg/20071102a.htm.
17. Supervisory Guidance: Supervisory Review Process of Capital Adequacy (Pillar 2) Related to the Implementation of the Basel II Advanced Capital Framework, 2007.
18. Statement of Christopher Cox, former chairman, U.S. Securities and Exchange Commission before the Committee on Financial Services U.S. House of Representatives, April 20, 2010. Retrieved from www.house.gov/apps/list/hearing/…dem/cox_testimony_2010-04-20.pdf.
19. "G20 Must Make Basel II Top Priority: Sources," April 20, 2010. Retrieved from www.reuters.com/article/idUSTRE63J2QU20100420.
20. "Strengthening the Resilience of the Banking Sector: Consultative Document." Bank of International Settlement, Basel Committee on Banking Supervision, 2009.
21. Ibid.
22. Retrieved from www.eba.europa.eu/documents/Publications/Standards—Guidelines/2010/Management-of-op-risk/CEBS-2010-216-(Guidelines-on-the-management-of-op-.aspx.
23. Retrieved from http://eba.europa.eu/getdoc/0448297d-3f85-4f7d-9fa6-c6ba5f80895a/CEBS-2009_161_rev1_Compendium.aspx.
24. "Chairman Cox Announces End of Consolidated Supervised Entities Program," SEC Press Release, 2008, 230. Retrieved fromwww.sec.gov/news/press/2008/2008-230.htm.
25. Ibid.
26. P. Madigan, "SEC Adoption of Basel II 'Allowed 30-to-1 leverage.'" *Risk,* October 29, 2009.
27. Retrieved from www.occ.gov/news-issuances/bulletins/2011/bulletin-2011-21a.pdf.
28. Davis Polk, "Summary of the Restoring American Financial Stability Act of 2009, Introduced by Senator Christopher Dodd (D-CT) November 10, 2009." Discussion Draft, 2009.
29. Senate Committee on Banking, Housing, and Urban Affairs, "Summary: Restoring American Financial Stability," 2009.
30. Ibid.

CHAPTER 3

The Operational Risk Framework

This chapter introduces the important elements that are recommended for an operational risk framework. These elements include the foundations of governance, risk appetite, culture and awareness, and policy and procedure; the building blocks of data collection including loss data, risk and control self-assessment, scenario analysis, and key risk indicators; and the final capstones of calculation of capital and reporting.

OVERVIEW OF THE OPERATIONAL RISK FRAMEWORK

As discussed in Chapter 1, an operational risk program should ensure that operational risk is identified, assessed, monitored, controlled, and mitigated. The Basel Committee on Banking Supervision's 2011 "Sound Practices for the Management and Supervision of Operational Risk"[1] provides helpful guidelines for best practices for operational risk departments. When meeting these standards, an operational risk framework needs to be developed that will fit with the culture of the bank and reflect best practice in the industry.

The main data building blocks of an operational risk framework are:

- Loss data collection
- Risk and control self-assessment
- Scenario analysis
- Key risk indicators

The framework must also address governance, provide policies and procedures, drive culture change, and respond to and inform risk appetite. In addition, the framework should feed data into any capital modeling and should feed data and analysis into risk reporting.

Figure 3.1 illustrates a possible framework that includes all of these elements.

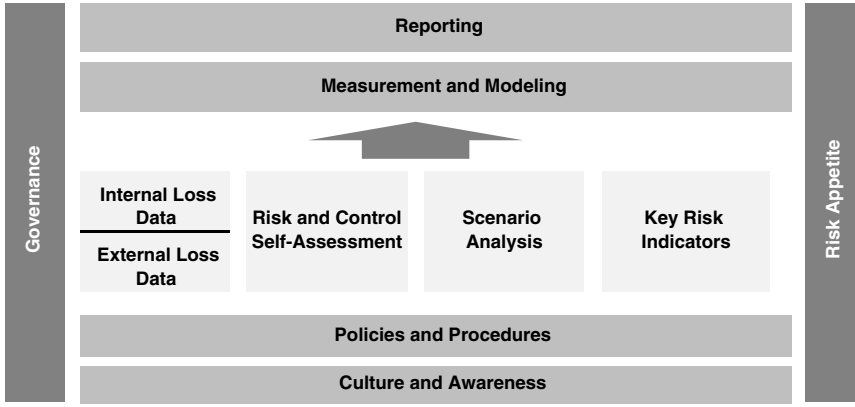

FIGURE 3.1 Operational Risk Framework

Each element is important, but the timing of implementation and the relative weight of each element in the framework, will vary depending on the culture of the bank and its regulatory and business drivers. The following chapters will consider each of these elements, their practical application, the tools that are available, and critical factors for their successful implementation.

THE FOUNDATIONS OF THE FRAMEWORK

There are two elements that drive the design and acceptance of the operational risk framework as a whole, and it is important to start with these. These two elements are *governance* and *culture and awareness*.

Governance

Governance determines the roles and responsibilities of the head of the operational risk function and her team that manages the framework, the committees that oversee and make key decisions about risk management, the operational risk managers in lines of business, and every employee who may encounter operational risk.

In order to develop an operational risk framework that is effective, an appropriate governance structure must be carefully considered at the outset. Governance should also be revisited at least annually, to check whether it is still working as intentioned. Good governance enables the escalation of risk and ensures that risk transparency is effective through all of the layers of operational risk management that may exist.

Governance holds the whole operational risk framework together. In Chapter 4 we will explore the various aspects of governance, including who should own the operational risk functions, and what the operational risk functions should own.

Culture and Awareness

Once governance has been addressed, the next step in developing an operational risk framework is to proactively tackle culture and awareness. While it may be tempting to jump into developing the building blocks of operational risk management, such as loss data collection and risk and control self-assessment, those building blocks will only be successful if sufficient time and energy has been spent on culture and awareness.

The implementation of a successful operational risk framework requires winning over the hearts and minds of the employees of the firm. Spotting operational risks is a developed skill. While the risks exist in all lines of business, it takes the right tone at the top, training and awareness to identify the risks. Operational risk can arise in any corner of the firm and can result in best practice responses, or may be met with indifference. The response will depend on the work that has been done in the area of culture and awareness. In Chapter 5, we look at various aspects of this essential activity, including training, marketing, and building a brand for the operational risk function.

Policies and Procedures

The next foundational element of the framework is policies and procedures. There was a time, not that long ago, when banks and financial institutions did not take their policy and procedure programs very seriously. Today, that has changed dramatically under the watchful eye of the regulators. Firms are expected to have clear, actionable, and measurable policies and procedures.

Indeed, there is a trend in financial services to pay closer attention to writing and actively managing policies and procedures. A well-managed policy framework gives lines of business increased flexibility because the rules of the road are not ambiguous. Having well-managed policies and procedures gives a financial firm a head start and increased autonomy when interacting with regulators. A good operational risk framework will have well documented policies and procedures that reflect the requirements of each of the elements.

In Chapter 6, we look at examples of standard policies and procedures and discuss best practices in how to design, implement, maintain, and track these documents.

THE FOUR DATA BUILDING BLOCKS

With governance, culture and awareness, and policy and procedures holding the framework together, we can now turn to the four main pieces of work that are needed in order to have an effective operational risk framework: loss data collection, risk and control self-assessment, scenario analysis, and key risk indicators.

Loss Data Collection

There are two types of loss data that are key to the framework: internal loss data, which occurs within the firm, and external loss data, which occurs outside the firm.

Internal Loss Data Operational risk management and measurement require access to data on events that have already occurred in the firm, and in the industry and loss data collection is the first of four activities that form the heart of an operational risk framework. The firm's own data is referred to as *internal loss data,* while industry data is referred to as *external loss data*.

Developing an effective set of internal loss data is often the first major task faced when building out an operational risk framework. Basel II requires a firm to have at least three years of internal loss data in order to pursue an advanced measurement approach. Therefore, loss data collection needs to be quickly established, and carefully implemented to ensure good quality data is in place.

If loss data collection is started before appropriate governance is established and before culture and awareness have been addressed, then the data collected is likely to be lower quality.

We will look into regulatory requirements and best practices in internal loss data collection in Chapter 7.

External Loss Data Operational risk events that have occurred in the industry (but outside the firm) are very important in understanding the operational risk faced by the firm. Therefore, the collection and analysis of external loss data is a key element in an effective loss data program.

There are regulatory requirements regarding the use of external data in an advanced measurement approach, but the lessons learned from peers are valuable beyond those requirements. External data help inform risk and control self-assessment and scenario analysis and are often an important component in effective reporting.

We look at sources and uses of external loss data in Chapter 8.

Risk and Control Self-Assessment

The second of the four main building blocks of operational risk management activity is risk and control self-assessment (RCSA). Risks and controls are identified and assessed through RCSA, with a view to controlling and mitigating any unacceptable risks.

While loss data tells us what has already happened, RCSA is designed to help us to understand what risks we face today. Loss data are backward looking, but RCSA looks at risk levels now.

The RCSA might be the most important part of the framework because it addresses the requirements that we first looked at in Chapter 1. Those requirements are that the operational risk framework should *identify*, *assess*, *control,* and *mitigate* risk.

While loss data allow us to identify and assess risks that have occurred and to consider how to control and mitigate those risks in the future, RCSA allows us to identify all risks, not just those that have already materialized. Loss data is about hindsight. Risk and control self-assessment is about foresight. In Chapter 10, we look at various methodologies and best practices for RCSA.

Scenario Analysis

The third activity in the framework is scenario analysis. Unlike risk and control self-assessment, scenario analysis is only looking for rare, catastrophic risks. It is focused on identifying plausible risks that are so large as to be potentially fatal or severely destructive to a firm.

Scenario analysis stresses the operational risk framework and pushes participants to think outside their comfort zone. RCSA centers on discussions of the risks that are faced and the controls that are in place, whereas scenario analysis requires participants to consider what could happen if there is a serious failure of controls or a previously unassessed combination of risks.

Scenario analysis is a challenging area, and many firms struggle with meeting the regulatory requirements while retaining business value in the process. We look at alternative approaches to scenario analysis and the uses of scenario analysis in operational risk management and measurement in Chapter 11.

Key Risk Indicators

The final building block of operational risk data gathering is key risk indicators. Operational risk practitioners sometimes use the terms *key risk*

indicator and *metric* interchangeably; however, they are quite different. Metrics provide an important monitoring function across the framework and they can be attached to loss data and to risks or controls in risk and control self-assessment and can provide useful input to scenario analysis. Metrics also provide information for the business environment internal control factors that are required for an advanced measurement approach.

A key risk indicator predicts that a risk is changing and would allow for proactive intervention. It is difficult to find metrics that are true key risk indicators or can be combined to form a key risk indicator, because many metrics are simply counting exceptions or measuring performance, rather than measuring an increase or decrease in risk levels. We will consider the challenges of developing key risk indicators in Chapter 9, where we will also discuss best practices in metrics.

MEASUREMENT AND MODELING

Once the four data-gathering building blocks of loss data, risk and control self-assessment, scenario analysis and key risk indicators are in place, then operational risk can be measured and modeled.

An advanced measurement approach capital calculation requires the following four elements: internal loss data, external loss data, scenario analysis, and business environment internal control factors. The latter can be gathered from risk and control self-assessment and from key risk indicators. In Chapter 12, we consider the basic indicator and standardized and advanced measurement approaches to operational risk capital calculation.

REPORTING

All of the above elements feed into operational risk reporting. Without effective reporting, the operational risk framework is a factory that is busy making data widgets that are not used. Reporting gathers all of the information that has been collected and analyzed in the loss data program, the RCSA program, the scenario analysis program, the metrics program, and the capital modeling program and puts it to use.

The quality of reporting is critical to the success of an operational risk framework. Reporting that leaves its audience asking "so what?" is of little value. Reporting that asks its audience to think or say or do something is of great value.

In Chapter 13, we explore ways to provide reporting that is not data gathering, but instead provides risk analysis and risk transparency and that leads to better business decision making.

RISK APPETITE

Finally, the whole framework is held together by risk appetite. It is difficult, but not impossible, to express a risk appetite for operational risk. It often takes time for an operational risk framework to mature to the stage where risk appetite can be effectively discussed and agreed upon.

While governance is the first pillar or support for the framework, risk appetite is its partner. Effective governance requires a clear articulation of risk appetite, and risk appetite can be set only when strong governance is in place. In Chapter 14, we explore ways that a risk appetite can be set and applied for operational risk.

KEY POINTS

The main building blocks of an operational risk framework are:

- The foundations:
  - Governance
  - Culture and awareness
  - Policy and procedure
- The four data elements are:
  - Loss data collection, including
    - Internal loss data
    - External loss data
  - Risk and control self-assessment
  - Scenario analysis
  - Key risk indicators
- The key outputs are:
  - Measurement and modeling
  - Reporting
- The framework operates under the firm's stated risk appetite.

REVIEW QUESTIONS

1. Which of the following is least likely to be part of an operational risk framework?
   a. Loss data collection
   b. Risk and control self-assessment
   c. Counterparty credit assessment
   d. Scenario analysis

2. Which of the following is the *best* description of a robust operational risk framework?
   a. It collects all operational risk losses that occur within the firm.
   b. It provides effective tools to identify, assess, control, and mitigate operational risk.
   c. It produces a capital calculation of operational risk.
   d. It is based on a framework that has been successful at another firm.

NOTE

1. Sound Practices for the Management and Supervision of Operational Risk, Risk Management Group of the Basel Committee on Banking Supervision, 2011. Retrieved from www.bis.org/publ/bcbs195.pdf.

CHAPTER 4

Operational Risk Governance

This chapter addresses the regulatory requirements for operational risk governance and provides alternative governance approaches that can be adopted. The roles and responsibilities of the first, second, and third lines of defense are outlined, as well as the roles and responsibilities of boards of directors, risk committees, and senior management. Finally, validation and verification requirements are introduced and explained.

ROLE OF GOVERNANCE

Appropriate governance is essential for effective operational risk management, and the people who are responsible for ownership of the operational risk management program will be unable to make a positive impact without a robust governance structure. An effective governance structure must be implemented to provide oversight of operational risk management and measurement and to ensure an effective route for risk escalation.

Governance holds the framework together, as illustrated in Figure 4.1.

The governance approach adopted by a firm needs to reflect the culture of the firm and must be practical in nature. However, it is not unusual for the creation of an operational risk function to upset the current overall risk governance framework.

One of the main potential challenges in developing and implementing effective operational risk management is the sheer magnitude of the scope of coverage which touches virtually all activities and functions within an organization. Market, credit, and liquidity risk management evaluate the outcomes and consequences of transactions and other acts of commerce on profitability and balance sheet management.

Operational risk management, in turn, evaluates the outcomes and consequences of the organization's ability to perform and execute those risk management activities as well as all other operations, control and business

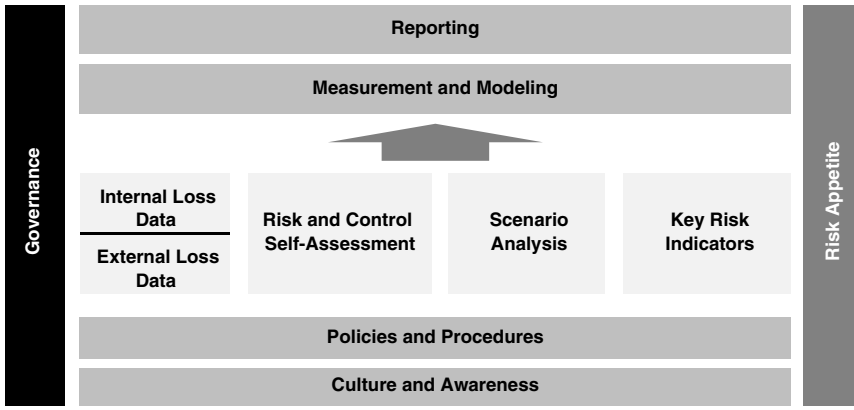

FIGURE 4.1 The Role of Governance in an Operational Risk Framework

functions on which the organization depends in order to remain viable and in business. Consequently, some changes beyond the visible lines of governance of operational risk might result.

To meet these challenges, the board of directors and senior management should treat operational risk management with the same level of stature, independence, and authority as the other core risk management disciplines such as market and credit. This core principle of equal stature has evolved steadily over recent years and has become most clearly articulated in various pronouncements by the Basel Committee on Banking Supervision.

The Basel Committee on Banking Supervision provided the "Principles for Enhancing Corporate Governance"[1] in 2010 and included guidance on the governance of risk, including:

> *Risk management and internal controls*
> - *A bank should have a risk management function (including a chief risk officer (CRO) or equivalent for large banks and internationally active banks), a compliance function and an internal audit function, each with sufficient authority, stature, independence, resources and access to the board;*
> - *Risks should be identified, assessed and monitored on an ongoing firm-wide and individual entity basis;*
> - *An internal controls system which is effective in design and operation should be in place;*
> - *The sophistication of a bank's risk management, compliance and internal control infrastructures should keep pace with any*

changes to its risk profile (including its growth) and to the external risk landscape; and

- *Effective risk management requires frank and timely internal communication within the bank about risk, both across the organization and through reporting to the board and senior management.*[2]

Therefore, a precursor for operational risk governance is the adoption of sound risk governance practices generally.

The Basel Committee on Banking Supervision updated its guidance on operational risk governance in its 2011 publication "Sound Practices for the Management and Supervision of Operational Risk."[3]

Sound internal governance forms the foundation of an effective operational risk management Framework. Although internal governance issues related to the management of operational risk are not unlike those encountered in the management of credit or market risk operational risk management challenges may differ from those in other risk areas.[4]

The role of the board and senior management in ensuring good governance is further expanded in Principles 3, 4, and 5 as follows:

Governance

The Board of Directors

Principle 3: The board of directors should establish, approve and periodically review the Framework. The board of directors should oversee senior management to ensure that the policies, processes and systems are implemented effectively at all decision levels.

Principle 4: The board of directors should approve and review a risk appetite and tolerance statement for operational risk that articulates the nature, types, and levels of operational risk that the bank is willing to assume.

Senior Management

Principle 5: Senior management should develop for approval by the board of directors a clear, effective and robust governance structure with well defined, transparent and consistent lines of responsibility. Senior management is responsible for consistently implementing

> and maintaining throughout the organization policies, processes and systems for managing operational risk in all of the bank's material products, activities, processes and systems consistent with the risk appetite and tolerance.[5]

The importance of ownership of operational risk by the board and by senior management is therefore clear, and the governance framework must reflect that ownership in the reporting structure and in the escalation of risk.

In addition, responsibility for good governance of operational risk lies in three lines of defense. These lines are generally considered to be the business, the corporate operational risk function and independent review by audit.

FIRST LINE OF DEFENSE

The first line of defense is the business line. The business owns operational risk and should be managing it as it arises. According to the Basel Committee on Banking Supervision:

> *This means that sound operational risk governance will recognize that business line management is responsible for identifying and managing the risks inherent in the products, activities, processes and systems for which it is accountable.*[6]

Each business line should have an operational risk function in place. The person responsible for operational risk in the business line may have a title such as business risk officer, nonfinancial risk officer, or operational risk manager. They need to maintain independence from the business and so need to have a reporting line that is at the top of the organizational structure. An appropriate reporting line would be to the head of the business or to their chief of staff or chief operating officer.

Business lines include support functions as well as revenue-generating areas. Therefore, there should be operational risk managers (or their equivalent) in operations, technology, finance, legal, compliance, and human resources as well as in any front office businesses such as fixed income, equities, retail banking, corporate banking, and so on.

The first line of defense operational risk managers might have a direct or dotted reporting line into the second line of defense. The larger and more complex the firm, the more likely it is that the first line of defense will be independent from the second line of defense.

SECOND LINE OF DEFENSE

The second line of defense is the corporate operational risk function. It is responsible for the development of the operational risk framework and reporting on operational risk matters to the firm's senior management and board of directors. The Basel Committee on Banking Supervision describes the corporate operational risk function and its relationship with the business line as follows:

> *A functionally independent corporate operational risk function (CORF) is typically the second line of defense, generally complementing the business line's operational risk management activities. The degree of independence of the CORF will differ among banks. For small banks, independence may be achieved through separation of duties and independent review of processes and functions. In larger banks, the CORF will have a reporting structure independent of the risk generating business lines and will be responsible for the design, maintenance and ongoing development of the operational risk framework within the bank. This function may include the operational risk measurement and reporting processes, risk committees and responsibility for board reporting. A key function of the CORF is to challenge the business lines' inputs to, and outputs from, the bank's risk management, risk measurement and reporting systems. The CORF should have a sufficient number of personnel skilled in the management of operational risk to effectively address its many responsibilities.*[7]

In order to meet this standard and to be able to effectively challenge the first line of defense and provide valuable reporting to the top of the house, there are two fundamental governance questions to consider for the second line of defense:

1. Who should own the operational risk function?
2. What should the operational risk function own?

Who Should Own the Operational Risk Function?

While it is critical that the board of directors and senior management demonstrate clear and unequivocal support for operational risk management, it cannot be effectively managed by "committee." Someone in the firm must be specifically accountable for the success of the operational risk function, or in other words, they must "own" the operational risk function.

The corporate operational risk function needs to report upward in such a way that it is endowed with three critical qualities: *independence*, *importance,* and *relevance*.

When selecting a governance structure for an operational risk function, or when reassessing the current governance of an existing operational risk function, these three qualities should be considered. The governance structure must support the *independence* of the operational risk function, it must bestow stature and *importance* of operational risk management and measurement and it must demonstrate their *relevance* to the organization. There are various options for the governance of operational risk, and each has practical and strategic advantages and disadvantages.

Option 1: Operational Risk Is Owned by the Chief Risk Officer This governance approach can be represented by the organization chart in Figure 4.2.

An operational risk function that reports directly to the chief risk officer (CRO) is in the fortunate position to be taken seriously by the rest of the organization. This governance structure best demonstrates the seriousness and commitment with which the board and senior management ensures that the operational risk function is *independent* from both the support and business functions, as it reports directly to the CRO. This reporting line also best reflects the aspirations of many supervisory and regulatory bodies domestically and internationally. In addition, the CRO is generally considered an *important* and highly *relevant* function in any firm, and the operational risk department can inherit these qualities in this governance structure.

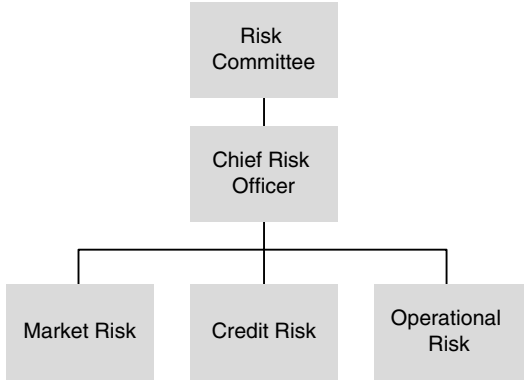

FIGURE 4.2 Example Governance Structure Where Operational Risk Is Owned by the Chief Risk Officer

The establishment of an independent CRO is recommended by the Basel Committee on Banking Supervision in its "Principles for Enhancing Corporate Governance"[8] as follows:

> ***Chief risk officer or equivalent***
>
> *Large banks and internationally active banks, and others depending on their risk profile and local governance requirements, should have an independent senior executive with distinct responsibility for the risk management function and the institution's comprehensive risk management framework across the entire organization. This executive is commonly referred to as the CRO. …*

The formal reporting lines and independence of the CRO is further outlined as follows:

> *Formal reporting lines may vary across banks, but regardless of these reporting lines, the independence of the CRO is paramount. While the CRO may report to the CEO or other senior management, the CRO should also report and have direct access to the board and its risk committee without impediment. Also, the CRO should not have any management or financial responsibility in respect of any operational business lines or revenue-generating functions. Interaction between the CRO and the board should occur regularly and be documented adequately. Non-executive board members should have the right to meet regularly—in the absence of senior management—with the CRO.*

The importance and relevance of the CRO is described as follows:

> *The CRO should have sufficient stature, authority and seniority within the organization. This will typically be reflected in the ability of the CRO to influence decisions that affect the bank's exposure to risk. Beyond periodic reporting, the CRO should thus have the ability to engage with the board and other senior management on key risk issues and to access such information as the CRO deems necessary to form his or her judgment. Such interactions should not compromise the CRO's independence.*
>
> *If the CRO is removed from his or her position for any reason, this should be done with the prior approval of the board and generally should be disclosed publicly. The bank should also discuss the reasons for such removal with its supervisor.*

A head of operational risk who reports to the CRO often enjoys opportunities to sit at the same table as his credit and market risk colleagues. This can help foster an environment where synergies between the risk categories can be identified and can provide the CRO with a more enterprise risk management view.

However, there are also potential disadvantages in this governance structure. In practice, operational risk can be overshadowed by market and credit risk if there is only one forum to present all risks at the same time. This can be especially significant if the CRO is from a market or credit risk background. Risk committee meetings can sometimes focus heavily on market and credit risk, to the detriment of operational risk, the latter being relegated to a five-minute briefing at the end of the meeting. A separate dedicated operational risk committee may be needed to overcome this problem. In other words, it may be necessary to augment this governance structure with additional reporting avenues for the operational risk function.

Another potential weakness of this governance structure is the distance it might create between operational risk and its related activities. An effective operational risk function needs to develop strong working relationships with the owners of the existing operational risk activities in the firm. An underlying principle, and a main goal of the Basel standards, is to ensure that operational risk management passes the "use test." This means that the firm's operational risk management policies, procedures, and tool sets are used by the practitioners who execute the day-to-day activities of the firm throughout its business, control, and support functions. These activities include Sarbanes-Oxley activities in the United States, the business continuity planning and information security teams, legal and compliance

EXAMPLE

Gamma Bank's management is considering changes in its business environment that might have an impact on all three risk categories. This structure facilitates the discussion in an integrative context, spanning market, credit and operational risk factors, and encourages transparency and communication between risk disciplines. The close working relationship between the risk functions can support an enterprise risk management (ERM) approach to risk.

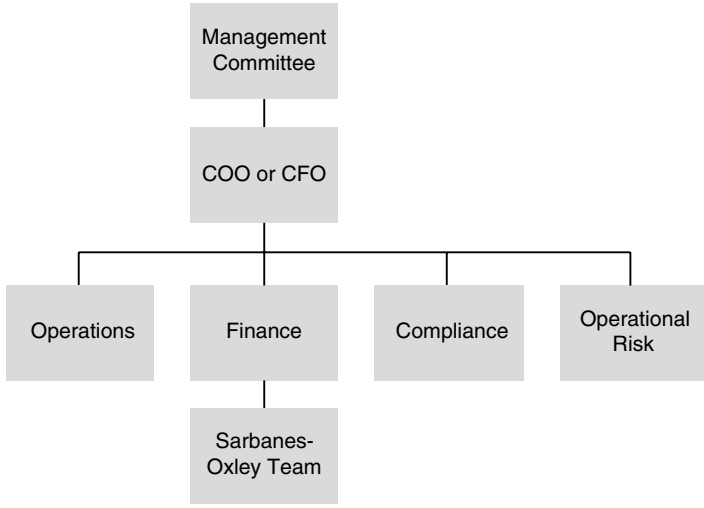

FIGURE 4.3 Example Reporting Structure Where Operational Risk Is Owned by Chief Operating Officer or the Chief Financial Officer

departments, and other support departments: operations, finance, and information technology. These functions will not report to the CRO, and it will require additional effort by the operational risk team to find and cultivate these partnerships.

Option 2: Operational Risk Is Owned by the Chief Operating Officer or the Chief Financial Officer This governance approach can be represented by the organization chart in Figure 4.3.

In the past, it was common for a firm-wide operational risk department to report to a senior executive such as the chief operating officer (COO), chief financial officer (CFO), or perhaps chief administrative officer (CAO). This structure may be viewed as imbedded in day-to-day operations and therefore not "independent." Consequently, it has been replaced in most firms by a CRO reporting line, but some do still maintain this type of governance structure. This alternative governance structure has its own advantages and disadvantages.

An operational risk function in such a structure has increased opportunities to partner with the other areas that own operational risks, such as legal and compliance, and the Sarbanes-Oxley team. In fact, the COO or CFO might mandate such working relationships.

EXAMPLE

If Gamma Bank's COO oversees both the compliance team and the operational risk team, then she is more likely to insist that there is an effective working relationship between them. This relationship can provide a path through the potential political challenges, such as possible conflicts and overlaps in roles and responsibilities that might otherwise arise.

As a result, such a governance structure raises the opportunity for governance, risk, and control (GRC) initiatives and GRC will be discussed in more depth later in Chapter 16.

The role of the COO, CFO, or CAO should provide the operational risk department with a good level of *importance* and *relevance*. However, this structure might weaken the operational risk department's *independence*. Significant levels of operational risk will exist within the departments that lie within the same reporting structure, and this may hinder the impartiality and objectivity of the operational risk department or at least tarnish the perception of its independence. Therefore, it is essential that in such a governance structure the operational risk department operates under clear policies and procedures that support its independence.

This governance structure also limits the opportunities for strong partnership with the market and credit risk functions, and therefore provides less opportunity for an ERM approach.

Option 3: Operational Risk Is Owned by the Chief Compliance Officer This governance approach can be represented by the organization chart in Figure 4.4.

In some firms, generally in smaller and less complex banks, the operational risk function reports directly into the compliance department. This is a more unusual arrangement, but for less complex institutions it has some advantages. There is a clear opportunity to partner closely with the compliance department and also to leverage the reporting cycles, regular meetings, and existing assessment activities that the compliance department may already have in place. The *independence* of the function can be well maintained in this structure.

The disadvantages of such an approach are that the operational risk function might be perceived to be out of touch with departments that do not usually interact with compliance. Part of the success of operational risk management is self-assessment and self-identification of

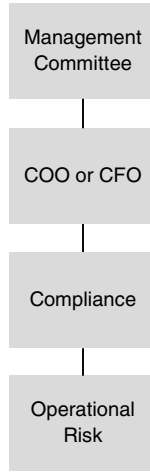

FIGURE 4.4 Example Reporting Structure Where Operational Risk Is Owned by Chief Compliance Officer

risk by the day-to-day business, operations, and support practitioners. Self-identification can be inconsistent with the way compliance departments function, and they might be viewed not as a trusted adviser, partner, or risk manager, but rather as a policing function. It may also be harder to demonstrate *importance* and *relevance*. As with the option where the operational risk is owned by the COO or CFO, partnerships with market and credit risk could be more challenging and an ERM approach would be difficult to achieve.

What Should the Operational Risk Function Own?

Once the upward reporting governance structure has been determined, the next challenge is to determine the right downward reporting structure for the corporate operational risk function. Who should report to operational risk, or what should operational risk own? There are many potential candidates. Whether a function can effectively report into operational risk will depend on several factors: the upward governance structure; the culture of the firm; the individual personalities involved; and the current maturity of the operational risk function in terms of its importance, relevance, and independence.

Following are areas that could report into a central operational risk function.

Other Operational Risk Teams Each business unit and support function should have its own first line of defense operational risk team. These teams may have been in place earlier than the corporate level function or may have been implemented as a result of the corporate level commitment to operational risk management. Unlike a corporate-level operational risk function, these teams can report to their own business head or support function head, as they are generally designed to assist that executive in managing the operational risk in their area.

They might also have a dotted line relationship with the corporate operational risk team. They certainly will have some reporting responsibilities to the corporate function, but often do not report directly to them, having at most a matrix reporting structure where they report into both their own division head, and the corporate operational risk head. An example of an appropriate reporting structure is shown in Figure 4.5.

Embedded Operational Risk Coordinators or Specialists or Managers The burden of rolling out an operational risk program usually results in a need for a designated operational risk coordinator, operational risk specialist, or operational risk manager in every department. If that department does not have an operational risk function of its own, then this designated individual provides a contact point for the central operational risk function.

An OR coordinator might be required to spend only a small percentage of their time on operational risk activities, and so may have another day job in which they report directly to a manager in their department. There should be a healthy and regular communication between the OR coordinator and the central operational risk team, as the OR coordinator will be the point person for the operational risk team as the operational risk framework is rolled out across the firm.

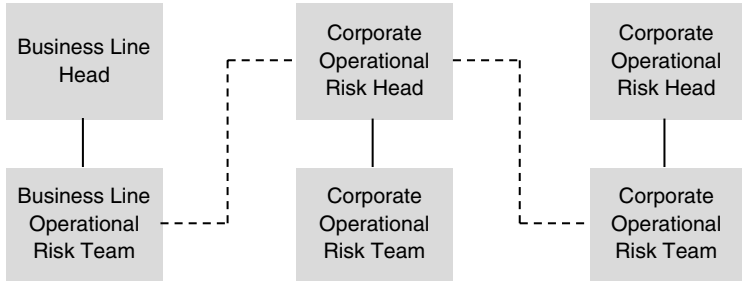

FIGURE 4.5 Operational Risk Team Reporting Structure

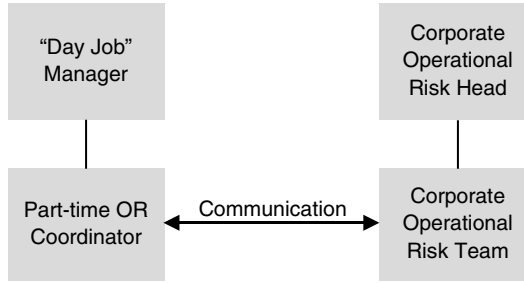

FIGURE 4.6 Operational Risk Coordinator Reporting Structure

Such a reporting structure is represented in Figure 4.6.

It can be useful to have such embedded resources also report to the central operational risk function, in a matrix fashion, but this is not essential. Such a reporting structure is represented in Figure 4.7.

The relationship between the central operational risk function and the OR coordinator can be informal and still be very successful.

Alternatively, there might be an OR coordinator who is working full time on operational risk activities in a particular department, and who reports directly to the central operational risk function. This can disrupt the clear independence between the first and second lines of defense, but might be sustainable if there are clear segregation of duties in place and policies to enforce them.

An example of the latter is shown in Figure 4.8.

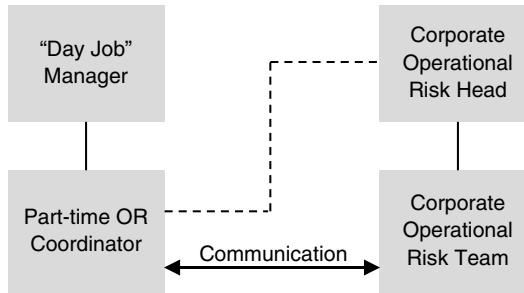

FIGURE 4.7 Operational Risk Coordinator Matrix Reporting Structure

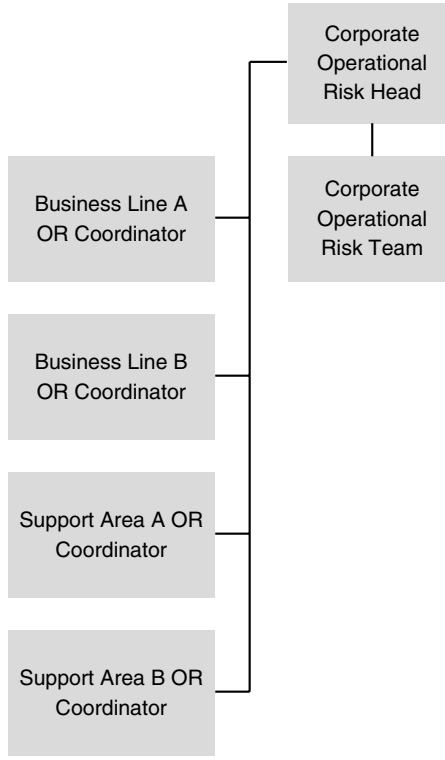

FIGURE 4.8 Embedded Independent Operational Risk Coordinator Reporting Structure

Business Continuity Planning (BCP) Business continuity planning (BCP) is often the most well-established preexisting operational risk function in a firm. BCP generally started life as an information technology function that focused on ensuring that the technology of the firm would continue to function in the case of a disaster. A lot of good BCP work came out of the response of firms to the 9/11 terrorist attack, and many BCP plans were significantly enhanced as a result of lessons learned at that time.

As a result, BCP often focused on disaster recovery plans for technology systems, ensuring that alternate backup sites, data, and systems were available should the main office be compromised for some reason.

Recently, BCP teams have expanded their role to cover other events that might disrupt the business, such as pandemic flu planning. The BCP plans developed for a pandemic raised some new considerations, such as how to

ensure business continuity if there were a high level of absenteeism (due to illness) and how to respond to social distancing requirements that might mean that a backup location was not a valid solution (often resulting in an enhanced remote computing contingency plan).

The activities of the BCP team fall squarely within the definition of operational risk: in particular two of the Basel II categories: Damage to Physical Assets and Business Disruption and System Failures.

For this reason, BCP might report into the corporate head of operational risk, and this is becoming more and more common in the financial services sector as firms recognize the synergies between the functions.

If there is no direct reporting line from BCP to operational risk, then a strong partnership is essential.

Information Security The information security function is endowed with the important task of preserving the confidentiality, availability, and integrity of the firm's data, whether it is electronic or otherwise. A failure in this area can result in a serious operational risk event, such as exposing confidential client data, compromising regulatory data compliance requirements or the loss of vital financial data. Many information security functions started out life in a technology department, where they were focused on protecting the security of the technology systems and data.

However, the information held in a firm is often also held in physical forms (such as paper), and the information security function usually provides policies and procedures for the safeguarding of these records also.

In order to effectively provide security for the firm's data, it is preferable for the function to sit outside of the technology department, as there may be a conflict between the technology department's needs and the information security departments concerns.

For this reason the information security function is often looking for an independent reporting line, and the operational risk function can provide this for them. Also, as information security risk is a subset of operational risk, it is appropriate to link these functions to ensure they effectively leverage each other's expertise and data.

For these reasons, several banks now have their information security function reporting into the operational risk head.

Sarbanes-Oxley Act The Sarbanes-Oxley Act (SOX) imposed operational risk management requirements regarding the accuracy of financial statements on U.S. publicly traded firms. SOX related activities are therefore a subset of operational risk. However, the SOX team often started in a separate area of the firm (usually in the finance department) and had specific deadlines and compliance requirements to meet. SOX work might

also predate the operational risk function, and the SOX team often exists separately from the operational risk team, with a different reporting line (perhaps to the CFO).

SOX assessments are conducted across the firm, and through these assessments risks and controls are identified and mitigating actions tracked to ensure compliance with SOX.

This overlaps with the risk assessment activities that will be conducted as part of the operational risk program, and for this reason many firms now have their SOX work incorporated into the operational risk function or have the SOX team report to the operational risk head.

In Chapter 16, we look at the ways that these SOX and operational risk activities can be combined in a GRC approach.

New Business Approval or New Product Approval Financial firms have new product programs that include policies, procedures, and processes to assess and facilitate the review of new products or businesses before they are launched. These new product approval processes require participants to consider all of the risks of the new product, including operational risk. New product approval provides a forum for discussions around the operational practicalities, accounting and tax practices, legal and regulatory requirements, and any other areas that should be addressed before launch.

The operational risk function sometimes administrates the new-product approval process, sometimes they are one of the required signatures for approval, and sometimes they might simply require that all other signatories consider operational risk when giving their sign-off.

Policy Office Many firms are establishing dedicated policy office functions to centralize and standardize firm-wide policies. The operational risk function will be a critical stakeholder in such a function, as they will be designing, mandating, approving, and monitoring policies that manage operational risk. In some cases, the operational risk function might have responsibility for the policy office, and it is embedded in the operational risk function.

The advantage of such an approach is that the operational risk unction will have a strong understanding of risk and control requirements and so can provide a strong hand in the development of appropriate and consistent policies.

In the past few years, we have seen a dramatic increase in regulators' interest in policies and procedures. A central repository and a standard template and approach are not just beneficial but are increasingly necessary in order to manage the myriad of regulatory requests regarding policies.

THIRD LINE OF DEFENSE

The third line of defense provides the final internal checks and balances for the operational risk framework. This third line is usually the internal audit function.

Audit

It is worth noting that the "Sound Practices" documents expressly forbid operational risk from reporting to the audit department. In the original 2003 "Sound Practices" document, it was simply stated as part of Principle 2:

> *The internal audit function should not be directly responsible for operational risk management.*[9]

In the 2011 "Sound Practices" document, this was further expanded with an in-depth description of the third line of defense responsibilities of audit.

> 16. *The third line of defense is an independent review and challenge of the bank's operational risk management controls, processes and systems. Those performing these reviews must be competent and appropriately trained and not involved in the development, implementation and operation of the Framework. This review may be done by audit or by staff independent of the process or system under review, but may also involve suitably qualified external parties. …*
> 18. *Internal audit coverage should be adequate to independently verify that the Framework has been implemented as intended and is functioning effectively. …*
> 19. *Internal audit coverage should include opining on the overall appropriateness and adequacy of the Framework and the associated governance processes across the bank. Internal audit should not simply be testing for compliance with board approved policies and procedures, but should also be evaluating whether the Framework meets organizational needs and supervisory expectations.*[10]

The audit function will measure the firm against the operational risk policies and procedures that are in place, and will measure the corporate operational risk function against its policies and procedures and its success in designing, maintaining, and monitoring an operational risk framework that meets the firm's regulatory requirements.

Validation and Verification

In June 2011, the Basel Committee on Banking Supervision published "Operational Risk—Supervisory Guidelines for the Advanced Measurement Approaches." This document has raised more third-line-of-defense challenges as it outlines complex validation and verification expectations as follows:

> 15. *Validation ensures that the ORMS [operational risk measurement system] used by the bank is sufficiently robust and provides assurance of the integrity of inputs, assumptions, process and outputs. Specifically, the independent validation process should provide enhanced assurance that the risk measurement methodology results in a credible estimate of operational risk capital that reflects the operational risk profile of the bank. The work of internal validation is not limited to quantitative aspects; it covers validation of data inputs, methodology and use of outputs of operational risk models.*
> 16. *Verification of the ORMF [Operational Risk Management Framework] is performed on a periodic basis and is typically conducted by the bank's internal and/or external audit, but may involve other suitably qualified independent parties from external sources. Verification activities test the effectiveness of the overall ORMF, consistent with policies approved by the board of directors, and also test ORMS validation processes to ensure they are independent and are implemented in a manner consistent with established bank policies.*[11]

In the June 2011 "Interagency Guidance on the Advanced Measurement Approaches for Operational Risk,"[12] the U.S. regulators made clear their request for an independent review outside the confines of the corporate operational risk function:

> *A bank's validation process must be independent of the advanced systems' development, implementation, and operation, or be subject to an independent review of its adequacy and effectiveness. As a general matter, a bank should ensure that individuals who perform the validation activities are not biased in their assessments due to their involvement in the development, implementation, or operation of the processes or products undergoing validation.*[13]

They also provided guidance on what they consider to be required validation activities:

> *Validation of a bank's AMA framework must include: (i) an evaluation of the conceptual soundness of the advanced systems (including developmental evidence supporting the advanced systems), (ii) an ongoing monitoring process that includes verification of processes and benchmarking, and (iii) an outcomes analysis process that includes back-testing.*[14]

Firms have been struggling with how best to respond to these *validation* requirements as they are not specifically in the hands of audit. Some firms have established a validation function that is independent from the rest of the corporate operational risk function and which validates the quantitative and qualitative elements of the framework.

An annual validation program is now in place in several of the firms that have more mature operational risk frameworks. This annual process may include a comparison of data between work streams, for example, comparing loss data to risk and control assessment, and a review of policies and procedures, for example, reviewing committee activities minutes to ensure compliance.

Some firms are also looking at developing rolling validation programs that continuously examine the accuracy and completeness of data.

Verification is similar to the usual role of audit and so, while it requires careful compliance, is causing less confusion.

RISK COMMITTEES

The risk committee structure that is put in place for the escalation and management of operational risk will reflect the first- and second-line-of-defense governance choices made by the firm.

The 2011 "Sound Practices" document provides the following guidance:

> *When designing the operational risk governance structure, a bank should take the following into consideration:*
>
> *(a) Committee structure—Sound industry practice for larger and more complex organizations with a central group function and separate business units is to utilize a board-created enterprise level risk committee for overseeing all risks, to which a management level operational risk committee reports. Depending on the nature, size and complexity of the bank, the enterprise level risk committee may receive input from operational risk committees by country, business*

or functional area. Smaller and less complex organizations may utilize a flatter organizational structure that oversees operational risk directly within the board's risk management committee;

(b) Committee composition—Sound industry practice is for operational risk committees (or the risk committee in smaller banks) to include a combination of members with expertise in business activities and financial, as well as independent risk management. Committee membership can also include independent non-executive board members, which is a requirement in some jurisdictions; and

(c) Committee operation—Committee meetings should be held at appropriate frequencies with adequate time and resources to permit productive discussion and decision-making. Records of committee operations should be adequate to permit review and evaluation of committee effectiveness.[15]

An example of a risk committee structure that would allow for operational risk to be escalated through the organization is shown in Figure 4.9.

FIGURE 4.9 A Sample Risk Committee Structure

In this example the business lines have their own operational risk committees, and separate committees exist for operational risk-related functions in the firm.

Often, many of these committees have different reporting paths up to the board. In those situations, it is important that operational risks are being consistently represented through the various paths that exist.

The board is required to periodically review and approve the framework and the committee structure can facilitate that process, for example, by requiring risk committee and then board approval as a final step in the validation and verification procedures.

KEY POINTS

- Boards of directors and senior management have specific accountability for operational risk management, including setting appetite and approving frameworks.
- Good governance requires three lines of defense: the first line is the business, the second line is the corporate operational risk function, and the third line is usually the audit function.
- Validation and verification activities must be put in place to ensure the integrity of the operational risk framework and data.
- A risk committee should be established to facilitate risk escalation and framework approval.
- Firms adopt governance structures that meet their business needs and their regulatory requirements locally and globally.
- There are advantages and disadvantages in each governance approach. Some promote Enterprise Risk Management (ERM), while others promote Governance, Risk and Compliance (GRC) strategies.

REVIEW QUESTIONS

1. Which governance structure is most likely to foster an enterprise risk management view?
   - **a.** The operational risk department is part of the compliance department.
   - **b.** The operational risk department reports to the Chief Risk Officer.
   - **c.** The operational risk department reports to the Chief Financial Officer.
   - **d.** The operational risk department reports to the Chief Operating Officer.

2. Which of the following are requirements of a strong governance structure?
   - **I.** There are first, second, and third lines of defense.
   - **II.** The first line of defense is in the business line.
   - **III.** The second line of defense is independent from the first line.
   - **IV.** The second line of defense is owned by the audit function.
   - **V.** The third line of defense is owned by the business.
     - **a.** I and II only
     - **b.** I, II, and III only
     - **c.** **I, II, and IV only**
     - **d.** I, II, and V only

NOTES

1. Basel Committee on Banking Supervision, "Principles for Enhancing Corporate Governance," October 2010. Retrieved from www.bis.org/publ/bcbs176.pdf.
2. Ibid., section 3.
3. Risk Management Group of the Basel Committee on Banking Supervision, "Sound Practices for the Management and Supervision of Operational Risk," 2011. Retrieved from www.bis.org/publ/bcbs195.pdf.
4. See note 3, section 12.
5. See note 3, section 14.
6. See note 3, section 15.
7. Ibid.
8. See note 1, sections 71–74.
9. See note 3.
10. Ibid., sections 16 and 18.
11. Basel Committee on Banking Supervision, "Operational Risk—Supervisory Guidelines for the Advanced Measurement Approaches," June 2011. Retrieved from www.bis.org/publ/bcbs196.pdf.
12. "Interagency Guidance on the Advanced Measurement Approaches for Operational Risk," June 2011. Retrieved from www.occ.gov/news-issuances/bulletins/2011/bulletin-2011-21a.pdf.
13. Ibid., p. 10.
14. Ibid.
15. See note 3, section 37.

CHAPTER 5

Culture and Awareness

This chapter explores the challenges of bringing about successful culture change that supports an effective operational risk framework. It considers planning, marketing and communication, training, and sponsorship. In addition, this chapter investigates the "use test" requirements of operational risk regulation and explores how activities that change the culture can contribute to meeting the required standards.

WINNING OVER THE FIRM

With a strong governance structure in place, an operational risk function can turn to the important next step: winning over the organization. The time invested in culture and awareness activities is indicative of the likely success of the framework. To be successful, operational risk must be identified, assessed, monitored, controlled, and mitigated across the firm, and this can be achieved only through an energized organizational change program.

The operational risk framework must be designed to reflect the culture of the firm. An approach that is a roaring success in one firm will fall flat in another. Even the best-designed framework needs to be promoted and communicated in order for operational risk management to be adopted and applied throughout the organization. To achieve this, the operational risk function should undertake three important activities—marketing, planning, and training—before it attempts to implement the other elements of the framework.

The role of culture and awareness in underpinning a sound operational risk framework is illustrated in Figure 5.1.

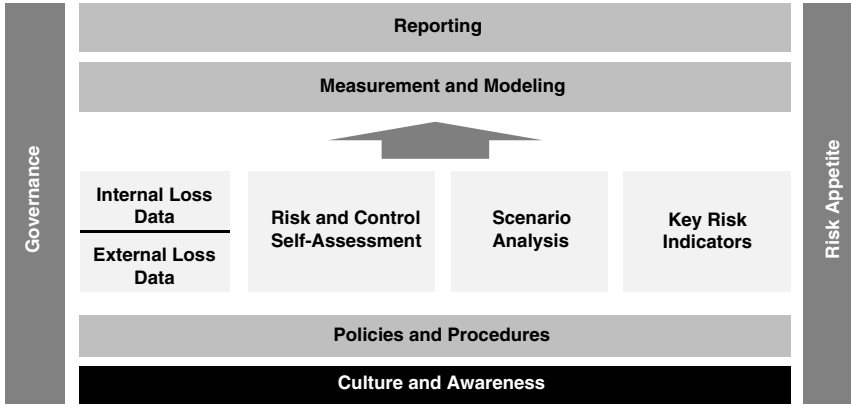

FIGURE 5.1 The Role of Culture and Awareness in an Operational Risk Framework

MARKETING AND COMMUNICATION

Every function in a firm has its own brand, whether it has invested any effort into cultivating that brand or not. Each function has a reputation, either good, bad or between the two, and this reputation is key to whether the function can achieve its goals. If the operational risk function is seen as a trusted partner, it will be able to progress more quickly toward its goals. If it is an unknown or misunderstood department, then its goals may be frustrated at every turn.

Colleagues, peers, managers, and employees will have formed an opinion of whether this function is one with which they want to work. If they have never heard of the department, there is even more work to do.

Unlike most departments, the operational risk function needs to work with everyone in the firm, as operational risk can arise in every nook and cranny of the organization. To build those working relationships, a firm-wide marketing effort is needed at the launch of the department, and also at every major rollout of the framework.

The firm might have a well-established approach to launching new initiatives, possibly through poster campaigns, e-mail blasts, or town halls. Whatever works well can be leveraged, and if there is nothing to leverage, new approaches can be tried. In fact, new methods of communication tend to draw notice, and so can even be preferable to the standard methods.

In addition to these internal marketing methods, it is important to allow time for face-to-face meeting with all of the key stakeholders. During those

meetings it can be helpful to ask "what are you hoping we will do?" and "what are you hoping we will not do?" The answers to those two questions provide insight into the current perceptions held about operational risk, both as a function and as a discipline. In addition, the answers to those two questions provide an opportunity to find and leverage mutual goals and aspirations. Armed with the answers to these questions, formal and informal marketing campaigns can be designed to ensure that the following minimal goals are met:

1. The organization knows what operational risk is.
2. People know what to do when they see it.
3. Managers are aware of the benefits of good operational risk management.
4. Managers are aware of the dangers of poor operational risk management.
5. Main supporters are identified and there is a plan for how to leverage that support.
6. Main protagonists are identified, and there is a plan to win them over.

The efforts taken in promoting cultural awareness and developing a relationship with key stakeholders are recouped later in reduced political roadblocks and improved support for operational risk management activities.

A framework that is technically excellent, but which has little organizational support, will never endure and will not succeed in ensuring that operational risks are identified, assessed, controlled, and mitigated. A framework that is built on a bedrock of strong culture and awareness can continue to evolve and mature as experience develops. That development will ensure that risk identification, assessment, control, and mitigation is continuously occurring and improving.

TRAINING

If operational risk is to be managed effectively in every corner of the firm, then it may be beneficial to roll out firm wide training in addition to a general announcement e-mail or town hall.

There are many ways to deliver effective training, and the type of training should reflect the culture of the firm. Training can be efficiently delivered to all employees using the intranet. If the firm already has an online training program then an operational risk training module could be added to that. If possible, everyone should be invited to complete the most basic training, with more in depth training for those who might be involved in specific activities.

A basic training module can facilitate cultural change in the firm, educating employees on the importance of operational risk management, and explaining the role of the operational risk team and any operational risk coordinators, specialists, or managers. There is no need for basic training to be overambitious. It can be short and to the point. For example, the goal of basic training could simply be to make employees aware of operational risk, and make sure they know what to do when they see it.

Additional in-person and group training will be needed for the practical implementation of the elements of the framework. For example, before a loss data collection program is launched, it will be necessary to train everyone who will be involved in entering losses. There are many considerations when entering an operational risk loss event, and these are addressed in Chapter 7. Without adequate training, the integrity of the data is likely to be compromised.

Similarly, training will be needed before any risk and control self-assessment (RCSA) activities are launched. There are multiple sources of expertise to assist with the design and roll-out of training. The firm may have its own training and development function that can assist with this or might even manage it entirely.

Possible topics for introductory operational risk awareness training are:

- What is operational risk? (Definition and examples)
- Why should we manage it? (Examples of operational risk events)
- What should I do when I see it?

There are some key success criteria for good training, which should be incorporated into the training design and delivery, including:

- Setting clear learning objectives and being sure to cover them adequately.
- Having realistic expectations of the learning curve of the trainees.
- Providing feedback so that trainees are comfortable that they have mastered the materials.

PLANNING

Planning can make or break an operational risk function. Good planning involves setting clear goals, realistic milestones, and achievable deliverables that add value. Publishing milestones beforehand, and then meeting them on time, builds the positive reputation of the function.

An operational risk framework is a complex and evolving challenge, and to keep its development under control it is important to apply strong project management skills to the design and implementation of each new element. It is good to plan for short-term and long-term goals so that the function can demonstrate its current successes, as well as its long-term importance to the firm.

Once the elements of an operational risk framework are up and running, they need to be monitored to ensure that they maintain their integrity and do not deteriorate over time. Indeed, an operational risk framework should continue to evolve with experience and in response to feedback from participants, partners, and sponsors. The validation and verification requirements introduced in Chapter 4 are important elements in ensuring that the framework continues to be embedded in the organization and that the quality and integrity of operational risk activities are maintained.

Poor planning can seriously tarnish the image of the department as it can lead to promises that are not kept and deadlines that slip. Every day spent planning is a solid investment in a successful framework and protects the brand of the function within the firm.

MAJOR DELIVERABLES CHECKLIST

In the early stages of an operational risk framework, progress against the deliverables of an implementation plan might be represented in several ways. One method to demonstrate progress is to have a simple checklist of implementation activities completed and pending. For example, the main deliverables that the implementation of an operational risk framework could include are listed below. These deliverables will be further explained in future chapters, but they are included here to provide a useful planning list of the major deliverables of an implementation plan for a new operational risk framework. They are not listed in chronological order, and the order of implementation can depend on the organization and the preferred approach to each area.

Governance

- ☐ First-line-of-defense operational risk managers established:
  - ☐ In all front office areas
  - ☐ In all support areas

(*Continued*)

- ☐ Second-line-of-defense corporate operational risk function established:
  - ☐ Reporting lines established
  - ☐ Team hired
- ☐ Audit has confirmed ownership of third line of defense.
- ☐ Operational Risk Committee(s) established.
- ☐ Board has acknowledged review and approval responsibility.
- ☐ Senior management has confirmed ownership of operational risk framework.
- ☐ Validation and verification program has been established.

Culture and Awareness

- ☐ Introductory meetings with senior management team completed.
- ☐ Marketing strategy developed and approved.
- ☐ Marketing activities kicked off (e.g., town hall or e-mail blast).
- ☐ Training strategy developed and approved.
- ☐ Operational risk awareness training delivered.
- ☐ All employees trained.

Policy and Procedures

- ☐ Firmwide operational risk policy established and approved by board.
- ☐ Loss data procedures established.
- ☐ RCSA procedures established.
- ☐ Scenario analysis procedures established.
- ☐ Metrics or key risk indicator procedures established.
- ☐ Validation and verification procedures established.
- ☐ Modeling procedures established.
- ☐ Reporting procedures established.
- ☐ Taxonomies established:
  - ☐ Risk taxonomy
  - ☐ Control taxonomy
  - ☐ Organizational taxonomy

Loss Data Collection

- ☐ Internal loss data standards established.
- ☐ Internal loss data procedures established.
- ☐ Internal loss data system implemented:
  - ☐ Business requirements gathered
  - ☐ System specifications complete

- ☐ Development complete
- ☐ Pilot complete
- ☐ System rolled out

☐ Internal loss data training designed and delivered:
- ☐ To front office
- ☐ To support areas

External Loss Data Collection

☐ External loss data sources established:
- ☐ Membership in consortium obtained
- ☐ Subscription(s) to external data sources established

☐ External loss data procedures established.
☐ External loss data system developed (if needed).
☐ External loss data trained designed and delivered as needed.

Risk and Control Self-Assessment

☐ RCSA procedures established.
☐ RCSA system implemented:
- ☐ Business requirements gathered
- ☐ System specifications complete
- ☐ Development complete
- ☐ Pilot complete
- ☐ System rolled out

☐ RCSA training designed and delivered.
☐ RCSA calendar established.
☐ RCSA program kicked off.
☐ RCSA first run results gathered.
☐ RCSA results validated.
☐ RCSA mitigation action tracking established.
☐ RCSA lessons learned gathered.

Scenario Analysis

☐ Scenario analysis procedures established.
☐ Scenario analysis system implemented:
- ☐ Business requirements gathered
- ☐ System specifications complete
- ☐ Development complete
- ☐ Pilot complete
- ☐ System rolled out

(*Continued*)

- ☐ Scenario analysis training designed and delivered.
- ☐ Scenario analysis calendar established.
- ☐ Scenario analysis program kicked off.
- ☐ Scenario analysis first run results gathered.
- ☐ Scenario analysis first run output provided to modeling team.
- ☐ Scenario analysis first run results validated.
- ☐ Scenario analysis mitigation action tracking established.
- ☐ Scenario analysis lessons learned gathered.

Key Risk Indicators (KRIs) or Metrics

- ☐ KRI standards established.
- ☐ KRI procedures established.
- ☐ KRI system implemented:
  - ☐ Business requirements gathered
  - ☐ Data sources identified
  - ☐ System specifications complete
  - ☐ Development complete
  - ☐ Pilot complete
  - ☐ System rolled out
- ☐ KRI training designed and delivered.
- ☐ KRI program kicked off.
- ☐ KRI first run results gathered.
- ☐ KRI results validated.
- ☐ KRI lessons learned gathered.

Capital Modeling

- ☐ Operational Risk capital modeling approach developed and approved.
- ☐ Operational Risk capital modeling procedures established.
- ☐ Capital modeling system implemented:
  - ☐ Business requirements gathered
  - ☐ Data sources identified
  - ☐ System specifications complete
  - ☐ Development complete
  - ☐ Pilot complete
  - ☐ System rolled out
- ☐ First run of capital model complete.
- ☐ Capital model validated.

Reporting

- ☐ Reporting procedures established.
- ☐ Reporting designed and implemented for the board, for senior management, for the front office, and for support functions including:
  - ☐ Loss data
  - ☐ RCSA
  - ☐ Scenario analysis
  - ☐ KRI
  - ☐ Capital

Risk Appetite

- ☐ Risk appetite methodology agreed.
- ☐ Risk appetite incorporated into reporting.
- ☐ Risk appetite incorporated into policy.
- ☐ Risk appetite incorporated into training.
- ☐ Risk appetite incorporated into procedures.

Alternatively, progress against the initial implementation plan may be represented in a milestones project chart as illustrated in Figure 5.2. (This example includes a project line for the development of a global OR system, including a request for information [RFI] and a request for proposal [RFP] from software vendors.)

Once an operational risk framework is implemented, the program should move from a project management phase into a business as usual phase. Once a program moves into business as usual it will be important to establish effective tracking and monitoring of repeating deliverables. This will be necessary not just from a practical management point of view, but it will also provide documented evidence of the program's continuous activities. This evidence will be useful to regulators and auditors in assessing the effectiveness of the framework.

THE "USE TEST"

The "use test" is a regulatory standard that requires a bank to show that risk management standards are being used across the firm to support management decision making.

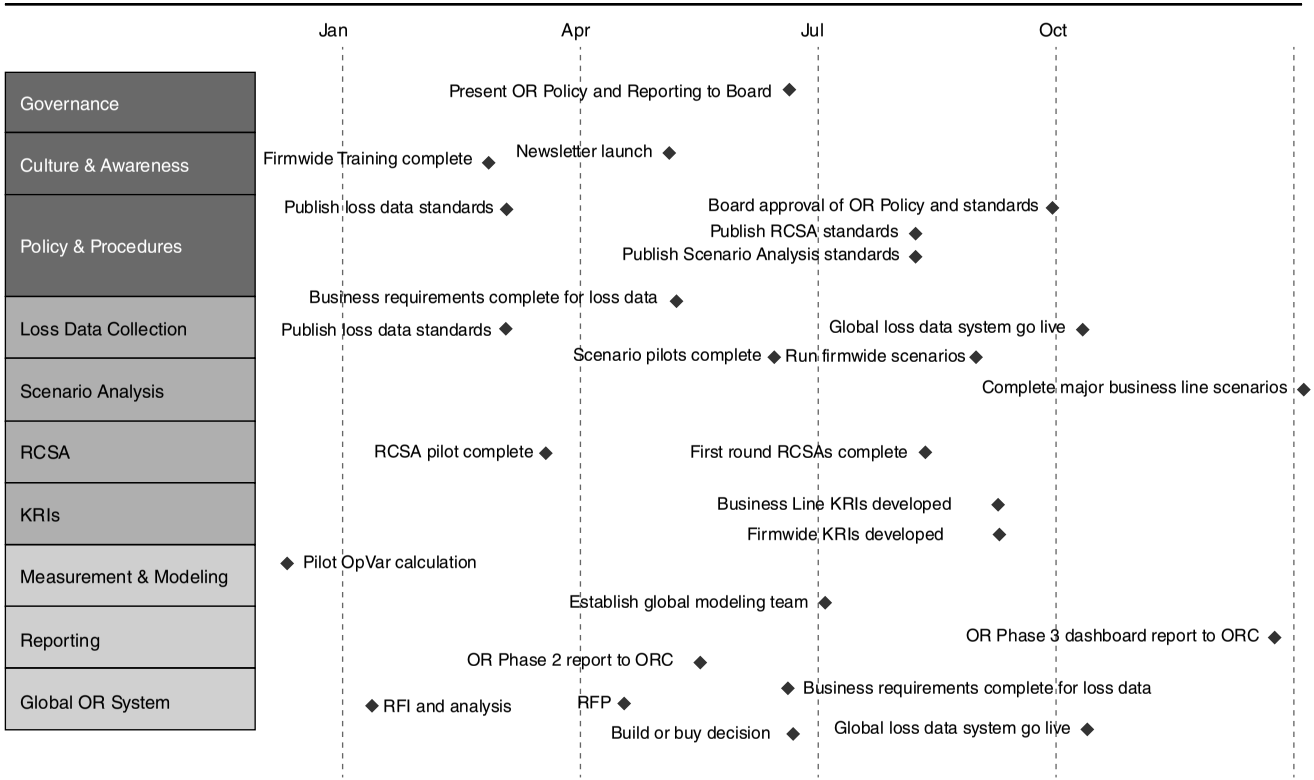

FIGURE 5.2 Sample Project Milestones for an Operational Risk Implementation Plan

The Basel Committee on Banking Supervision has established how an advanced measurement approach bank can demonstrate that the operational risk framework is embedded and effective and so meets the use test. In June 2011, the Committee published "Operational Risk—Supervisory Guidelines for the Advanced Measurement Approaches." In this document, the use test is described as follows:

> *A bank may use various approaches to articulate and demonstrate the integrated use of its ORMF [Operational Risk Management Framework]. …*
>
> *The level to which the broader ORMF processes and practices have been embedded at all organizational levels across a bank is referred to as "embeddedness."…*
>
> *A bank should have sustainable and embedded ORMFs and policies that are used in its risk management decision-making practices, with clear evidence of the integration and linkage between the measurement and management processes of the ORMF through the entire institution.*[1]

There are several ways in which this "embeddedness" must be demonstrated according to the Guidelines. First, operational risk must be a key factor in the bank's strategic and business planning processes. Second, the board should approve an operational risk appetite and tolerance statement and there should be controls in place to stay within that appetite (which is considered more fully in Chapter 14).

Third, the business units must be able to demonstrate how they are using the operational risk framework to inform their decision making. The Guidelines also provide details of how reporting can be used to meet the use test requirements, but the important cultural aspects for consideration in this chapter are the first and the third points above.

It is not enough to have a corporate operational risk framework, and it is not enough to have an engaged board of directors. Senior management and the business units must demonstrate that they use their knowledge and awareness of operational risk and appropriate risk measures when making business decisions.

The role of culture and awareness in the framework is vital to meeting this requirement. The business units need to analyze their own operational risk outputs when making decisions. Therefore, operational risk should be under consideration when a business decides to take on a new product, exit a region, expand their workforce, or change their strategy, for example. Operational risk management and measurement need to become an integral part of a business's management practices.

By engaging the business in the early development stages of the operational risk framework, and by training them carefully and comprehensively, the corporate operational risk function can assist the business unit in meeting this regulatory requirement. Simply put, do they genuinely use operational risk information in their decision making? A well-constructed, -documented, and -managed operational risk framework should supply them with the data that they need to be both meet this requirement in practice and to be able to demonstrate to a regulator or auditor how they have met this requirement.

The loss data, RCSA, and KRI elements that the businesses gather through their first-line-of-defense operational risk program can and must be integrated into their day-to-day decision-making processes. Scenario analysis, capital modeling, and firm-wide risks can also provide color to decisions and can be provided to them by the second line of defense, the corporate operational risk function.

The use test is taken seriously by regulators. Often, it results in their going directly to a business unit to see how they are participating in the operational risk framework and to review documented evidence of how they incorporate operational risk considerations into their business decision making. It is no surprise that a regulator is most satisfied if a business can demonstrate that it reached a "no" decision based on an operational risk level that it found unacceptable or a "yes" decision based on careful consideration of the risk metrics and potential risk losses.

The implementation of an operational risk framework is likely to require significant organizational change. This can be achieved through proactive marketing, careful planning, excellent training, and an energized enthusiasm from the operational risk team. The business also needs to fully embrace operational risk management and measurement in order to ensure it is truly "embedded" in the firm.

KEY POINTS

- The use test requirements mean that the firm must be able to demonstrate that operational risk management and measurement is "embedded."
- "Embeddedness" is considered successful if the business unit is using operational risk as a key input into its decision-making processes, the board is fully engaged, senior management are fully engaged, and reporting is effective.
- Effective internal marketing, planning and training activities are essential in order to successfully embed an operational risk function in a firm.

REVIEW QUESTION

1. Which of the following are elements of the Basel II definition of "embeddedness"?
   - **I.** Operational risk is a key factor in the bank's strategic and business planning processes.
   - **II.** The board has approved the Operational Risk appetite.
   - **III.** The business units are able to demonstrate how they are using the operational risk framework to inform their decision making.

   a. I and II only
   b. I, II, and III
   c. I and III only
   d. III only

NOTE

1. Basel Committee on Banking Supervision, "Operational Risk—Supervisory Guidelines for the Advanced Measurement Approaches," June 2011. Retrieved from www.bis.org/publ/bcbs196.pdf, sections 17–18.

CHAPTER 6

Policies and Procedures

This chapter explores the important role of strong policies and procedures in an effective operational risk framework. It also considers the role of standards and guidelines documents. Example content is provided for an operational risk policy, as well as samples from procedures, standards, and guidelines.

THE ROLE OF POLICIES, PROCEDURES, GUIDELINES, AND STANDARDS

In recent years, financial services firms have embraced the importance of having clearly articulated and consistently documented policies, procedures, standards, and guidelines. These written documents serve to articulate the firm's interpretation of rules and regulations, and their chosen approach to meeting those requirements.

It has become clear that it is necessary to have objective goals against which to measure performance. Well-documented policy and procedure documents can help to meet this need. Firms have also learned the sometimes painful lesson that good documentation is needed in order to demonstrate that regulatory requirements have been incorporated into the business processes of the firm.

Policies and procedures form an essential foundation for a successful operational risk framework, as is illustrated in Figure 6.1.

As well as continuously improving the content of such documents, many firms have sought efficiency improvements for their documentation. The rapidly increasing level of regulatory scrutiny and the associated increase in regulatory examinations has made it necessary for firms to streamline and standardize their approach to policies and procedures.

Some have developed centralized policy functions and have even written a "policy on policies" that requires standard templates, minimum content,

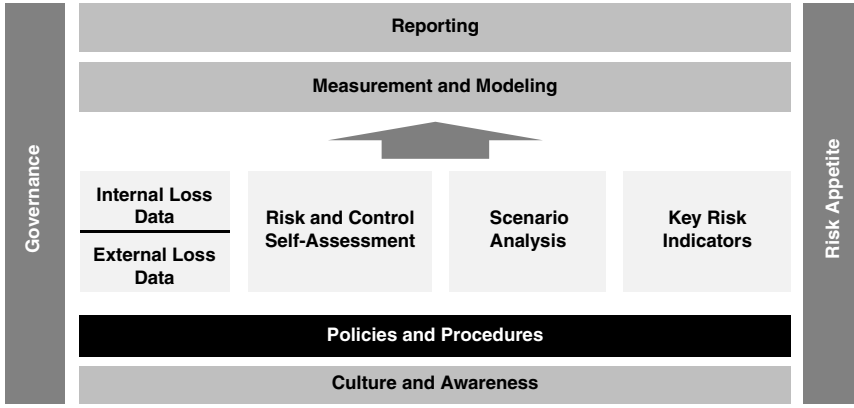

FIGURE 6.1 Policies and Procedures in an Operational Risk Framework

and appropriate approval processes for policies and for procedures. While this may sound overly complex, it can ultimately reduce the effort needed to create and maintain a policy library. With clear guidance on what is and is not appropriate in a given document, employees have an easier time creating material that is useful, implementable, and meets both management's and regulator's expectations.

Different firms define the terms *policy* and *procedure* differently and some also have separate *standards* and *guidelines* documents. Whatever approach is taken, is important for firm's to be clear about what they mean by each of these terms.

The New York–based Finance Industry Policy Forum has recently proposed the following definitions for policy and procedure:

Proposed Definition of "Policy"

Policy establishes minimum requirements and controls to address business strategy, compliance with law, rules, regulations; mitigation of other identified risks. Policies must be actionable and enforceable.

Proposed Definition of "Procedure"

Procedures are specific instructions for implementing a policy or performing a task, and may include such things as examples, scenarios, links, job aids, Q&As.

Standards usually set the minimum requirements that need to be met with the procedures. Guidelines offer supporting guidance on methods that might be used, rather than requirements.

An analogy using cars may be helpful in understanding the differences between these related documents. A policy may state that you must drive safely, including obeying required speed limits. The standards vary from country to country as the top speed limit is 55 or 65 miles per hour on most highways in America, but is 130 kilometers an hour on motorways in France. How you accelerate or decelerate is outlined in your car procedure manual, which provides the step-by-step instructions for how to use the gas pedal (accelerator) and the brake. When approaching a corner, you may see a chevron sign that indicates that this is a tight corner—this is a guideline, encouraging you to consider lowering your speed, but not requiring it.

Simply put, policy usually outlines *why* something should be done, standards establish *what* specific criteria need to be met, and procedures and guidelines outline *how* it should be done.

The relationship between regulation and the four categories of documentation can be represented as shown in Figure 6.2.

When authoring each document, care needs to be taken to ensure that it meets the requirements contained in documents that lie further up the pyramid.

A firm may combine policies and standards. However, policies generally require senior management approval, and so it can be helpful to keep standards separate so that full senior management approval is not needed if the standards change. A firm might also combine procedures and guidelines and will often incorporate certain principle statements into the policy document.

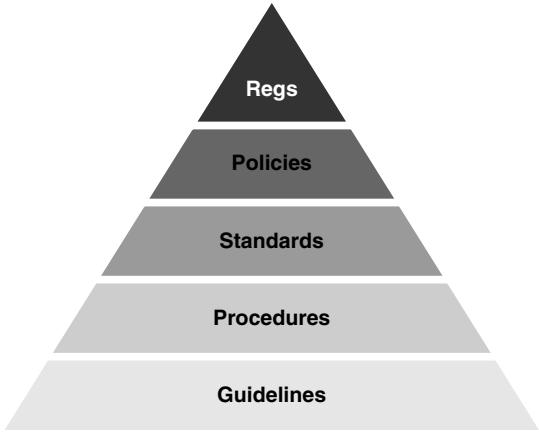

FIGURE 6.2 Policy Documentation Hierarchy

BEST PRACTICES

The volume of regulatory interest in policies and procedures has led to significant improvements in the authoring of policies and procedures, as well as in the associated review and approval processes. These improvements include the use of standard templates, the establishment of an indexed and searchable central repository for the documents, and the implementation of a robust version control process.

Some firms allow regulators direct access to their policy portals, thereby bringing more efficiency and transparency to their relationship. This approach can ease some of the pain of examinations and ensures accuracy and consistency in responses to regulatory requests.

As firms attempt to improve their policy approval processes they sometimes find that they need to adjust their committee structures and governance frameworks as a result. Policies are tightly linked to governance, and when policies are well designed, approved, implemented, and monitored, this provides evidence of strong governance.

The practicalities of publishing policies, standards, policies, and procedures will depend on the culture of the firm. If the culture of the firm requires strong consensus, then a lot of work will be needed to ensure that all key stakeholders are engaged in development and implementation. If the culture requires senior management approval for all major documents, then an appropriate and efficient approval workflow must be put in place.

The operational risk framework will need supporting policies, standards, procedures, and guidelines. Audit will measure the firm against these, the regulators will look to them to ensure that the framework is well designed, and the firm will need them to ensure consistent implementation of the framework.

OPERATIONAL RISK POLICY

Firstly, there needs to be an operational risk policy. This might be part of the overall risk policy, or it may stand alone. The policy should be approved by the board and include:

- The firm's definition of operational risk.
- The firm's approach to operational risk governance.
- A description of the main activities and elements of operational risk, including the roles and responsibilities of the participants.

The policy might also include information on each of the elements of the program, or these might be covered in lower level procedure documents if they are likely to be subject to change. Policy documents usually require a

formal sign-off process from the firm's risk committee or similar governance structure, and possibly also from the board. Therefore, the policy should be written at an appropriate level—not so high level that it provides no guidance, and not so low level that it requires formal amendment every time the operational risk framework evolves.

Policies, standards, procedures, and guidelines should cover the minimum requirements for the loss data program, the RCSA program, the scenario analysis program, and the KRI program. There may be additional procedures needed for validation and verification activities and for the capital model. These documents should clearly state the roles and responsibilities of those involved and should not be aspirational. That is to say, if something is not yet in place, it should not be a requirement.

Some regulators are comfortable with the inclusion of certain aspirational aspects, as long as there is also a stated plan for how and when that future state will be achieved.

SAMPLE OPERATIONAL RISK POLICY

Figure 6.3 is an example of a possible Operational Risk Policy.

Drafted: 12/12/12 Revised: 1/3/13 Version: 2.5

PURPOSE

The management of operational risk is a vital activity within the firm. The firm is subject to Basel II and must therefore implement an operational risk framework that meets the Basel II requirements. In addition, there are strong business drivers for effective operational risk management. This policy outlines a framework that meets both the regulatory and business requirements.

DEFINITION

The firm's definition of operational risk is "the risk of loss resulting from failed or inadequate people, process, systems and external events." This definition includes legal risk. This definition excludes strategic and business risk. Reputational risk will also be managed as part of the operational risk framework.

OBJECTIVES

The goal of the operational risk management framework is to identify, assess, control, and mitigate operational risk within the firm. A standard operational risk framework is applied across the firm in order to ensure consistency and completeness.

FIGURE 6.3 Sample Operational Risk Policy

FIGURE 6.3 (*Continued*)

The framework includes the following key elements:

- Governance
- Culture and awareness
- Loss data collection
- Risk and control self-assessment (RCSA)
- Scenario analysis
- Key risk indicators (KRIs)
- Measurement and modeling
- Reporting
- Risk appetite

There are three lines of defense to ensure effective operational risk management. The business units provide the first line of defense, the Corporate Operational Risk Department provides the second line of defense, and the Audit Department provides the third line of defense.

SUPPORTING DOCUMENTS

Standards, procedures, and guidelines are published for each of the framework elements to support the implementation of this policy.

SCOPE

This policy applies to all employees of the firm globally and failure to comply with this policy can result in disciplinary action, including dismissal.

ROLES AND RESPONSIBILITIES (GOVERNANCE)

BOARD OF DIRECTORS

The board of directors is responsible for establishing, approving, and periodically reviewing the operational risk framework. The board of directors oversees senior management to ensure that the policies, processes, and systems are implemented effectively at all decision levels.

The board of directors approves and reviews the risk appetite and tolerance statement for operational risk that articulates the nature, types, and levels of operational risk that the bank is willing to assume.

RISK MANAGEMENT COMMITTEE

The Risk Management Committee (RMC) develops for approval by the board of directors a clear, effective, and robust governance structure with well defined, transparent and consistent lines of responsibility. Senior management is responsible for consistently implementing and maintaining throughout the organization policies, processes, and systems for managing operational risk in all of the bank's material products, activities, processes, and systems consistent with the risk appetite and tolerance.

FIGURE 6.3 (*Continued*)

The RMC is responsible for setting the operational risk appetite for the firm and reviewing operational risk reporting and making decisions based on this information. Matters requiring escalation for resolution will be presented to the RMC for their consideration.

RMC is responsible for approving the Operational Risk Policy.

CORPORATE OPERATIONAL RISK DEPARTMENT

The Operational Risk Department (CORD) provides the second line of defense. CORD has a reporting structure independent of the risk generating business lines and is responsible for the design, maintenance, and ongoing development of the operational risk framework within the firm. A key function of CORD is to challenge the business lines' inputs to, and outputs from, the bank's risk management, risk measurement, and reporting systems.

CORD has the following responsibilities:

- Develop firm wide strategy for operational risk to meet regulatory and business drivers
- Design and maintain operational risk framework
- Provide consolidated reporting to RMC
- Provide training and awareness activities
- Coordinate collection and reporting of loss data, and track resolution of mitigating actions
- Plan and track RCSA activities across the firm and report output to RMC
- Coordinate design and collection of KRIs
- Plan and execute Scenario Analysis activities across the firm
- Analyze operational risk and present regular reporting on risk profile to RMC
- Validate operational risk data collected by business units

OPERATIONAL RISK COORDINATORS

The business line is the first line of defense and every business unit must have an operational risk coordinator identified. The responsibilities of the OR Coordinator are:

- Provide main communication contact with CORD
- Ensure complete and timely reporting of loss data in their area
- Manage RCSAs in their area
- Coordinate KRI collection in their area
- Track action items to completion for their area
- Assist area in timely completion of all operational risk reporting requirements
- Coordinate training and awareness activities in their area
- Provide business heads with operational risk data for consideration in decision making

(*Continued*)

FIGURE 6.3 (*Continued*)

ALL EMPLOYEES

Every employee in the firm is responsible for effective operational risk management in their activities and for the timely reporting of any operational risk loss events of which they are aware.

PRINCIPLES

CULTURE AND AWARENESS

Operational risk training is provided to all employees and to all new hires. The training provides an overview of operational risk, its definition, scope and importance.

Additional specific training is provided as needed for each element of the operational risk framework. Training is designed and coordinated by CORD.

In addition to training, a newsletter is distributed to all employees once each quarter and a website is accessible on the firm intranet.

LOSS DATA COLLECTION

INTERNAL LOSS EVENTS

Internal loss events are events that occur within the firm and which meet the definition of operational risk. Internal loss events are collected in accordance with the Operational Risk Event Standards (published separately). Internal loss events are used to assist with the identification, assessment, control, and mitigation of operational risk. Lessons learned from loss events are applied throughout the framework and mitigating actions are tracked by CORD and the OR Coordinators to assist with future risk mitigation.

A threshold for loss events is set in the Operational Risk Event Standards. All events that are above this threshold must be reported in the loss event database. Additional events may be reported.

EXTERNAL LOSS EVENTS

External loss events are those that occur outside the firm. External loss events are used to inform the operational risk framework. In particular, external losses provide an input into the RCSA, scenario analysis, culture and awareness, and reporting elements of the framework. Various sources are used to identify external events, including commercially available databases, news articles, and Internet searches.

FIGURE 6.3 (*Continued*)

RISK AND CONTROL SELF-ASSESSMENT

Risk and control self-assessments are used to identify potential operational risks and to provide a scoring for risks and controls in each area. RCSAs are forward looking and subjective. They are conducted on an annual basis in all areas. RCSA outputs are collated and analyzed by ORD and matters requiring escalation are reported to RMC for decision making and/or action.

SCENARIO ANALYSIS

The purpose of scenario analysis is to identify rare, catastrophic potential events and to estimate the potential financial impact and frequency of such events. Scenario analysis is conducted in selected areas of the firm. CORD facilitates the identification and scoring of scenario analysis.

KEY RISK INDICATORS

KRIs provide a monitoring tool to report on the performance of controls, changes in levels of risk, and trends that may inform the operational risk program. CORD may identify key KRIs which must be collected across the firm. The OR Coordinators are responsible for ensuring the collection of these KRIs. In addition, unique KRIs may be identified by each area for the purposes of effective operational risk management.

MEASUREMENT AND MODELING

For the purposes of Basel II the firm is required to calculate capital for operational risk. The Operational Risk Measurement Team is responsible for the development of capital models using the inputs from the operational risk framework. Further information is outlined in the Risk Modeling Policy (published separately).

REPORTING

ORD provides reporting to RMC on a quarterly basis. The Operational Risk Report includes the following:

- Internal loss data
- Relevant external loss data
- Action tracking
- RCSA output (when appropriate)
- KRI summary
- Capital requirements (when appropriate)
- Matters requiring decisions or escalation
- Analysis of current operational risk profile

(*Continued*)

FIGURE 6.3 (*Continued*)

RISK APPETITE

Operational Risk Appetite is set by RMC and the board.

It is anticipated that the operational risk framework will continue to evolve as experience develops. As the framework matures the elements of the framework will inform the firm of the current risk profile and will allow for refinement of the setting of future risk appetite. The strategy and objectives of the operational risk framework will be continually reviewed and revised to ensure effective identification, assessment, control, and mitigation of operational risk.

APPROVAL

This policy will be reviewed and approved annually by the RMC and the board.

SAMPLE STANDARDS, PROCEDURES, AND GUIDELINES

Following are examples of the type of wording that might be found in governance documents for loss data collection. Extracts from a standards document, a procedures document, and a guidelines document are provided.

Extract from a Loss Data Standards Document

Operational Risk Event Minimum Data Requirements When reporting an operational risk event, the reporter must provide the following minimum data in a timely manner:

- Date reported
- Date event occurred
- Name of reporter
- Reporting department
- Name of event
- Description of event:
  - The description must be sufficient that a person from a different area can understand what occurred. The use of shorthand, jargons, and acronyms should be avoided. The name of a client or individual should not be included.
  - The description should not apportion blame for the event, but should provide a factual recounting of what occurred.

- Involved departments: Include all departments that were involved in the event.
- Business line: Regardless of where the error occurred, all events must be allocated to a revenue area.
- Amount of direct loss.
- Amount of indirect loss: Indirect losses include legal fees, consulting fees, and the like.
- Recovery to date.
- Other impacts: Where appropriate, select additional nonfinancial impacts from reputational, client, regulatory, and life safety.
- Event category: Select from event categories as established in the Risk Taxonomy Standards.
- Event subcategory: Select from event subcategories as established in the Risk Taxonomy Standards.
- Cause: Select from people, process, systems, and external events.
- Action: A mitigating action must be identified, or it must be stated that no mitigating action will be taken and a reason must be given.

Extract from a Loss Data Procedures Document

Data Collection On identification of an operational risk event, the identifying person will immediately inform the business unit operational risk coordinator. The operational risk coordinator will determine whether the event is one that meets the definition of operational risk and, if so, will enter the event into the loss data system including all data elements as outlined in the Loss Data Standards.

Extract from a Loss Data Guidelines Document

Training To ensure timely identification and entry of loss events, it is recommended that all employees in a business unit receive operational risk management training annually.

Linkage between Documents

As can be seen from these examples, careful drafting of these documents can allow for updates to the standards, procedures, or guidelines without requiring additional changes to the related documents.

In these examples, the exact data requirements are set in the standards, the method of collecting the data is provided in the procedures and opportunities for quality improvement are recommended in the guidelines.

However, it is common for standards to be combined with policy or with procedures, and for guidelines to be incorporated into procedures.

As the operational risk framework evolves through experience, regular updates to the documents are likely. It is therefore important to ensure that the update and approval process is designed to be as efficient as possible within the culture of the firm.

KEY POINTS

- An operational risk policy should include:
  - The firm's definition of operational risk
  - The governance of operational risk including who owns it, what it owns, and how issues are escalated
  - The main activities/elements that are managed by the operational risk function
- An operational risk policy should be realistic and not aspirational.
- Each element of the framework must have written policies and procedures against which the firm is audited by its internal audit department.
- Standards provide detailed measures of what criteria must be met by the procedures.
- Procedures outline how activities should be undertaken, with step to step tasks explained.
- Guidelines are nonmandatory in nature and provide support for the procedures and further details as needed.

REVIEW QUESTION

1. Which of the following best describes a quality of a good policy document?
   a. Content requires continuous updating.
   b. Detailed steps and activities are outlined.
   c. Is approved by a senior management committee on an annual basis.
   d. Represents the future state goal for best practices.

CHAPTER 7

Internal Loss Data

This chapter explores the collection of operational risk loss data. It explores the reasons for data collection and the methods used. The seven Basel operational risk categories and the Basel business line categories are described and their use in the framework is discussed. Loss data standards are introduced, along with examples of regulatory expectations and best practices for the many elements of an operational risk event data collection process.

OPERATIONAL RISK EVENT DATA

Once governance, culture, and awareness and initial policies and procedures are in place, the four core elements of the operational risk program can be designed and launched. These four elements are:

1. Loss data
2. Risk and control self-assessments (RCSAs)
3. Scenario analysis
4. Key risk indicators (KRIs)

The first of these, loss data, is better named "operational risk event data," as it refers not just to losses, but to a broader category of operational risk events.

A robust operational risk framework includes consideration of both internal and external operational risk events. Internal events are those that have happened in or to the firm. External events are those that have happened not in or to the firm but elsewhere in the industry.

INTERNAL LOSS DATA OR INTERNAL OPERATIONAL RISK EVENTS

Loss data is a key element in the operational risk framework as is illustrated in Figure 7.1. Firms have found that collecting and analyzing operational risk events, or loss data, provides a valuable insight into the current operational risk exposure of the firm. Until these data are collected, there can be a mistaken perception that operational risk is not a real concern. Once internal loss data start to come in, there is often a new appreciation of the importance of managing this category of risk.

Many loss data programs are started as a result of a realization that you cannot manage what you cannot measure. Others are started as a result of specific regulatory requirements, such as Basel II.

When collecting loss data, it is important to consider many aspects of the program, including who, what, where, when, and why. We will start with "why."

Why Collect Operational Risk Event Data?

The design of a loss event database will be driven by the purpose of the program. There are several possible purposes for implementing a loss data program, and most firms have more than one in mind when implementing a loss data program. When designing operational risk event collection policies, procedures, standards, and guidelines, a firm should consider which of the following reasons apply:

- They are collecting data for capital modeling purposes.
- They wish to use events to help identify control weaknesses.

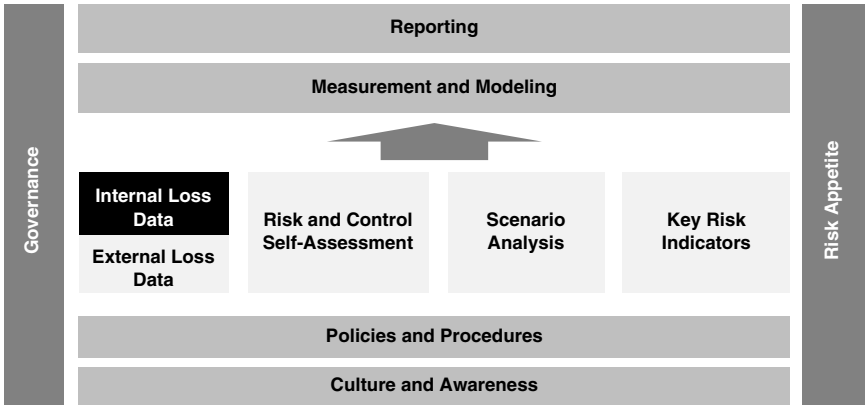

FIGURE 7.1 Internal Loss Data in an Operational Risk Framework

- They wish to kick off risk mitigation activities when events occur.
- They wish to evaluate risk events and outcomes.
- They wish to use events to help them to understand their current operational risk exposure and any areas of excessive risk.
- They wish to use event collection as a way to embed the operational risk discipline.

Each purpose will result in different design elements in the program, and will impact the policies and procedures that are developed around loss data. An effective loss data, or operational risk event program, will be designed to reflect the specific purposes and culture of the firm. It will also be accompanied by a strong training program to maximize participation.

The audit department should audit the departments of the firm against the loss data policies, procedures, and standards.

It is pragmatic to expect the initial quality of the database to be somewhat disappointing. It takes some time for culture change to take effect and for a significant number of operational risk events to be captured as intended.

Who Should Collect the Loss Data?

Who will be responsible for reporting operational risk-related events in the firm? Responsibility must be clear in order to ensure good participation. The operational risk policy might assign responsibility, or it might be outlined in a separate operational risk event policy or procedure document.

The firm might designate a particular representative in each department to ensure that all events are collected for their department. For example, an operational risk coordinator, specialist, or manager for each department might be tasked with ensuring all events are entered into the operational risk event database. This empowers them to seek out and report events that might otherwise languish unreported. It also ensures that someone owns the data reporting responsibility.

Some departments will be in a position to identify events that did not occur in their area, but which are captured by their controls. For example, the operations or finance departments may catch events during reconciliation activities.

It may be prudent, therefore, to endow these departments with additional responsibilities to inform the operational risk department of likely events that they come across in their day-to-day activities. Finance may also be involved in reconciling operational risk events to the general ledger if that is one of the goals of the loss data capture program in that firm. However, some firms do not attempt to reconcile loss events to the general ledger.

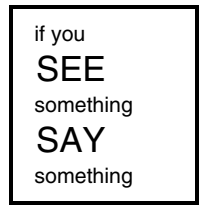

FIGURE 7.2 Loss Data Marketing Poster

It can be helpful to adopt an "if you see it, you must report it" policy; or perhaps, more practically, an "if you see it, you must ensure someone reports it" policy. This is reminiscent of the antiterrorism posters in the subways of New York City today (as illustrated in Figure 7.2) and may form the basis of a strong marketing campaign to ensure good participation in operational risk event collection.

This helps to ensure that an event does not remain unreported when several people are aware of it, but they all believe it is someone else's responsibility to report it.

Reporting of events should not be associated with fault, but rather should be associated with effective operational risk management. An open access database allows all employees at a firm to enter an event. However, if it is not practical to allow everyone to be able to report an event, then there needs to be a policy or procedure that allows for anyone to pass an event to a designated operational risk event reporter.

If there is an open access database approach, then it may be prudent to allow only very minimal data to be entered, with more being gathered by someone who has been trained in loss data collection. This will help to avoid some of the dangers of poor reporting. These dangers will be covered below.

What Should Be Collected in the Loss Data Program?

Any event that meets a firm's definition of operational risk should be captured in the loss event data database, subject to any conditions that are outlined in the loss data or operational risk event policy.

There are several useful pieces of information that should (or must if under Basel II) be captured for each event. First, it is important to assign an event to one, and only one, appropriate risk category. Risk categories are provided by Basel II, and many firms adopt these at the highest level and then customize lower levels to better match their firm's culture and products.

RISK EVENT CATEGORIES

Every event should be mapped to the risk event categories being used at the firm. These risk categories should be clearly outlined in the policies, procedures, standards, or guidelines that have been published in the firm for operational risk management.

Basel II provides a useful set of seven categories, which most firms have adopted or adapted to meet their own reporting needs. Basel II describes the seven categories as shown in Table 7.1.

TABLE 7.1 Basel II Operational Risk Event Categories

Event-Type Category (Level 1)	Definition
Internal Fraud	Losses due to acts of a type intended to defraud, misappropriate property, or circumvent regulations, the law, or company policy, excluding diversity/discrimination events, which involves at least one internal party.
External Fraud	Losses due to acts of a type intended to defraud, misappropriate property, or circumvent the law, by a third party.
Employment Practices and Workplace Safety	Losses arising from acts inconsistent with employment, health, or safety laws or agreements, from payment of personal injury claims, or from diversity/discrimination events.
Clients, Products, and Business Practices	Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product.
Damage to Physical Assets	Losses arising from loss or damage to physical assets from natural disaster or other events.
Business Disruption and System Failures	Losses arising from disruption of business or system failures.
Execution, Delivery, and Process Management	Losses from failed transaction processing or process management, from relations with trade counterparties and vendors.

Source: Bank for International Settlements, Annex 9, "International Convergence of Capital Measurement and Capital Standards: A Revised Framework," 2004.

I have found these seven categories to be remarkably resilient. I have tested them extensively within the financial services industry, but also in firms in other industries. At this highest level, they do seem to effectively capture all types of operational risk events.

It is true that there is a sometimes confusing mixture of events and causes in this list of seven (for example, fraud *causes* a loss, but damage to physical assets might *be* the actual loss). However, despite this, these seven categories have lived on successfully since they were first published in the Basel II document.

The severity and frequency of losses can be quite different in the different categories. For example, events are more frequent in the last category—Execution, Delivery, and Process Management—as this category captures lots of small errors. In contrast, events in the Clients, Products, and Business Practices category tend to be more rare, but can be very large when they occur (for example, class action lawsuits).

For this reason, the modeling of loss data can be quite different in each category and so it is important to ensure an event is placed in the correct category.

Having said that, it can still be argued that consistency is more important than accuracy. In other words, as long as similar events are always categorized in the same way, then operational risk management can be effective. In order to ensure this consistency, it is necessary to go down to a lower level of categorization. Let us consider each category from Table 7.1 in turn.

Internal Fraud

Losses due to acts of a type intended to defraud, misappropriate property, or circumvent regulations, the law, or company policy, excluding diversity/discrimination events, which involves at least one internal party.

Internal Fraud captures any event where there has been intentional wrongful behavior by an employee of the firm. In Annex 9 of the Basel II document, this category is further explained at a lower level, Level 2.

At Level 2, Internal Fraud is broken down into two subcategories: Unauthorized Activity and Theft and Fraud. Basel II provides Level 3 examples to illustrate these subcategories, as shown in Table 7.2.

From these second and third levels, it becomes clear that insider trading and unauthorized trading are captured under this category. It is also clear that unintentional acts are not captured here. In fact, you will see similar activities fall under Execution, Delivery, and Process Management or under Clients, Products, and Business Practices when they are unintentional mistakes.

Capturing operational risk events that have a fraud element is likely to be very sensitive. This category and the External Fraud category often

TABLE 7.2 Internal Fraud Subcategories

Categories (Level 2)	Activity Examples (Level 3)
Unauthorized Activity	Transactions not reported (intentional) Transaction type unauthorized (w/monetary loss) Mismarking of position (intentional)
Theft and Fraud	Fraud/credit fraud/worthless deposits Theft/extortion/embezzlement/robbery Misappropriation of assets Malicious destruction of assets Forgery Check kiting Smuggling Account takeover/impersonation/etc. Tax noncompliance/evasion (willful) Bribes/kickbacks Insider trading (not on firm's account)

Source: Annex 9, Basel II.

require legal review before being entered into a database. They might also have only minimal information entered in order to ensure confidentiality.

External Fraud

Losses due to acts of a type intended to defraud, misappropriate property, or circumvent the law, by a third party.

External Fraud captures all events where there has been fraud, with no collusion or participation from an internal employee.

At Level 2, External Fraud is broken down into two subcategories: Theft and Fraud and Systems Security. Basel II provides level three examples to illustrate these subcategories, as shown in Table 7.3.

TABLE 7.3 External Fraud Subcategories

Categories (Level 2)	Activity Examples (Level 3)
Theft and Fraud	Theft/Robbery Forgery Check kiting
Systems Security	Hacking damage Theft of information (w/monetary loss)

Source: Annex 9, Basel II.

From these second and third levels, we can see that one of the most high-profile operational risks is captured here: cyber security. In 2004, the Basel Committee was unaware just how dangerous cyber-attacks would become for the financial services industry, but they had the foresight to include it as a Level 3 example in their risk categories. In the past few years, the volume, sophistication, and effectiveness of cyber-attacks has increased dramatically.

As a result, this risk category is currently enjoying intense scrutiny. The proliferation of politically motivated attacks such as events involving WikiLeaks and Anonymous are of high concern. In addition, the threat of cyber terrorism is considered very real and has been consistently highlighted by governments in the past 12 months.

Traditional external fraud is also captured here, theft and forgery being examples of criminal events that are captured in OR databases.

Employment Practices and Workplace Safety

Losses arising from acts inconsistent with employment, health, or safety laws or agreements, from payment of personal injury claims, or from diversity/discrimination events.

The Employment Practices and Workplace Safety category captures losses that result from harm suffered by employees, either due to workplace accident or due to mistreatment by the firm.

At Level 2, Employment Practices and Workplace Safety is broken down into three subcategories: Employee Relations, Safe Environment, and Diversity and Discrimination. Basel II provides Level 3 examples to illustrate these subcategories, as shown in Table 7.4.

Events that are captured in this category might be highly sensitive, and some firms have a policy that allows only the human resources department to enter events in this category.

TABLE 7.4 Employment Practices and Workplace Safety Subcategories

Categories (Level 2)	Activity Examples (Level 3)
Employee Relations	Compensation, benefit, termination issues Organized labor activity
Safe Environment	General liability (slip and fall, etc.) Employee health and safety rules events Workers' compensation
Diversity and Discrimination	All discrimination types

Source: Annex 9, Basel II.

Workers' compensation items are captured in this category, and it can be helpful to set up an automatic link with any workers' compensation database so that such data can be automatically linked or reconciled.

Discriminatory actions are likely to be kept confidential and will often have only minimal information entered for that reason.

There is sometimes confusion regarding termination payments. If someone is compensated beyond the usual termination notice period due to grievances, then should such a payment be considered an operational risk event? Firms treat these sensitive cases differently. Going back to the definition of operational risk, it should certainly be entered if, but only if, there is a loss resulting from failed or inadequate processes, people, systems, or external events. Consistency is key here. Whatever approach a firm decides to adopt, a clear standard needs to be established and kept.

Clients, Products, and Business Practices

Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product.

This category has some of the largest events, as large legal losses are often captured here. A class action lawsuit that alleges client misselling will fall into this category, as will any large litigation concerning a badly flawed financial product.

At Level 2 there are many subcategories for Clients Products and Business Practices: Suitability, Disclosure, and Fiduciary; Improper Business or Market Practices; Product Flaws; Selection, Sponsorship, and Exposure; and Advisory Activities. Basel II provides Level 3 examples to illustrate these subcategories, as shown in Table 7.5.

You will notice that the Level 3 examples present a frightening list of the worst things that can go wrong for a financial institution, from model error to money laundering. Criminal activity may be captured in this category along with regulatory breaches. Regulatory fines and legal penalties often dominate this category. In fact, some are tempted to rename this category "Legal Events." However, legal events can certainly arise in other categories, as we have just seen in the Employment Practices and Workplace Safety category.

Clients, Products, and Business Practices events often have a serious reputational impact as well as a financial cost. Items in this category are most likely to get negative press coverage, and the legal department is usually (painfully) aware of these events.

TABLE 7.5 Client, Products, and Business Practices Subcategories

Categories (Level 2)	Activity Examples (Level 3)
Suitability, Disclosure, and Fiduciary	Fiduciary breaches/guideline violations Suitability/disclosure issues (KYC, etc.) Retail customer disclosure violations Breach of privacy Aggressive sales Account churning Misuse of confidential information Lender liability
Improper Business or Market Practices	Antitrust Improper trade/market practices Market manipulation Insider trading (on firm's account) Unlicensed activity Money laundering
Product Flaws	Product defects (unauthorized, etc.) Model errors
Selection, Sponsorship, and Exposure	Failure to investigate client per guidelines Exceeding client exposure limits
Advisory Activities	Disputes over performance of advisory activities

Source: Annex 9, Basel II.

The process for ensuring that events that are being considered by legal are also being captured in the operational risk database needs to be clearly established and maintained. Regulators are now asking for legal reserves to be captured along with realized losses. For this reason, it can be beneficial to have an automated link between any legal database and the operational risk database, to ensure accurate and timely reporting and to reconcile between the two sources.

Damage to Physical Assets

Losses arising from loss or damage to physical assets from natural disaster or other events.

Damage to Physical Assets can occur for a variety of reasons. There is only one Level 2 subcategory provided by Basel II—Disasters and Other Events—and little further explanation in Level 3, as seen in Table 7.6.

TABLE 7.6 Damage to Physical Assets Subcategories

Categories (Level 2)	Activity Examples (Level 3)
Disasters and Other Events	Natural disaster losses Human losses from external sources (terrorism, vandalism)

Source: Annex 9, Basel II.

Most events in this category will be covered, at least in part, by insurance. However, the original loss should still be captured and regulators allow only a small amount of insurance recovery to be considered. The reason for this is clear: it might take more than a year to receive an insurance recovery, and during that period the firm needs to be able to demonstrate that is has enough capital to cover the loss. We consider insurance further in Chapter 12.

Business Disruption and System Failures

Losses arising from disruption of business or system failures.

There is only one Level 2 subcategory for Business Disruption and System Failures: Systems. Basel II provides Level 3 examples of the systems to be considered as shown in Table 7.7.

It is often hard to put a value on losses in this category. While the impact of a major network or telecommunications outage can be serious, it is often best measured in lost opportunities, rather than in direct losses. An operational risk event database might be designed to capture both the opportunity costs as well as direct costs, but many firms do not take that extra step.

Losses in this category are also often challenging in that they need to be assigned to a particular business line, but the impact may be firm-wide. If that is the case, then an allocation methodology needs to be established, and this is discussed further below.

TABLE 7.7 Business Disruption and System Failures Subcategories

Categories (Level 2)	Activity Examples (Level 3)
Systems	Hardware Software Telecommunications Utility outage/disruptions

Source: Annex 9, Basel II.

In the past few years, we have seen many wide-scale power outages as a result of extreme weather, as well as examples of simple human error and equipment errors.

Extreme weather may well cause damage to physical assets as well as business disruption. For example, Hurricane Sandy hit the eastern states in America in the autumn of 2012. The resulting physical damage was severe, and there were major disruptions to telecommunications and utilities. It can be seen from this example that one cause might produce multiple operational risk events that sit in different risk categories.

Execution, Delivery, and Process Management

Losses from failed transaction processing or process management, from relations with trade counterparties and vendors.

The majority of operational risk events occur in the Execution, Delivery, and Process Management category. The frequency of events is usually relatively high compared to other categories. However, many of the events may be small, and so the severity might be relatively low compared to other categories.

There are many Level 2 subcategories: Transaction Capture, Execution, and Maintenance; Monitoring and Reporting; Customer Intake and Documentation; Customer/Client Account Management; Trade Counterparties; and Vendors and Suppliers. Basel II provides Level 3 examples, as shown in Table 7.8.

As can be seen, the list of examples is comprehensive. Anything that goes wrong somewhere in the process of executing a trade, onboarding a client, creating regulatory reports, or dealing with third parties can end up captured in this category. Many support functions are designed to manage controls to prevent these types of errors, so you may find that your operations, controllers, and technology departments already capture information on events that occur in the category.

USING THE BASEL RISK CATEGORIES

The Basel risk categories must be used to report operational risk events for firms that are required to meet the Basel regulations. However, they can also be used effectively in other ways. Most firms use the same categorization taxonomies for their risk and control self-assessment (RCSA) programs as they do for their loss data. They may also align any key risk indicators (KRIs) and any scenario analysis work with the same categories.

TABLE 7.8 Execution, Delivery, and Process Management Subcategories

Categories (Level 2)	Activity Examples (Level 3)
Transaction Capture, Execution, and Maintenance	Miscommunication Data entry, maintenance, or loading error Missed deadline or responsibility Model/system misoperation Accounting error/entity attribution error Other task misperformance Delivery failure Collateral management failure Reference data maintenance
Monitoring and Reporting	Failed mandatory reporting obligation Inaccurate external report (loss incurred)
Customer Intake and Documentation	Client permissions/disclaimers missing Legal documents missing/incomplete
Customer/Client Account Management	Unapproved access given to accounts Incorrect client records (loss incurred) Negligent loss or damage of client assets
Trade Counterparties	Nonclient counterparty misperformance Misc. nonclient counterparty disputes
Vendors and Suppliers	Outsourcing
	Vendor disputes

Source: Annex 9, Basel II.

While the seven Level 1 categories are mandatory for capital calculation and loss data capture by a Basel firm, the second and third levels are often adapted to better suit those firms.

The Basel risk categories are used to capture a risk event, not a cause. This does result in some confusion, as the wording used by the Basel Committee does suggest "cause" in some cases. However, when designing a risk categorization taxonomy for a firm, it is important to be clear about the difference between risk impacts and causes.

These risk categories are helpful buckets in which to gather operational risk event data, and the categorization scheme that is used in the loss data program should be applied across the operational risk framework.

If a different set of Level 1 categories is used in a firm, then a behind-the-scenes mapping to the seven Basel categories is needed for Basel firms.

For example, JPMorgan Chase uses the following Level 1 categories in its operational risk framework:

- *Client Service and Selection*
- *Business Practices*
- *Fraud, Theft, and Malice*
- *Execution, Delivery, and Process Management*
- *Employee Disputes*
- *Disasters and Public Safety*
- *Technology and Infrastructure Failures, Including Cyber Security Breaches*[1]

They will need to map these to the Basel II categories for regulatory reporting purposes.

Firms that do not have Basel II requirements often find these categories a helpful starting place for the development of their own risk classification system.

MINIMUM LOSS DATA STANDARDS

It is important to have a clear policy and standards on the minimum reporting requirements for operational risk event data. The loss data standards should contain minimum reporting criteria as mandated by regulation,[2] plus those data requirements that have been selected to facilitate strong operational risk management practices at the firm.

Examples of minimum criteria considerations include the following.

Comprehensive

The loss data program must be comprehensive and capture all material activities and exposures from all appropriate subsystems and geographic locations.

Practically speaking, it can be extremely difficult to ensure that every nook and cranny of the organization is participating effectively in the loss data collection program. However, it is important that the operational risk department regularly reviews the business structure of the firm to ensure that new acquisitions, mergers, or business changes are reflected in the coverage of the loss data program.

Threshold

The loss data program must include all material losses that are above a de minimis gross loss threshold, for example, €10,000.

There should be a threshold over which events *must* be entered. Setting a threshold will depend on the risk appetite of the firm and any regulatory requirements that it needs to meet. Basel II suggests that a threshold of €10,000 would be appropriate, but even Basel II firms have selected different thresholds: from zero to $100,000. In recent years, regulatory pressure has been downward, and most firms are now requiring mandatory reporting of all events over €10,000 or $10,000.

A zero threshold will set a high reporting burden on the firm. Every error that is a result of inadequate or failed processes, people, and systems or from external events will have to be captured. Taken literally, this would mean that a pencil stolen from the supply cabinet would be an event that needs to be entered in the loss event database.

In practice, firms that have a zero threshold apply it only to areas of the firm where it is practical to collect that data. For example, if they have a data feed for all trading errors, then it is not burdensome to capture them all, however small.

Some departments may want to capture all losses, regardless of the threshold. For example, an operational department may want to track every error, or a finance department might want to track every time there is a wire transfer error.

However, there will be other requirements around each event in addition to the amount, and these may be unnecessary details for smaller losses and might be excluded from the reporting requirements. A firm that has a zero threshold for operational risk event reporting is therefore likely to have a higher threshold for full details to be mandatory.

Many firms do indeed have varying reporting thresholds for different departments, but there must also be a minimum corporate threshold, over which an operational risk event must be reported and will be included in the firm's program and in any operational risk capital calculation.

Amount

Each loss data entry must include the loss amount.

This can be the source of some contention and may need intervention from the operational risk department, or a dedicated controller, as there may be some confusion over the exact amount lost. Some firms reconcile their operational risk events to their general ledger, others do not. The actual gross loss amount will often be different from the net loss amount or the loss after all recoveries. Both the gross and net amounts should be captured.

There may be conflicting views as to how much was actually lost in the first place. For example, a trade error that results in a loss can give rise

to disagreements regarding the time and price at which the resulting loss should be calculated. A hedging error might produce a loss, but it may be unclear exactly what loss was realized.

In addition to ensuring that the correct amount of loss is entered, there are considerations as to which losses should be included in the loss data system. In June 2011, the Basel Committee on Banking Supervision issued "Operational Risk—Supervisory Guidelines for the Advanced Measurement Approaches" in which they offered further guidance on how to determine the correct gross amount.

> **Measures of the gross loss amount**
>
> *There are different ways to measure the gross loss amount:*
>
> *(a)* ***Mark-to-market:*** *the economic impact of an operational risk loss is usually the same as the accounting impact when an operational risk loss affects assets or accounts treated on a mark-to-market basis. In such cases, the gross loss amount is the loss or adjustment as recognized in the comprehensive statement of income.*
> *(b)* ***Replacement cost:*** *the economic impact of an operational risk loss usually differs from the accounting impact when losses affect assets or accounts that are not maintained on a mark-to-market basis such as property, plant, equipment or intangible assets. The gross loss amount is the replacement cost of the item. Replacement cost means the cost to replace an item or to restore it to its pre-loss condition.*[3]

The Committee also provided guidance on what should be included in a gross loss amount:

> *The following specific items should be included in gross loss computation.*
>
> *(a)* **Direct charges** *(including impairments) to the statement on comprehensive income and write-downs due to operational risk events.*
> *(b)* **Costs incurred as a consequence** *of the event that should include external expenses with a direct link to the operational risk event (e.g., legal expenses directly related to the event and fees paid to advisors, attorneys or suppliers) and costs of repair or replacement, to restore the position that was prevailing before the operational risk event.*

(c) ***Provisions*** *("reserves"); the potential operational loss impact is reflected in the comprehensive income statement and should be taken into account in the gross loss amount.*
(d) ***Pending losses*** *stem from operational risk events with a definitive financial impact, which are temporarily booked in transitory and/or suspense accounts and are not yet reflected in the statement of comprehensive income. For instance, in some countries, the impact of some events (e.g., legal events, damage to physical assets) may be known and clearly identifiable before these events are recognized through the establishment of a reserve. Moreover, the way this reserve is established (e.g., the date of recognition) can vary across institutions or countries. "Pending losses," that are recognized to have a relevant impact, should be included in the scope of operational risk loss within a time period commensurate to the size and age of the pending item; this can be done through the recognition of their actual amount in the loss database or pertinent scenario analysis.*[4]

Until the publication of these guidelines there was a wide range of practice regarding the definition of "gross" and "net" loss. The Committee went further and provided clarification of what should *not* be included in the gross amount as follows:

The following specific items should be excluded from the gross loss computation. It should not be considered to be an exhaustive list:

(a) Costs of general maintenance contracts on property, plant or equipment;
(b) Internal or external expenditures to enhance the business after the operational risk event: upgrades, improvements, risk assessment initiatives and enhancements;
(c) Insurance premiums.[5]

National regulators are applying their interpretation of this guidance to all of their AMA banks. As has been noted earlier, even financial institutions that are not technically required to adopt AMA practices are increasingly being told that AMA standards are "best practices" and therefore should be adopted anyway.

Indirect Costs In addition to the direct financial impact of the loss, there may be other indirect costs such as resulting legal fees, or the costs to fix the control failure that caused the loss. In the preceding guidelines,

these indirect costs are referred to as "costs incurred as a consequence of the event."

The inclusion of associated legal fees in the gross amount can have a large impact on the loss data. Legal fees can be extremely high and may be incurred over several years. What if an event crosses the reporting threshold only because of the associated costs incurred? The loss data policy and standards of a firm need to clearly articulate whether such items are exempt because the initial loss was under the threshold, or whether they become reportable as soon as the associated costs take it over the threshold. In the latter case, there needs to be a mechanism for tracking events that are too small now, but have the potential to be large later due to legal costs. The reporting timing issues that can result are discussed below under the date consideration.

A firm's loss data policy, procedures, and standards must clearly state whether these indirect costs must be captured, and if they are, then the methods to be used to calculate them.

Gains, Near-Misses, and Opportunity Costs Most loss data programs also collect gains that are realized due to operational risk events. For example, a trade error might be followed by a market move that results in an inadvertent gain to the firm.

Near-misses are also valuable opportunities to manage operational risk proactively. An event might produce a loss under the threshold or no loss at all, but indicate an unmitigated operational risk.

Similarly, opportunity costs or lost revenue might result from an event, even though there is no direct loss. For example, if a trading system fails and no trades can be made for a day, then that day's revenue has been lost.

The event itself is still a concern to the firm as it indicates that a control failed or a process is flawed, and the next time the market could move in the other direction, causing a loss.

For this reason, gains, near-misses, and opportunity costs are valuable additions to the loss database, and often a loss database is renamed to reflect this. For example, it might be called the "operational risk event database" to more accurately reflect its purpose and content.

The AMA Guidelines reinforce this as follows:

> *Some items are important for risk management although they may be beyond the scope required for quantification. In particular, the items below can be useful for promptly detecting failures and errors in processes or internal control systems. These items may also be useful inputs for scenario analysis.*

(a) **"Near-miss events":** *operational risk events that do not lead to a loss. For example, an IT disruption in the trading room just outside trading hours.*
(b) **"Operational risk gain events":** *operational risk events that generate a gain.*
(c) **"Opportunity costs/lost revenues":** *operational risk events that prevent undetermined future business from being conducted (e.g., unbudgeted staff costs, forgone revenue and project costs related to improving processes).*[6]

Accounting Adjustments or Timing Events Some operational risk event databases include accounting adjustments as well as actual losses. For example, if the accounting treatment that has been used by a firm is declared incorrect by a regulator, then the books and records of the firm need to be adjusted. This can result in significant downward adjustments even though no payment has actually been made to correct the error.

Some firms use the operational risk event database to track such events and include balance sheet or profit and loss adjustments as loss events. The threshold for these events is often much higher than the minimum threshold for a direct financial loss, and they might be excluded from any capital calculations.

There is some discussion as to whether these are actual losses or "timing events" or "accounting adjustments." The loss data standards in the firm's policy must clearly outline whether such events should be included and the criteria that should be applied to them.

The AMA Guidelines consider these items as follows:

> ***Timing losses*** *are defined as the negative economic impacts booked in an accounting period, due to operational risk events impacting the cash flows or financial statements of previous accounting periods. Timing impacts typically relate to the occurrence of operational risk events that result in the temporary distortion of an institution's financial accounts (e.g., revenue overstatement, accounting errors and mark-to-market errors). While these events do not represent a true financial impact on the institution (net impact over time is zero), if the error continues across two or more accounting periods, it may represent a material misrepresentation of the institution's financial statements. Material "timing losses" due to operational risk events that span two or more accounting periods should be included, i.e., full amount that includes make-up payments as well as penalties and interest, in the scope of operational risk loss when they give rise to legal events.*[7]

Recoveries Each loss data entry must include any recoveries against the gross loss amount.

This can cause some confusion as is best illustrated with an example. If a wire transfer is sent to the wrong party, and the amount is above the threshold, then this would be an operational risk event that must be reported. However, if the amount is quickly returned by the erroneous party, some firms consider this to be a "near miss" and do not consider it a realized event. Other firms consider this a gross loss, with a recovery equal to the gross loss and therefore with a net loss of zero. The treatment of such events must be clearly established in the loss data policy in order to avoid confusion and inconsistency.

The AMA Guidelines acknowledge this range of practice, and confirm that if the recovery is rapid, then the event can be considered a near-miss rather than a loss event.[8]

For both recoveries and timing events, the AMA Guidelines state that "the inclusion or exclusion of the… items depends on their nature and materiality."[9]

Date

Each loss data entry must include the date of the event.

Perhaps surprisingly, this can be a difficult piece of data to nail down. For example, if the loss is the result of several consecutive control failings, then is the date of the event the date that the first control failing occurred, or the date that the last control failing occurred? Or is the correct date the date the loss hit the accounts? Or is it the date that it was detected? The date requirements must therefore be clearly defined in the loss data policy or standards.

Date Challenges for Legal Events

Reserves Recent regulatory guidance has added the requirement that legal reserves should be collected at the time of reserve. For some years the industry has been arguing that this might amount to double counting. The strongest argument was: Why collect loss data to calculate capital to cover something that is already being reserved for? Another concern was the possibility that information would be discoverable and could compromise the bank or lead to further litigation. However, most firms have procedures in place that protect the confidentiality of such matters by providing only minimum information in the database.

Despite these arguments, regulators have determined that it is better to include all known losses as promptly as possible, and they point out that

that holding a reserve is not double counting capital, as the event would only be one data point in the operational risk capital calculation.

Legal Fees Date issues can arise when legal fees are collected, as these fees continue to accrue over time. Some firms have adopted an approach where a legal event is entered as a loss only once it is final. Final might be determined as when a final settlement had been reached, or a case closed with no further appeals anticipated. The legal fees accrued up to that date could then be entered as a final amount.

However, some cases span several years, and if a legal reserve has been taken, there may be an expectation that associated fees are being collected on a regular basis. The AMA Guidelines provide an excellent example of the complexities that can arise with dating legal events:

> *Bank X is named in an investor lawsuit claiming inadequate and misleading disclosure of mortgage-related losses on 4 May 2006 (discovery date). The suit asks for monetary damages for investment losses in the amount €5 billion. At the discovery date, when the bank was served with a potential exposure of €5 billion, legal counsel indicated that the suit had no merit, and that the likelihood of loss is remote. On 15 November 2008, following a review of internal documents/discovery the bank's legal counsel recommends that the "least cost" would be to settle the case for €1 billion. As a result, the bank takes a reserve for that amount. The case is settled two years later (settlement date) for €2 billion.*
>
> *At the reserve date, the exposure of €1 billion is reasonably probable and it has been reasonably estimated. Supervisors expect the reserve amount of €1 billion to be reflected as a direct input into the AMA model. However, between the discovery date and the reserve date, legal counsel updates the probability that some settlement would be paid. During that time period the bank should consider reflecting this exposure in the capital calculation, for instance by a scenario analysis.*
>
> *Between the reserve date and settlement date, the exposure may increase or decrease based on the outcome of settlement negotiations. In this example, the settlement amount increased to €2 billion, so during the period between the reserve date and settlement date that bank should reflect the increased exposure in its' AMA capital requirement estimation process. Alternatively, if the exposure declined to €500 million, the bank should reflect the decreased exposure in its AMA capital requirement estimation process. However, if the bank paid a settlement as a provisional*

> *execution following a court decision, only to have the decision/settlement overturned or reduced, the bank should reflect the paid amount as its gross loss with any reduction reflected as a recovery.*[10]

The Guidelines recommend that the event be included in the loss event database at the date of reserve, that any changes to exposure be captured in the capital modeling through alternative methods, such as scenario analysis, and that there should be a robust process to update the amount between the reserve date and the final settlement date.[11]

Description and Causes

Each loss data entry must include descriptive information about the drivers or causes of the loss event.

The most sensitive information about the event will often be in the description of the drivers and causes.

A firm's loss data standards may include a list of possible causes to select from—often related to the firm's operational risk definition. For example, the cause might be selected from people, process, systems, or external event. Alternatively, there may be a more sophisticated list of causes to select from, that are specific to the firm, or to the department in the firm.

It is always politically challenging to memorialize fault or blame, and so care must be taken in providing clear guidelines on what should (and should not) be included in a description. Good training must be provided on these guidelines. Some firms are concerned enough about this information to engage their legal departments in reviewing and editing the entries where necessary, so as to avoid inadvertently exposing the firm to legal risk through inappropriate wording.

The Operational Riskdata eXchange Association (ORX) is a not-for-profit industry association dedicated to advancing the measurement and management of operational risk in the global financial services industry. The ORX database collects operational risk event data from a consortium of banks, and it will be discussed more fully in Chapter 8. For events over $10 million the member banks are required to select a cause for the event. ORX provides a helpful taxonomy of causes as shown in Table 7.9.

As there may well be more than one cause, ORX allows its members to select up to three causes. In the same way, many firms' loss data standards allow for several causes to be selected for a single event. They also provide lower-level descriptions and examples that can be found in their standards document and are easily accessible online.

TABLE 7.9 Level 1 Causes in ORX

Cause	Description
External	Actions by agents external to the firm
People/Staff	Factors related to actions by staff/employees or management of staff/employees of the firm or consolidated companies
Governance and Structure	Factors related to the governance and oversight practices of the bank
Processes	Factors related to the way that the firm is organized and certain broad management processes
Internal Systems Failures	Factors related to inadequacies or failures in internal technology, physical, and communication systems

Source: ORX Operational Risk Reporting Standards, Edition 2011, Appendix: detailed description of data categories, pp. 86–93, www.orx.org/lib/uploads/public_folder/ORRS_Appendix_v1-2_12_July_2012_120718_Clean.pdf.

TABLE 7.10 Basel II Business Line Categories

Level 1	Level 2	Activity Groups
Corporate Finance	Corporate Finance Municipal Government Finance Merchant Banking Advisory Services	Mergers and acquisitions, underwriting, privatizations, securitization, research, debt (government, high yield), equity, syndications, IPO, secondary private placements
Trading and Sales	Sales Market Making Proprietary Positions Treasury	Fixed income, equity, foreign exchanges, commodities, credit, funding, own position securities, lending and repos, brokerage, debt, prime brokerage
Retail Banking	Retail Banking	Retail lending and deposits, banking services, trust and estates
	Private Banking	Private lending and deposits, banking services, trust and estate, investment advice
	Card Services	Merchant/commercial/corporate cards, private labels, and retail
Commercial Banking	Commercial Banking	Project finance, real estate, export finance, trade finance, factoring, leasing, lending, guarantees, bills of exchange

(*Continued*)

TABLE 7.10 (*Continued*)

Level 1	Level 2	Activity Groups
Payment and Settlement	External Clients	Payments and collections, funds transfer, clearing and settlement
Agency Services	Custody	Escrow, depository receipts, securities lending (customers) corporate actions
	Corporate Agency	Issuer and payer agents
	Corporate Trust	
Asset Management	Discretionary Fund Management	Pooled, segregated, retail, institutional, closed, open, private equity
	Non-Discretionary Fund Management	Pooled, segregated, retail, institutional, closed, open
Retail Brokerage	Retail Brokerage	Execution and full service

Source: Basel II, Annex 8, Mapping of Business Lines.

Criteria for Allocation to Business Line

There must be documented, objective criteria for allocating losses to specified business lines.

Every event needs an owner, or in other words, it must be determined which front office area suffered the loss. This can cause some tension where the cause of the loss may occur in a department outside the front office, but the impact is placed on the profit and loss account of the business area. For this reason, it is helpful to have clear, objective criteria, including a limited list of business areas to select from when identifying where the loss hit the firm's accounts.

Basel II provides the following guidance on business line categorization as shown in Table 7.10.

The organizational structure of a firm might well not fit neatly into this categorization structure, and most firms have developed a mapping behind the scenes. This mapping allows them to collect data in a way that makes sense to their firm, but also allows them to group data appropriately for regulatory reporting as needed.

Criteria for Allocation to Central Function

If an event occurs in a central function and impacts the whole firm or several business lines, such as a network outage, then the loss data policy

must clearly outline how any resulting loss is allocated to each business line. Basel II outlined this requirement for operational risk event collection as follows:

> *A bank must develop specific criteria for assigning loss data arising from an event in a centralized function (e.g. an information technology department) or an activity that spans more than one business line, as well as from related events over time.*[12]

All Impacted Departments

It is often helpful to specify in the loss data criteria that all departments that are involved in the event must be identified as the event is entered. This helps to ensure good communication around the event. Many events impact several areas, and the loss data system often needs strong workflow components to facilitate entries and discussions by multiple parties.

Boundary Events Identified

Credit risk–related events and market risk–related events should be collected and flagged as boundary events. When using loss data as an input into a capital calculation, credit risk boundary events can be excluded from the calculation, but market risk events must be included. An example of a boundary credit risk/operational risk event is where a counterparty fails and the collateral that was supposed to have been collected has not been requested.

An example of a boundary market risk/operational risk event is where a trade error occurs and the market moves dramatically in a direction that increases the loss.

It is generally accepted that credit risk/operational risk boundary events are captured in credit risk capital calculations, and so can be excluded from any operational risk capital calculations. In contrast, market risk/operational risk boundary events are not captured in market risk capital calculations, and so should be included in operational risk capital calculations.

If a loss event database is being used to calculate operational risk capital, then these boundary events need to be carefully tagged to ensure they are appropriately included or excluded from the operational risk calculation.

Action Items

As losses are gathered, there should also be identified mitigating actions, either to ensure the recovery of the moneys, or the prevention of future

similar events. Actions should include an owner and due date for each task, and should be tracked to completion. From a practical point of view, it is necessary to have good action tracking processes in places to ensure that actions do not sit ignored in the loss database, but are being actively pursued in order to mitigate the operational risk that has been identified by the event.

Nonfinancial Impacts

In addition to the financial impact of the event, there may be other impacts that can be gathered as part of the loss event data collection program. While it may be difficult to put a value on impacts such as reputational damage, a firm's loss data standards might include a field for a qualitative or free prose assessment of any reputational impact.

WHERE SHOULD OPERATIONAL RISK EVENT DATA BE COLLECTED?

Most firms have implemented robust technology systems to manage their operational risk event data. This allows them to effectively manage the multiple data standards and complex workflow requirements of the program.

While most operational risk event databases started life as simple spreadsheets, it was quickly evident that a more sophisticated approach would be needed. Some firms developed in-house solutions, some purchased off-the-shelf solutions. In the past five years, off-the-shelf solutions have proliferated and improved. The implementation of a new operational risk event database should certainly be preceded by an assessment of the advantages and disadvantages of building in-house versus purchasing a system readymade.

Operational risk event databases are sometimes stand-alone elements in an operational risk framework, and sometimes they are integrated into the other elements of the program—sharing data with RCSA systems, KRI systems, scenario analysis, and capital calculation systems.

In JPMorgan Chase's annual report, they describe their integrated operational risk system, Phoenix, as follows:

> *The Firm's operational risk framework is supported by Phoenix, an internally designed operational risk software tool. Phoenix integrates the individual components of the operational risk management framework into a unified, web-based tool. Phoenix enhances*

> *the capture, reporting and analysis of operational risk data by enabling risk identification, measurement, monitoring, reporting and analysis to be done in an integrated manner, thereby enabling efficiencies in the Firm's monitoring and management of its operational risk.*[13]

Today, many firms are investigating the best way to integrate their operational risk systems to best support excellent operational risk identification, assessment, monitoring, and mitigation.

WHEN SHOULD OPERATIONAL RISK EVENT DATA BE COLLECTED?

Operational risk event reporting is most effective when there is prompt and accurate reporting of events and tracking of remediation activities. For this reason, many firms adopt standards that require timely reporting of an event, sometimes in an initial draft form, and timely maintenance of the event record to reflect new or more accurate information.

The final sign-off on an event might occur much later, once all parties are comfortable that the record is accurate. Depending on the culture of the firm, an event might remain out of sight of the central operational risk function until the business line or department involved is ready to sign off and pass it on. Some of the reluctance to enter draft data can be alleviated through robust security features in the system, to prevent general viewing of an item either until it is final or perhaps to prevent its ever being viewed by others outside the departments that are directly involved.

HOW SHOULD OPERATIONAL RISK EVENT DATA BE COLLECTED?

The workflow for loss data collection will depend on each firm's policies and procedures regarding who, what, where, and when data is collected. One example of a possible operational risk event data collection process for the initial reporter of the event is provided in Figure 7.3. The workflow shows the progress of the event from the identification to reporting and the role of the corporate operational risk function (CORF). The complete workflow for all parties involved would be more complex and may vary from department to department and region to region within a firm.

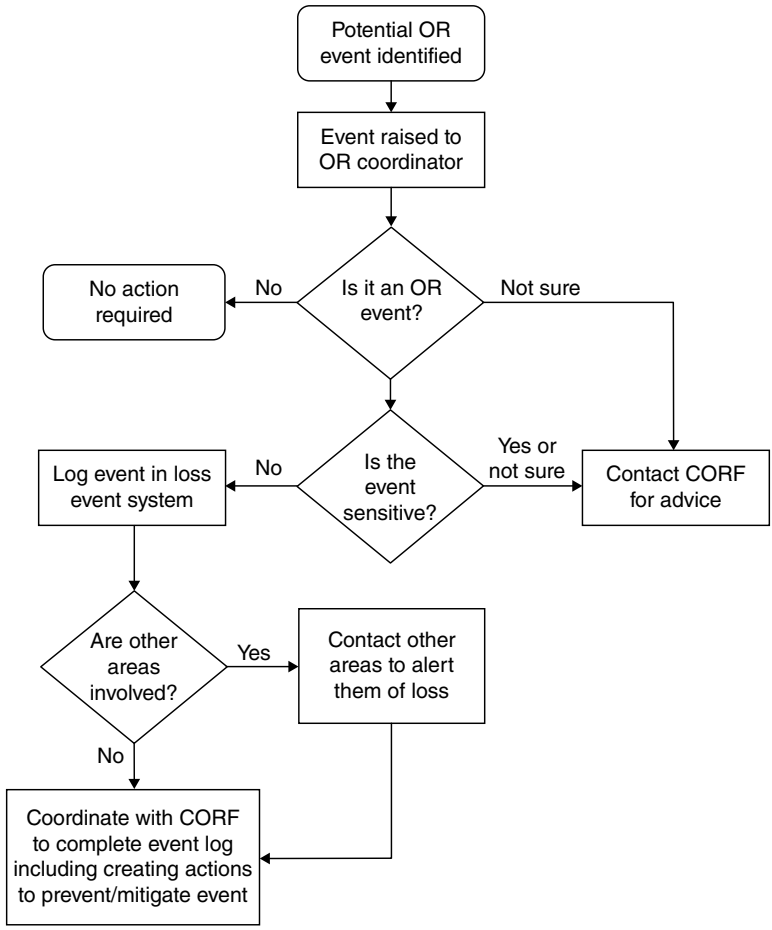

FIGURE 7.3 Simple Operational Risk Event Workflow for the Initial Reporter of an Event

KEY POINTS

- Internal loss data collection is often required for regulatory compliance, but it also provides valuable business benefits as it allows a firm to learn from past events.
- Losses are categorized into appropriate risk types, often using the Basel II categories which are:
  - Internal fraud
  - External fraud

- Employment Practices and Workplace Safety
- Clients, Products, and Business Practices
- Damage to Physical Assets
- Business Disruption and System Failures
- Execution, Delivery, and Process Management

- Policies and procedures are needed to set minimum criteria for loss data collection and to establish the collection process methodology. These need to consider the following key data elements:
  - Threshold for mandatory collection
  - Calculation of gross and net amounts
  - Gains, near-misses, and opportunity costs
  - Accounting adjustments
  - Recoveries
  - Selection of appropriate dates
  - Timing of including legal events, including treatment of legal fees and reserves
  - Allocation methodologies for centralized events
  - Boundary events with credit risk and market risk elements
  - Action tracking of mitigating activities
  - Nonfinancial impacts
- A loss database IT system is needed and might be integrated with other elements of the operational risk framework.

REVIEW QUESTIONS

1. Which of the following are Basel II Level 1 operational risk categories?

I. Clients, Products, and Business Practices
II. Employment Practice and Workplace Safety
III. Internal Fraud
IV. Damage to Systems
V. Unauthorized Trading

a. I only
b. I and II only
c. I, II, and III only
d. I, II, III, and IV only
e. All of the above

A U.S. bank's operational risk department has established a loss data system, which is accessible on the intranet by all employees and requires the completion of several fields, some of which are mandatory. All operational risk loss events over $10,000 must be entered into the system. An employee in the trade support department has discovered that an

error has been made by a trader. The trader has written a buy order on his blotter, but has entered a sell order into the trading systems. This has resulted in a loss of $150,000.

Using the information above, answer questions 2 through 4.

2. The loss event should be mapped to which of the following level 1 Basel II categories?
   a. Trading Error
   b. Execution, Delivery, and Process Management
   c. Business Disruption and System Failure
   d. Transaction Capture, Execution, and Maintenance
   e. Data Entry, Maintenance, or Loading Error
3. Why should the trade support employee enter the loss event into the database? Select the best answer.
   a. Because the trader should be free to focus on making a profit for the firm
   b. Because it might not have been the trader's fault
   c. Because the trade support employee is in the back office
   d. Because $150,000 is over the threshold
   e. Because every employee is responsible for reporting operational risk events
4. The trade support employee decides not to enter the data into the loss event database and does not inform anyone of the error. What is most serious consequence of this action? Select the best answer.
   a. He is risking being fired for breaching company policy.
   b. The trader cannot learn from his mistake.
   c. Audit will issue an audit point if the omission is discovered.
   d. Effective operational risk management in the firm is undermined.
   e. The firm might fail its Basel II examination.

NOTES

1. JPMorgan Chase & Co., Annual Report, 2011, p. 166.
2. Basel II provides minimum requirements.
3. www.bis.org/publ/bcbs196.pdf, section 88.
4. Ibid., section 85.
5. Ibid., section 86.
6. Ibid., section 89.
7. Ibid., section 87(a).
8. Ibid., section 87(b), which states: "Rapidly recovered loss events are operational risk events that lead to losses recognized in financial statements that are recovered over a short period. For instance, a large

internal loss is rapidly recovered when a bank transfers money to a wrong party but recovers all or part of the loss soon thereafter. A bank may consider this to be a gross loss and a recovery. However, when the recovery is made rapidly, the bank may consider that only the loss net of the rapid recovery constitutes an actual loss. When the rapid recovery is full, the event is considered to be a 'near miss.'"

9. Ibid., section 87.
10. Ibid., section 135.
11. Ibid., section 134.
12. Bank for International Settlements, "International Convergence of Capital Measurement and Capital Standards: A Revised Framework, 2004, section 673.
13. See note 3, p. 166.

CHAPTER 8

External Loss Data

In this chapter, we consider the use of external loss data in the operational risk framework. In addition to the events that have occurred within a firm, the operational risk department will look at those that have occurred outside the firm. These events can offer valuable insight into the operational risks faced at the firm, and may also provide input into any operational risk capital calculation. External data is also a required element in an advanced measurement approach (AMA) capital calculation. The use of external data in capital calculations is considered further in Chapter 12.

EXTERNAL OPERATIONAL RISK EVENT DATA

External events are useful in many areas of the firm's operational risk framework. They can help inform the risk and control self-assessment activities, they can provide sample input for scenario analysis and they might be used to develop key risk indicators that monitor the changing business environment.

The role of external data in the operational risk framework is illustrated in Figure 8.1.

External events are often of real interest to senior management, who may be surprised to discover that major new headlines are associated with operational risk. External data is therefore a key element in the development of a strong operational risk culture and awareness. Seeing events occur in the industry among peers and competitors helps to underscore the importance of effective operational risk management and mitigation.

An example of an operational risk event that had a huge impact on the discipline was the $7 billion unauthorized trading scandal at Société Générale in 2006, which is discussed later in the chapter. This was an internal loss data event for Société Générale, but for the rest of the industry

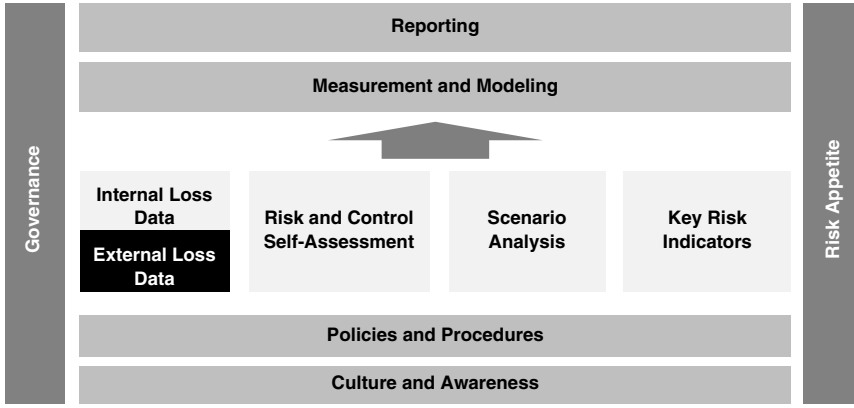

FIGURE 8.1 The Role of External Loss Data in the Operational Risk Framework

it was a very large external event that underscored the size of losses that can be experienced as a result of operational risk.

Despite the lessons learned from that event, the industry saw another huge unauthorized trading event at UBS in 2011. This led financial firms to revisit what they had learned from Société Générale just five years earlier and to reassess the way that they respond to large external events to ensure that the lessons have truly been learned. The UBS event is discussed in more depth in Chapter 18.

Chapter 18 considers several operational risk case studies. Each of those cases would be important external data points for the firms that were not involved (and painful internal loss data points for those that were).

SOURCES OF EXTERNAL LOSS EVENT DATA

There are many good online sources of operational risk event data in the form of news articles, journals, and e-mail update services. Some operational risk system vendors also have external databases that they make available on a subscription basis. For example, SAS offers an external database to its technology users, and IBM offers a subscription service called IBM® Algo FIRST®.[1] There are also consortiums of operational risk losses.

External events are a valuable source of operational risk information on an individual event basis and also as a benchmarking tool. Comparing internal loss patterns to external loss patterns can provide insight into whether the losses in a firm reflect the usual losses in their industry.

Subscription Databases

These databases include descriptions and analyses of operational risk events, gleaned from legal and regulatory sources and from news articles, and they provide helpful data to assist with mapping the events to the appropriate business lines, risk categories, and causes. The mission of these external databases is to collect tail losses and so to provide examples of potential large exposures.

For example, the total operational risk losses to date by risk category in the IBM Algo FIRST database are represented in Table 8.1.

From these statistics it is clear that a majority of the operational risk events that are included in this database, 46 percent of all records, fall into the category of Clients, Products, and Business Practices. This category also accounts for 48 percent of the dollar value of the losses.

TABLE 8.1 Total Operational Risk Losses Recorded to Date in Algo FIRST, Q4 2012

Event Type	Losses ($)	% of Losses	Records	% of Records	Average Loss ($)
Business Disruption and System Failures	5,941,530,424	0.41%	113	1.54%	52,579,915
Clients, Products, and Business Practices	704,366,741,158	48.25%	3,381	46.11%	208,330,891
Damage to Physical Assets	280,556,835,241	19.22%	233	3.18%	1,204,106,589
Employment Practices and Workplace Safety	12,793,739,772	0.88%	438	5.97%	29,209,452
Execution Delivery and Process Management	97,465,053,049	6.68%	534	7.28%	182,518,826
External Fraud	57,551,520,972	3.94%	712	9.71%	80,830,788
Internal Fraud	301,091,891,856	20.63%	1,921	26.20%	156,737,060
Grand Total	**1,459,767,312,472**	**100.00%**	**7,332**	**100.00%**	**199,095,378**

Source: IBM Algo FIRST for Web Edition on Cloud, Q4 2012.

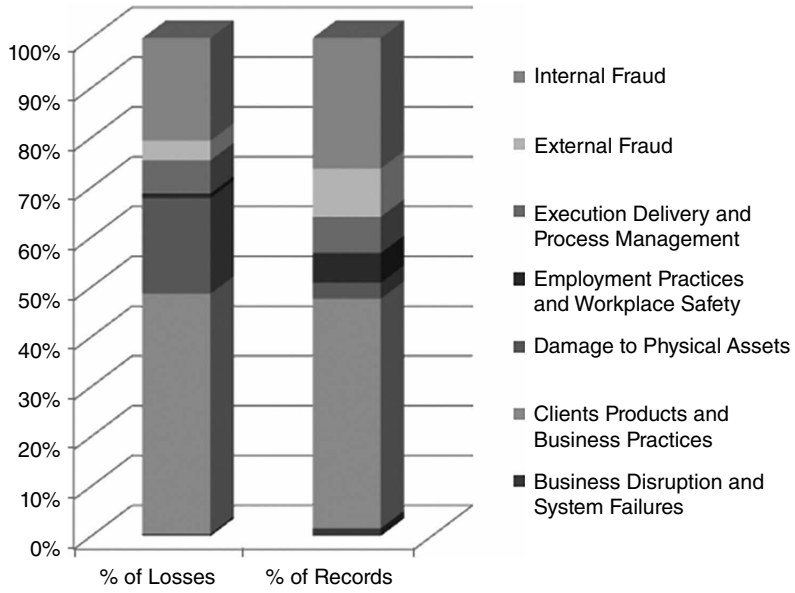

FIGURE 8.2 Percentage of Dollar Losses and Number of Events to Date for the Financial Services Industry[2]

Although Internal Fraud accounts for only 26 percent of the records, this category represents 21 percent of the dollar loss amount. Damage to Physical Assets is the next most expensive category, with only 3 percent of the loss events, but an impressive 19 percent of the cost of losses.

This information is further illustrated in Figure 8.2.

This shows that in an external database such as IBM Algo FIRST (FIRST) the operational risk data collected suggests that the losses from Internal Fraud, Damage to Physical Assets, and Client, Products, and Business Practices are much more significant than those from other categories. However, it is important to note that the FIRST data includes business lines other than the Basel BIS business lines. This accounts for the relatively high Damage to Physical Assets losses as insurance company losses are included.

It is also possible to examine a subset of losses in FIRST by BIS business lines as follows. In Table 8.2, all losses attributed to businesses that are not one of the BIS business lines have been removed.

It can be seen from this view that although about 10 percent of events occur in Retail Brokerage, that business line has generated only 1 percent of the dollar value of the losses, as the average losses in this business line are relatively small. In contrast, Corporate Finance generated only 9 percent of

TABLE 8.2 FIRST Losses to Date by BIS Business Line, Q4 2012

BIS Business Unit	Losses ($)	% of Losses	Records	% of Records	Average Loss ($)
Agency Services	4,092,601,937	0.35%	174	2.22%	23,520,701
Asset Management	169,054,229,189	14.40%	1,284	16.37%	131,662,172
Commercial Banking	274,983,936,373	23.42%	1,388	17.70%	198,115,228
Corporate Finance	206,271,120,093	17.56%	706	9.00%	292,168,725
Payment and Settlement	31,938,754,339	2.72%	463	5.90%	68,982,191
Retail Banking	278,008,980,318	23.67%	1,631	20.79%	170,453,084
Retail Brokerage	15,260,092,920	1.30%	810	10.33%	18,839,621
Trading and Sales	194,759,791,628	16.58%	1,388	17.70%	140,316,853
Grand Total	**1,174,369,506,797**	**100.00%**	**7,844**	**100.00%**	**149,715,643**

the events but 18 percent of the dollar value of the losses, as losses in this line tend to be more expensive. The relative weight of loss amounts and number of events in the FIRST data is represented in Figure 8.3.

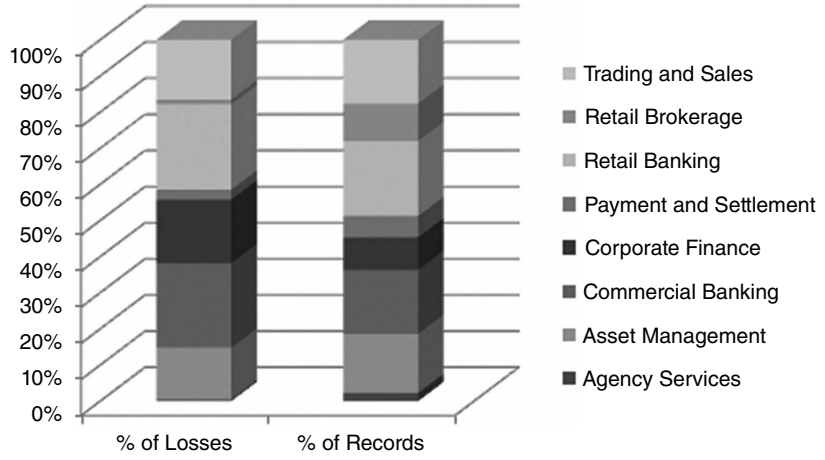

FIGURE 8.3 Percentage of Losses and Number of Events to Date, by BIS Business Line in FIRST[3]

This analysis is based on the publicly available data for operational risk events and, as such, is subject to reporting bias, as will be discussed further later in this chapter.

FIRST external data is useful to financial services firms as they considers its own risk profile and compares it to the risk levels in the industry for each risk category and business line. The data also provides insight into the types of events that have occurred in the industry, but which the firm has not yet experienced itself.

Consortium Data

In addition to subscription-based external data services, there are consortium-based operational risk event services that provide central data repositories and benchmarking services to their members. ORX provides such a service to its 67 members.

ORX gathers operational risk event data from its members and produces benchmarking information. It applies quality assurance standards around the receipt and delivery of data to promote members' anonymity and to provide consistency in definitions.

Unlike news-based subscription services, ORX data does not suffer from the availability bias that skews the IBM® Algo FIRST® data, which relies on public sources of data. In contrast, *all* operational risk events are provided anonymously into the database. However, the data relate only to a subset of financial services, those member banks that provide data to ORX. ORX publishes reports that summarize the data. Table 8.3 is derived from ORX data and illustrates the number of losses and the amount of losses in euros for each business line and each risk category.

ORX use slightly different business lines, as they split out Retail Banking into two groups: Retail Banking and Private Banking. They also rename Payment and Settlement as Clearing.

To date, ORX has gathered nearly 30,000 events that have cost their consortium members over €100 billion euros. The cost of operational risk is abundantly clear. This table shows that ORX business line data is dominated by Retail Banking events, both in size of losses and frequency of events.

To further understand the relative impact to the different businesses and from the different risk categories, it is helpful to take another look at this data in percentage format as shown in Table 8.4.

From Table 8.4 we can see that nearly 58 percent of the total number of events is generated in the Retail Banking business area and most of those are in the External Fraud category. Trading and Sales and Commercial Banking are the next business lines, with about 10 percent of the total number of events each.

TABLE 8.3 Number and Amount of Losses (EURO) by Business Line and Risk Category

	Internal Fraud	External Fraud	Employment Practices and Workplace Safety	Clients, Products, and Business Practices	Damage to Physical Assets	Business Disruptions and System Failure	Execution, Delivery, and Process Management	Total Number of Losses, Total Amount of Losses
Corporate Finance	40 / 27,808,954	259 / 201,187,224	303 / 118,968,064	589 / 10,338,924,836	234 / 19,809,931	24 / 1,338,255	1,220 / 1,271,895,367	2,669 / 11,979,932,631
Trading and Sales	229 / 2,239,862,424	364 / 2,161,739,938	1,275 / 408,306,565	1,941 / 7,433,539,652	153 / 33,297,270	1,690 / 299,546,583	23,365 / 9,914,939,994	29,017 / 22,491,232,426
Retail Banking	7,320 / 1,574,185,214	72,562 / 6,900,955,788	21,060 / 2,409,914,928	20,705 / 37,059,980,235	2,912 / 1,024,928,564	2,132 / 1,710,492,902	40,660 / 11,926,956,855	167,351 / 62,607,414,487
Commercial Banking	538 / 689,292,132	9,283 / 3,856,185,404	1,113 / 137,566,589	5,572 / 4,686,349,743	268 / 39,160,870	558 / 336,939,426	10,975 / 4,020,356,604	28,307 / 13,765,850,768
Clearing	67 / 48,316,882	1,219 / 124,640,083	129 / 25,551,512	283 / 473,570,941	11 / 2,203,899	579 / 88,231,353	2,732 / 838,347,699	5,020 / 1,600,862,369
Agency Services	72 / 98,922,139	749 / 145,382,012	575 / 121,902,241	1,210 / 3,235,132,043	40 / 8,630,010	241 / 29,142,665	9,116 / 1,578,861,818	12,003 / 5,217,972,927
Asset Management	90 / 227,632,060	203 / 72,570,551	315 / 158,123,983	1,281 / 2,290,082,550	38 / 50,088,892	241 / 33,092,369	4,670 / 1,568,696,090	6,838 / 4,400,286,493
Retail Brokerage	887 / 404,552,140	511 / 74,433,686	2,652 / 995,217,387	11,682 / 4,184,548,472	39 / 10,819,472	161 / 17,347,297	4,496 / 648,575,461	20,428 / 6,335,493,916
Private Banking	257 / 428,501,503	1,076 / 395,668,975	509 / 98,393,103	4,175 / 2,457,942,214	52 / 5,135,532	182 / 13,534,865	5,071 / 645,778,821	11,322 / 4,044,955,013
Corporate Items	86 / 299,929,406	425 / 40,274,573	2,741 / 475,482,092	915 / 1,629,724,162	330 / 206,336,028	206 / 45,974,521	1,567 / 1,037,628,696	6,270 / 3,735,349,479
Total Number of Losses / Total Amount of Losses	9,586 / 6,039,002,852	86,651 / 13,973,038,233	30,672 / 4,949,426,465	48,353 / 73,789,794,849	4,077 / 1,400,410,468	6,014 / 2,575,640,237	103,872 / 33,452,037,404	289,225 / 136,179,350,508

These data were generated using the Q4 2012 ORX Global Data Set, which contains losses up to the end of 2012 Q3 (most recent date of recognition), September 30, 2012

TABLE 8.4 The Percentage Contribution to Number of Events and Amount of Losses by Business Line and Risk Category

	Internal Fraud	External Fraud	Employment Practices and Workplace Safety	Clients, Products, and Business Practices	Damage to Physical Assets	Business Disruptions and System Failure	Execution, Delivery, and Process Management	Total Number of Losses, Total Amount of Losses
Corporate Finance	0.0% / 0.0%	0.1% / 0.1%	0.1% / 0.1%	0.2% / 7.6%	0.1% / 0.0%	0.0% / 0.0%	0.4% / 0.9%	0.9% / 8.8%
Trading and Sales	0.1% / 1.6%	0.1% / 1.6%	0.4% / 0.3%	0.7% / 5.5%	0.1% / 0.0%	0.6% / 0.2%	8.1% / 7.3%	10.0% / 16.5%
Retail Banking	2.5% / 1.2%	25.1% / 5.1%	7.3% / 1.8%	7.2% / 27.2%	1.0% / 0.8%	0.7% / 1.3%	14.1% / 8.8%	57.9% / 46.0%
Commercial Banking	0.2% / 0.5%	3.2% / 2.8%	0.4% / 0.1%	1.9% / 3.4%	0.1% / 0.0%	0.2% / 0.2%	3.8% / 3.0%	9.8% / 10.1%
Clearing	0.0% / 0.0%	0.4% / 0.1%	0.0% / 0.0%	0.1% / 0.3%	0.0% / 0.0%	0.2% / 0.1%	0.9% / 0.6%	1.7% / 1.2%
Agency Services	0.0% / 0.1%	0.3% / 0.1%	0.2% / 0.1%	0.4% / 2.4%	0.0% / 0.0%	0.1% / 0.0%	3.2% / 1.2%	4.2% / 3.8%
Asset Management	0.0% / 0.2%	0.1% / 0.1%	0.1% / 0.1%	0.4% / 1.7%	0.0% / 0.0%	0.1% / 0.0%	1.6% / 1.2%	2.4% / 3.2%
Retail Brokerage	0.3% / 0.3%	0.2% / 0.1%	0.9% / 0.7%	4.0% / 3.1%	0.0% / 0.0%	0.1% / 0.0%	1.6% / 0.5%	7.1% / 4.7%
Private Banking	0.1% / 0.3%	0.4% / 0.3%	0.2% / 0.1%	1.4% / 1.8%	0.0% / 0.0%	0.1% / 0.0%	1.8% / 0.5%	3.9% / 3.0%
Corporate Items	0.0% / 0.2%	0.1% / 0.0%	0.9% / 0.3%	0.3% / 1.2%	0.1% / 0.2%	0.1% / 0.0%	0.5% / 0.8%	2.2% / 2.7%
Total Number of Losses / Total Amount of Losses	3.3% / 4.4%	30.0% / 10.3%	10.6% / 3.6%	16.7% / 54.2%	1.4% / 1.0%	2.1% / 1.9%	35.9% / 24.6%	100.0% / 100.0%

These data were generated using the Q4 2012 ORX Global Data Set, which contains losses up to the end of Q3 2012 (most recent date of recognition), September 30, 2012.

Data sourced from ORX as in Table 8.1 above.

Retail Banking also has a lion's share of the total costs of events, with 46 percent of the total losses. Trading and Sales has over 16 percent of losses, and Commercial Banking and Corporate Finance follow with 10 percent and 9 percent.

It is clear that External Fraud and Execution, Delivery, and Process Management produce the greatest number of events in a risk category, accounting for nearly 36 percent of the number of events and 25 percent of the total costs.

Clients, Products, and Business Practices accounts for about 17 percent of the events, but carries more than 50 percent of the total loss amount. This demonstrates that for the member banks of ORX, Clients, Products, and Business Practices events tend to be larger events. It is for this reason that many firms carefully investigate this category in scenario analysis to attempt to identify potential "fat tail" events—that is, events that are infrequent but very large.

The data can also be used to visually represent the relative levels of operational risk in each business line, as shown in Figure 8.4.

Figure 8.4 clearly illustrates the relatively high levels of operational risk that exist today in the Retail Banking sector.

COMPARISONS BETWEEN SUBSCRIPTION AND CONSORTIUM DATABASES

The differences in collection method and scope have an interesting impact on the relative distribution of the losses between ORX and IBM® Algo FIRST® (FIRST) data. ORX data shows significantly different patterns to those in the FIRST database.

Size of Losses by Risk Category

If we compare the data in FIRST and in ORX we can see strong differences between the two data sets. First, let us compare the size of losses in the two sources.

As can be seen in Figure 8.5, the FIRST database contains a significantly higher percentage of losses being attributed to Internal Fraud cases than is indicated in the ORX data. In contrast, the ORX data shows a significantly higher percentage of Execution, Delivery, and Process Management (EDPM) losses than is indicated in the FIRST data. This may be explained by the fact that not all EDPM events are reported in the press, so many of those events would not appear in the FIRST database. This is an unavoidable collection bias that impacts FIRST's data.

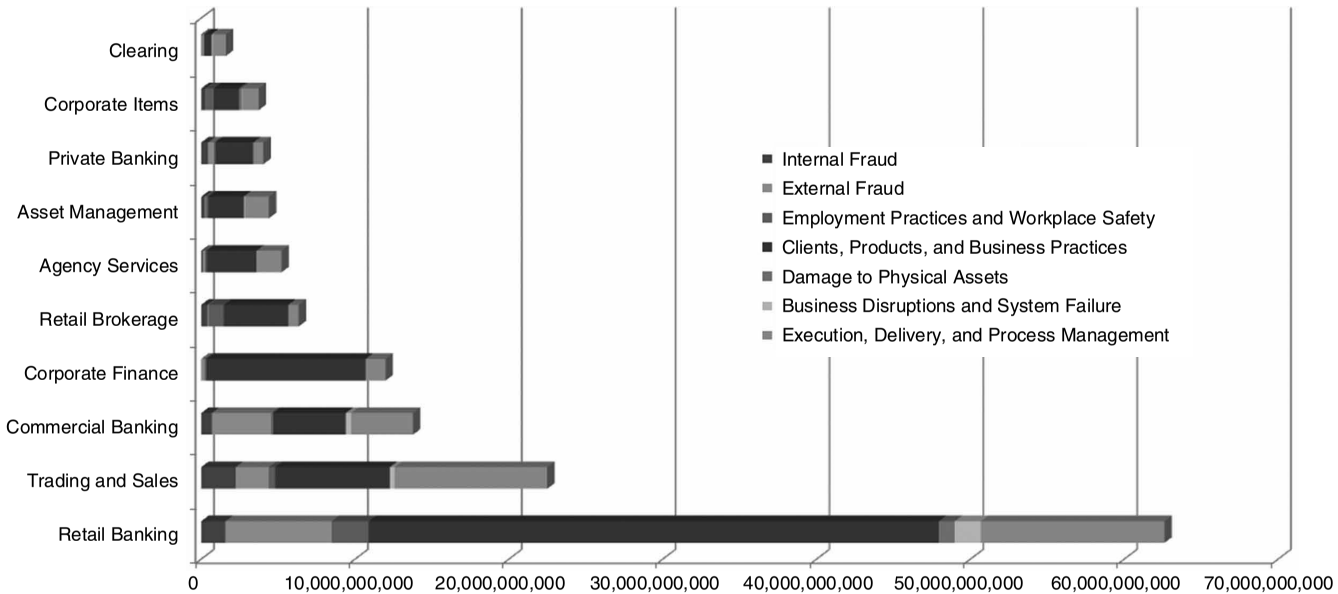

FIGURE 8.4 Dollar Value Losses to Date, by Risk Category for All Business Lines

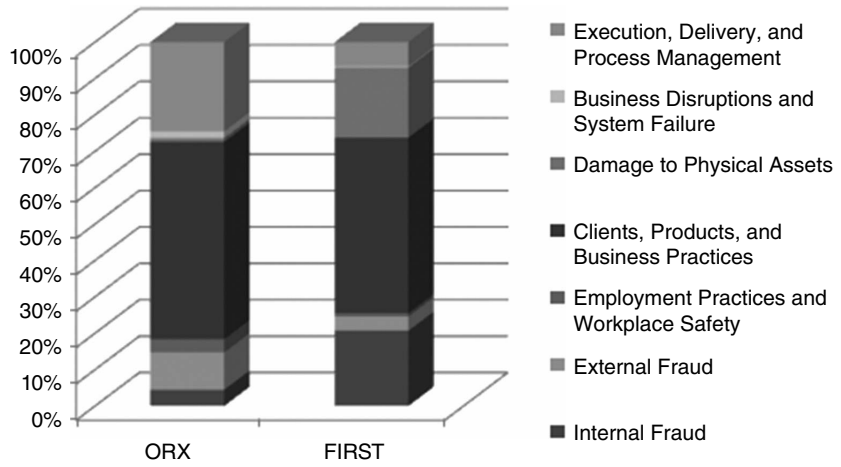

FIGURE 8.5 Percentage of Dollar Value Losses to Date in ORX and First Databases, by Event Category, for All Business Lines[4]

However, these EDPM events are included in the ORX data as it is supplied directly from the member banks. Alternatively, this difference might be driven by a difference in the scope of firms that are covered in the two databases. ORX membership is limited, with not all banks participating and so ORX also suffer from a collection bias.

In contrast, FIRST collects data on all firms, including a significant number of firms that are outside of Basel II, and that are not BIS business lines, for example, insurance companies.

Frequency of Losses by Risk Category

A comparison of the relative frequency of events in the two databases is also interesting and is illustrated in Figure 8.6.

It is clear from Figure 8.6 that EDPM events rarely result in public press coverage, and so are missing from the FIRST data. ORX also has larger number of External Fraud events than FIRST, suggesting that External Events are often successfully kept out of the press. The ORX underlying data show that the dominance of External Fraud events occurs mostly due to the participation of retail banks in the consortium. (Most, if not all, ORX members had a retail banking division for the period covered by the report). Retail Banking includes credit card services, and so it may be that this dominance by the External Fraud category is driven by many relatively small credit card and retail banking frauds. The threshold for loss data delivery to

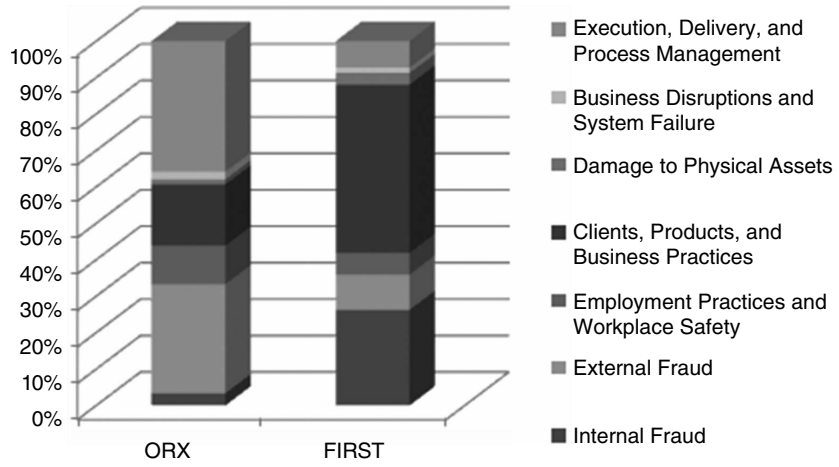

FIGURE 8.6 Percentage of Number of Events to Date in ORX and FIRST Databases, by Event Category, for All Business Lines
Sources: ORX Report, Q4 21012 and FIRST Database, Q4 2012.

ORX is €20,000, so "small" losses are obviously only relatively small when compared to the very large frauds that are covered in the media.

Size of Losses by Business Line

When comparing the relative role of the different business lines, there is also a marked difference in the ORX and FIRST data when comparing the size of losses. For Figure 8.7 and 8.8 the ORX data has been mapped[5] into equivalent BIS lines to allow for a comparison with FIRST data. Similarly, all non-BIS business line data have been removed from the FIRST data.

It is clear from this chart that while FIRST's loss amounts are dominated by Commercial Banking and then Retail Banking, in ORX the loss amounts are more heavily weighted to the Retail Banking business line. In the ORX database, Commercial Banking accounts for a smaller percentage of the financial value of the losses. This is probably a reflection of the fact that recent commercial banking events have made it into the press, and so into FIRST's data, while those firms might not be members of ORX.

ORX has an additional category "Corporate Items," which it does not map to a Basel business line. Events in this category are corporate-level events such as the kidnapping of the CEO or fines for group-level financial misreporting.

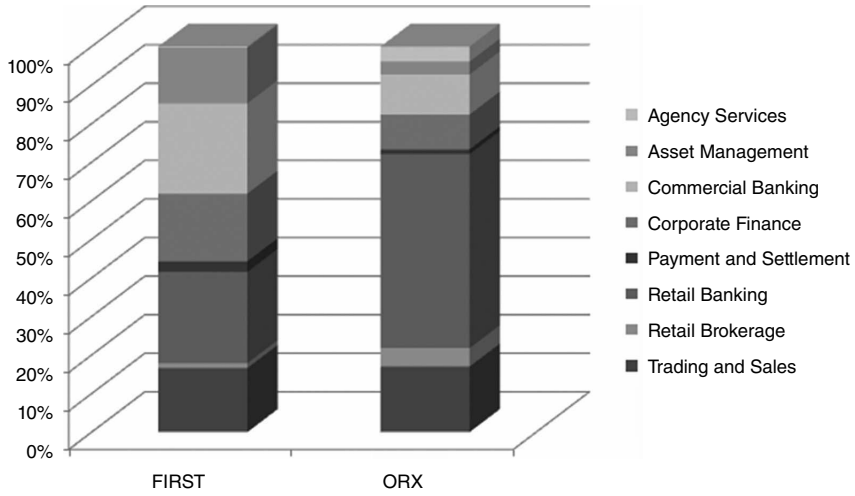

FIGURE 8.7 Percentage of Value of Losses to Date in ORX and FIRST Databases, by BIS Business Lines
Sources: ORX Report, Q4 2012, and FIRST Database, Q4 2012.

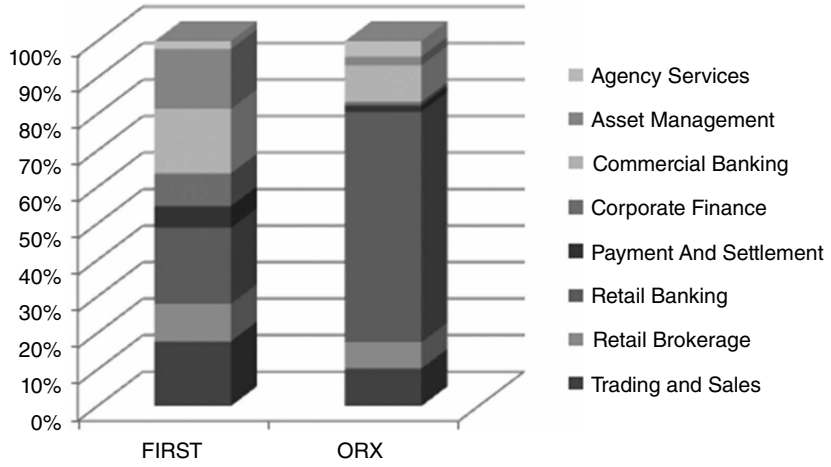

FIGURE 8.8 Percentage of Number of Events to Date in ORX and FIRST Databases, by Business Lines
Sources: ORX Report, Q4 2012, and FIRST Database, Q4 2012.

Number of Events by Business Line

Similarly, the number of events in the two databases can be compared (see Figure 8.8).

This chart dramatically demonstrates how the ORX data is driven by Retail Banking events, whereas the FIRST data has events more evenly distributed among the business lines. The majority of events occur in Retail in the ORX data. Retail Banking also has the majority in the FIRST database, but at a much slimmer margin.

CHALLENGES OF EXTERNAL DATA

Many operational risk functions use ORX or FIRST or other provider data and then supplement these with their own research by subscribing to online news feeds and relevant industry journals.

However, it is clear from the data set comparisons above that these data must be used with caution. There are several challenges with external data.

First, if the external data are gathered from news sources, then they are subject to a bias in reporting. Only events that are interesting to the press are reported in the press, resulting in a bias in favor of illegal and dramatic events over errors. For example, a large fraud will receive intensive coverage, while a major systems outage might not make it into any press report. It is also unlikely that a major gain will make the press in the same way that a major loss would, although the same lessons could be learned in both cases.

Second, it can be difficult to determine whether an event is relevant. The fact that a firm has the same business line does not mean it could have the same event occur, as it may have a different product or a stronger (or weaker) control environment. Indeed, many external events might be ignored simply because they "could not happen here" for one or many reasons. However, external data are not best used to try to spot an exact event that should be avoided, but rather to determine the types of errors and control failings that can occur so as to avoid similar (rather than identical) losses.

An external event may have direct relevance regardless of the exact details. For example, the Société Générale event (which is considered in detail later) led to many firms overhauling their fraud controls, regardless of whether they had any traders working on the exact same desks as Mr. Kerviel.

Third, the use of benchmarked data relies on the quality of the underlying data, and there may be a chance that the comparisons made are not accurate due to a different interpretation of the underlying definitions.

However, if all of these challenges are acknowledged, then external data have a very valuable role to play in operational risk management. It provides

insight into lessons that can be learned, prior to an event's occurring at the firm. It demonstrates that the size of an event may be beyond the initial estimation made by the firm. It provides context and highlights trends in the industry.

Internal and external operational risk events provide a rich source of data on what has already gone wrong. It is possible to use these data to implement mitigating controls to prevent future repetitions of the same events. Moreover, operational risk event data provide a valuable input into the other elements of the operational risk framework that will be designed to predict potential events that have not yet occurred.

Loss data provides useful examples for risk and control self-assessment and scenario analysis discussions and analysis, as well as key risk indicators (KRIs) that can indicate trends of losses and control weaknesses.

Société Générale and the External Event that Shook the Operational Risk World

This event is reported in IBM Algo FIRST as follows:

> *In what the Wall Street Journal (1/24/2008) called a "singular feat in the world of finance" Societe Generale announced a €4.9 billion (USD $7.2 billion) loss on January 24, 2008, arising from the misdeeds of a single rogue trader. The bank characterized the largest rogue trading event to date as involving "elaborate fictitious transactions" that allowed Jerome Kerviel to circumvent its internal controls. The trades involved the arbitrage of "plain vanilla" stock-index futures. Mr. Kerviel had previously worked in a back office function and learned how to circumvent the bank's systems. Although he was initially characterized by the governor of the Bank of France as a "computer genius" later he was described as an unexceptional employee who worked very hard to conceal unauthorized trading positions, which SocGen estimated to have a value of €50 billion ($73.26 billion). The French Finance Ministry said that Kerviel's rogue trading started in 2005; he was allegedly given a warning at the time concerning trading above prescribed limits. In addition to the €4.9 billion trading loss, the French Banking Commission levied a €4 million fine against Societe Generale on July 4, 2008, bringing the total loss amount to €4,904,000,000. On October 5, 2010, a court in Paris sentenced Mr. Kerviel to three years' imprisonment, plus a two year suspended sentence and ordered him to repay €4.9 billion ($6.7 billion) to his employer.*[6]

On October 24, 2012, a French appeals court upheld Kerviel's fraud conviction and lifetime trading ban.

This external event galvanized the operational risk world as it clearly demonstrated the dangers that exist in unmitigated operational risk. In 2008, many firms were still engaged in developing their early operational risk frameworks and were often focused on first-run delivery of new reporting, new loss data tools, and new adaptions to their RCSA and scenario analysis programs. The regulatory requirements were paramount in many programs, with the business benefits being developed as rapidly as possible, but sometimes lagging behind the urgent regulatory pressures.

However, when the news hit of Mr. Kerviel's audacious activities and their multibillion-dollar impact on his firm many heads of operational risk found themselves in front of their executive management being asked the urgent question: "Could that happen here?"

This was a classic large operational risk event in that it resulted from numerous control failings. Mr. Kerviel's job was to make arbitrage trades that would result in small gains, but he began taking unauthorized "directional" positions starting in 2005, and these grew in size until he was discovered in January 2008.

Reports on the events suggest that Mr. Kerviel may have been more motivated by a sense of pride than an attempt to defraud the firm. His unauthorized activities did not result in secret transfers into his bank account; they resulted in huge positions at the bank.

At one point, Mr. Kerviel's activities allegedly resulted in gains for the firm that have been estimated to have been as high as €1 billion in 2007. It has been suggested that he realized that these gains were too large to explain and so pursued a strategy to reduce them. That strategy, it is alleged, resulted in losses of €1.5 billion by February 2008. The adverse market conditions that existed when Société Générale discovered the unauthorized trading and unwound the positions resulted in the loss growing to €4.9 billion.[7]

This is an extreme example of how an operational risk event can be exacerbated by a market risk event.

IBM Algo FIRST provides an in-depth prose analysis of the event based on extensive press reviews. The highlights of the many contributing factors that are alleged can be summarized as follows:

1. Mr. Kerviel engaged in extensive unauthorized activities in order to demonstrate his prowess as a trader, rather than to defraud the bank.
2. He was insufficiently supervised and at times had no supervisor at all.
3. He had worked in the middle and back offices prior to becoming a trader and used his knowledge of those controls to ensure that his activities were not detected.

4. He gained password access to back office systems that allowed him to manipulate data and approve his own trades.

It is alleged that many red flags were raised but were ignored or were dismissed as unimportant.

> *The head of the Bank of France, Christian Noyer, said that Mr. Kerviel managed to breach "five levels of controls." The controls were identified in the earlier Mission Green report[8] and included cancelled or modified transactions; transactions with deferred dates; technical (internal) counterparties; nominal (non-netted exposures) and intra-month cash flows. In addition, the second and more detailed Mission Green report[9] identified a host of supervisory lapses, organizational gaps, and warning signs that were never heeded.[10]*

It is alleged that there were numerous other red flags that were not heeded including:

1. Mr. Kerviel requested an unusually high bonus due to his above market returns.
2. He frequently breached limits, and despite being reprimanded for this in the past, was able to continue to do so.
3. Concerns were raised by EUREX regarding his trading volume, but were dropped after a response from Mr. Kerviel satisfied their concerns.
4. At least 75 compliance alerts were raised, but were dismissed when Mr. Kerviel supplied minimal, and sometimes forged, documentation to explain his unusual activity.
5. Mr. Kerviel never took his vacation time, allowing him to be on site to continue to maintain and conceal his unauthorized activities.
6. The bank had to rely on manual processing due to inadequate technology to support the increasing volumes in the market.
7. Net cash flows were monitored, whereas monitoring of nominal flows might have revealed the unauthorized activity.

IBM Algo FIRST categorizes this event, as shown in Table 8.5.

ORX now provides a news service also, and they categorized this event as shown in Figure 8.9.

The industry responded to this event with energy. Operational risk teams met with senior management, as executive teams and boards asked whether it could happen at their firm. Perhaps for the first time, the possible size of an operational risk event was fully appreciated, and the operational risk function had an opportunity to demonstrate its relevance and importance.

TABLE 8.5 Classification in IBM Algo FIRST

Entity Type	Financial services/Banking/commercial/Full-service bank
Business Unit Type	Trading and Sales (BIS)/Trading
Service/Product Offering Type	Derivatives, structured products, and commodities/ derivative products/futures and options/equity index futures
Contributory/ Control Factors	Corporate Governance/General Corporate Governance Issues, Corporate/Market Conditions/Corporate and Market Conditions, Employee Action/Inaction/Employee Misdeeds, Employee Action/Inaction/Employee Omissions, Lack of Control/Failure to Question Above-Market Returns, Lack of Control/Failure to Reconcile Daily Cash Flows, Lack of Control/Failure to Test for Data Accuracy, Lack of Control/ Lack of Internal Controls, Lack of Control/Lax Security, Lack of Control/Rules, Regulations, and Compliance Issues, Management Action/Inaction/Lack Management Escalation Process, Management Action/Inaction/Undertook Excessive Risks,Omissions/Failure to Set or Enforce Proper Limits,Omissions/Failure to Supervise Employees,Omissions/ Inadequate Due Diligence Efforts,Omissions/Omissions and Lapses,Organizational Structure/Inadequate Organizational Structures, Organizational Structure/Organizational Gap(s), Strategy Flaw/Inadequate Technology Planning Process, Organizational Structure/Organizational Structure—General, Lack of Control/Lack of Internal Controls—General, Management Action/Inaction/Undertook Excessive Risks, Omissions/Omissions—General
Loss Impact	Direct Loss/Regulatory/Compliance/Taxation Penalty (BIS)/Fines/Penalties, Direct Loss/Write-Down (BIS)/ Write-Downs, Indirect Loss/Management Remediation, Indirect Loss/Ratings Agency Downgrade/Ratings Watch, Indirect Loss/Related Market Risk Losses, Indirect Loss/ Reputational (Nonmonetary), Indirect Loss/Share Price
Loss Detection Sources	Whistle Blowing/Employee Originated
Market Focus	Institutional Services
Event Trigger	People Risk Class/Trading Misdeeds/Unauthorized Trading/Activity above Limits/Unauthorized Trading—Proprietary Accounts
Basel Levels I & II	Internal Fraud/Unauthorized Activity/Trans type unauthorized (w/monetary loss)
Basel Business Line	Investment Banking/Trading and Sales/Proprietary Positions
Entity Type	Financial Services/Banking/Commercial/Full-Service Bank
Business Unit Type	Trading and Sales (BIS)/Trading

Event	Published in Media	Date of Occurrence – From	Date of Occurrence – To	Discovery Date	Date of Recognition / Settlement
	24/Jan/2008	01/Jan/2005	20/Jan/2008	19/Jan/2008	31/Dec/2007

Loss Amount USD	Loss Amount EURO	Provision	Boundary Risk
USD 7,232,400,000.00	EUR 4,900,000,000.00	No	Other Risk

Industry Event	Scenario	Product	Process
N/A	ROGUET - Rogue Trader	PD0310 - Equity Derivatives	PC0603 - Position or Portfolio Mgt (proprietary)

Parent Company	ORX Member	Role of Firm	AMA Status
N/A	Yes	LS0307 - Position Taking (Principal)	N/A

Cause 1	Cause 2	Cause 3
CS0206 - Unauthorised Activity	CS0204 - Management / Control of Staff	CS9999 - Not Identifiable

Counterparty	Jurisdiction / Choice of Law	Environmental Volatility
LS0212 - Not Identifiable	LS0105 - Western Europe (excluding United Kingdom)	LS0403 - Market Risk

FIGURE 8.9 ORX Classification of the Société Générale Event

Fraud risk assessments were conducted in many firms and numerous control improvements were implemented. Mandatory vacation policies were written, and enforced. Passwords were disabled for employees that had moved to new roles. Supervisory oversight was reviewed.

Industry forums were held as operational risk managers compared notes on how best to minimize the risk such an event could not happen in the industry again. As an external data point, the event galvanized many aspects of operational risk frameworks across the industry and also paved the way for how to respond to future serious events.

Work plans were drawn up to evaluate the current state of the controls that had failed at Société Générale and to kick off work to remediate any control gaps that might be uncovered. RCSAs and scenario analysis were updated in the unauthorized trading aspects of internal fraud. Working groups were formed, Board packs prepared, and external event tracking was enhanced. As IBM Algo FIRST notes in its longer description of the event:

> *The AFP press agency reported (October 8, 2010) that Société Générale's own efforts to enhance its internal controls in the wake of the event were estimate to have cost the bank at least 150 million euros over a three-year period.*

The Société Générale event shocked the financial services industry, and turned the spotlight on to operational risk. However, only three years later another startlingly similar event occurred at UBS and this will be discussed in the case studies in Chapter 20.

KEY POINTS

- Loss events that have occurred outside the firm can provide valuable insight into potential catastrophic events, as well as opportunities to benchmark internal data against the industry.

- Subscription databases use legal, regulatory, and press reports of events to provide analysis and categorization of operational risk events.
- Consortium databases collect data from members and share trends and benchmarking information with members.
- The methods of collection can produce biases in data that must be considered when analyzing external sources of data.

REVIEW QUESTION

1. Which of the following statements best describes the value of using external database sources?
   a. ORX consortium data provides a full data set for a bank to use for benchmarking.
   b. IBM® Algo FIRST® provides a full data set for a bank to use for benchmarking.
   c. A combination of ORX and FIRST data provides a full data set for a bank to use for benchmarking.
   d. ORX and FIRST provide helpful information on external loss data trends that can help inform a bank's operational risk framework.

NOTES

1. IBM Algo FIRST for Web Edition on Cloud. Property of IBM. 5725-H59 © Copyright IBM Corp. and others 1992, IBM, the IBM logo, ibm.com, Algo FIRST, and Algorithmics are trademarks of IBM Corporation, registered in many jurisdictions worldwide. SAS also has a subscription database available.
2. IBM Algo FIRST, 2012, 4th Quarter Overview, nonoperational risk categories removed.
3. See note 1.
4. *Sources:* ORX Report, 2012 and FIRST Database, 2012—4th Quarter Overview, nonoperational risk categories removed.
5. Clearing has been renamed Payment and Settlement, and Private Banking has been included in Retail Banking and items mapped to corporate items have been removed.
6. Reproduced with permission of IBM Algo FIRST.
7. Excerpted and reproduced with permission of IBM Algo FIRST.
8. Investigatory report published on February 20, 2008, by Société Générale.
9. Investigatory report published in May 2008 by Société Générale.
10. IBM Algo FIRST report.

CHAPTER 9

Business Environment Internal Control Factors: Key Risk Indicators

This chapter explores the benefits and challenges of the use of metrics in the operational risk (OR) framework. Metrics can provide the business environment and internal control factors (BEICF) needed for an AMA capital approach, but perhaps more important, they can provide insight into the changing operational risk environment.

KEY RISK INDICATORS

Key risk indicators, or KRIs, are used in the operational risk framework to keep a finger on the pulse of the changing risk environment. External risk factors, internal risk factors, and the control environment can be monitored using metrics.

In Basel II, there is a requirement for AMA banks to collect BEICF for use in the capital model. These BEICF have proved elusive and capital models have struggled with how to incorporate them. The use of BEICF in capital modeling is discussed later in Chapter 12.

However, it is common sense that monitoring our environment and our controls will lead to better operational risk management, regardless of their use in the capital model and all firms attempt to develop a key risk indicator (KRI) structure of some kind. Some are highly sophisticated, some are simple.

KRIs are an important pillar in the operational risk framework as illustrated in Figure 9.1.

At its most complex, a metrics or KRI program can lead to the danger of frisking the ant while the elephant walks by. That is to say, we can become

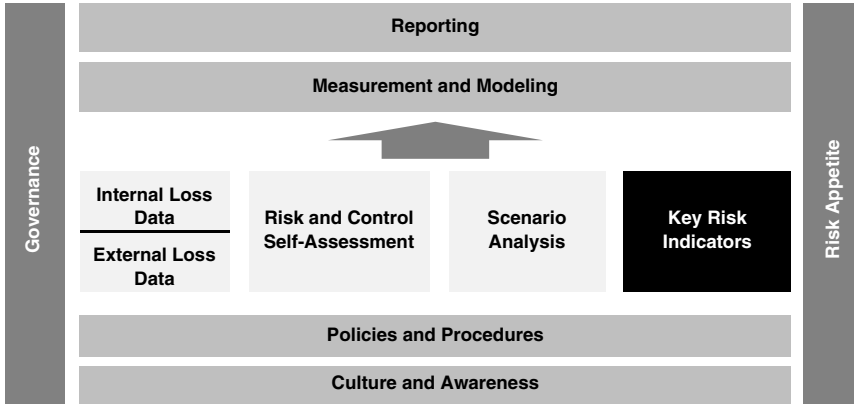

FIGURE 9.1 Key Risk Indicators in the Operational Risk Framework

so focused on detailed data that we miss the major looming operational risk that is not being capture in our metrics systems.

The challenge is to identify a suitable metric that is truly measuring risk levels. Most metrics only count something and should not be confused with a true KRI.

For this reason, it may be safer to refer to gathered metrics as "indicators" rather than KRIs until they have proven their worth. For example, the number of failed trades per day is a metric. However, this metric alone does not indicate rising or falling risk levels unless it is combined with other related metrics, such as volume. So an indicator that measures the percentage of failed trades in the total volume of trades is a more helpful indicator and might be a true KRI.

There are many types of indicators, and each has its own strengths and weaknesses and can be used effectively in the right place.

When considering the role of KRIs in the operational risk framework, it is important to remember that they provide input into the framework. They are not the end; they are simply one of the means to the end. There is a danger in relying too heavily on metrics in that we can become overconfident that we are collecting all of the right data, and that a green dashboard of metrics means everything is fine and operational risk is under control. Conversely, we may panic over a red dashboard when the all that has happened is that we set our thresholds too low.

An analogy may be helpful. If managing operational risk is like driving a car, then KRIs are the dashboard of the car. No one would be foolish enough to drive without a dashboard, as it tells us important information

such as our speed, our fuel levels, and whether we have any issues such as overheating or running low on oil.

But we do not drive with our heads down looking at the dashboard of our cars. We look ahead at the road to see where we are going and what is coming over the horizon. We learn to drive, and we drive safely and carefully.

To take the analogy one step further, sometimes, through no fault of our own, we get crashed into by a truck. That is why we have insurance, and that is why we calculate and hold operational risk capital. We hold capital for the rare catastrophic events that can occur, either through our own reckless behavior or through no fault of our own.

It is important to have a good functioning dashboard and to rely on it appropriately and build out the rest of the framework that you need in order to "drive safely."

Key Performance Indicators

Key performance indicators, or KPIs, measure how well something is performing, or how efficient it is. For example, the average time taken to resolve a help desk request would be a KPI. KPIs are used extensively in sales to track which sales area is performing best or which sales method is producing the best results.

Key Control Indicators

Key controls indicators, or KCIs, measure how effectively a control is working. For example, the number of viruses caught in a virus protection screen is a KCI. The number of viruses that got past the virus protection is also a KCI.

Whether a metric is a KPI or a KCI, it may be one of three types of metric: an exception monitor, a lagging indicator, or a leading indicator.

Exception Monitoring

Exception monitoring indicators raise a flag when an exception occurs. For example, if a report fails to print then this could produce a "yes" flag for a "Report Print Failure" indicator. Another example might be where a new product has been launched without the proper approvals. This could raise a red flag in the new-product approval process. More important, exception monitoring can raise red flags in urgent situations to ensure remediation.

Exceptions are easily understood as they have a binary outcome. They typically produce ad-hoc reporting to alert managers to the issue that has arisen.

Lagging Indicators

Lagging indicators track past activity and look for trends over time. Lagging indicators can be very useful but have limitations, as they can only show us what has already happened, not what is going to happen. As we all know, past performance is not necessarily an indication of future performance. However, analysis of trends can be helpful in the formation of strategy and in identifying changing risk profiles.

A KCI that is showing a constant deterioration of a control will allow for decisions to be made to alleviate any rising risk. Lagging indicators are the most common metrics in most reporting packs, and management is generally very comfortable interpreting them.

Perhaps the strongest lagging indicator in the operational risk framework is operational event data. The losses that were suffered in the past can be analyzed for trends and patterns.

However, as mentioned earlier, lagging indicators can give a false sense of urgency or complacency if they are not carefully designed and managed. Lagging indicators are often found in regular monthly and quarterly reporting decks.

Leading Indicators

A true KRI will be a leading indicator. Leading indicators attempt to predict points of emerging risk. They are rare. An example of a leading indicator might be customer complaints. A higher number of customer complaints might correlate with the size and number of class action lawsuits that a retail firm faces. If so, then the number of customer complaints is a leading indicator for legal risk.

Perhaps we can go further back the chain of causation. If it can be shown that a drop of more than 30 percent in the asset value in a customer account produces a significant increase in complaints, then a drop in asset value in an account becomes a leading indicator for legal risk.

If strong leading indicators can be found, they allow for preventative measures to be taken. In this example, whenever an account drops more than 30 percent, there could be a process in place to ensure that the customer is called within one day to discuss their needs and any changes they might wish to make.

Leading, lagging, and exception indicators are often monitored by line managers as part of ensuring efficiency and excellence in their processes. The operational risk framework can look for such indicators, link them to risks through the risk and control self-assessment (RCSA) process, and then produce a dashboard of operational risk-relevant indicators for tracking.

SELECTING KRIs

The indicators selected by a firm to monitor its risk may be KPIs or KCIs or combinations of the two. There are many challenges in finding appropriate KRIs for the operational risk framework. Metrics that are valuable for the day-to-day running of a department might be inappropriate or insufficient for operational risk management.

Many operational risk functions are faced with a sea of metric data when they first request KRIs.

These metrics needed to be filtered and enhanced in order to find the most appropriate indicators. It is helpful to complete the RCSA program before seeking KRIs so that the search can be narrowed down to only those metrics that are relevant to the risks that have been identified in the RCSA.

The RCSA will assist the operational risk manager in identifying which are the high risks and which risks are currently low but are in danger of alleviating if the control environment deteriorates. She can then explore which controls are contributing to the risk rating and how those controls might be monitored by a KRI.

Having identified the areas of interest, she can set about developing a metric and hopefully one that is a KRI. She will often need to work with managers in other departments in order to establish ownership and find a reliable source for the data. She will also need to ensure that the quality of the metric is validated.

Once the risks that need to be monitored are identified, SMART principles can be applied in the selection or creation of an appropriate KRI. SMART principles suggest that a KRI should be:

Specific
Measurable
Attainable
Relevant
Timely

In practice, it is difficult to find indicators that meet all of these criteria, and it may be necessary to use proxy indicators temporarily, or even permanently.

Having established what data needs to be collected, the operational risk manager must then put in place thresholds and appropriate reporting scales and processes.

THRESHOLDS

The thresholds that are set for a metric are critical. Once thresholds are set, they are unlikely to be changed for some time and so they need to be set at the correct point.

Picking a threshold for a metric might produce an outcome that gives a high, medium, or low risk score. For example, if a firm's system has been shown to become unstable above one million trades, then a metric that tracks number of trades in a day might have three thresholds set as shown below.

Example of Thresholds for a Trade Volume Metric

Metric	Low Risk	Medium Risk	High Risk
Daily trade volume	< 500,000	500,001–1,000,000	> 1,000,000

This is a purely subjective and qualitative approach and can work well for many metrics as it is based on the management experience within the firm.

However, a more scientific approach can be helpful. If you have a data set for the metric that spans a good period of time, then you can apply statistical analysis to that data set and determine the properties of those data. By establishing the mean and the standard deviation it is possible to apply a consistent threshold approach to all metrics.

For example, the operational risk function might establish in the KRI standards that a standard deviation in a metric above 0.5 should result in a medium risk rating and a standard deviation above 1 should result in a high risk rating. This assumes that the metrics are set up appropriately so that increases or decreases are appropriately tracked where they may indicate increased risk.

KRI STANDARDS

Each KRI must be monitored, and the minimum standards for KRIs should be set by the operational risk department. Gathering KRIs can be a manually intensive task, and many firms have implemented technology systems to extract metrics automatically where possible and to house metrics for analysis.

For each KRI, certain criteria need to be set, including:

- Name of the indicator
- Risk that it is being monitored against

- Method of calculation
- Owner of the KRI
- Red flag threshold, or red, amber, green or high, medium, low thresholds
- Reporting period

KRI CHALLENGES

The biggest challenge with KRIs is finding the right one. There is no consensus on which KRIs should be collected, although some best practice is starting to emerge. It is also often practically challenging to collect data that might be very helpful in managing operational risk. Einstein put it best when he said: "Not everything that can be counted counts, and not everything that counts can be counted."[1]

Industry collaboration has led to some recommendations from the American Banking Association and from the Risk Management Association (RMA) on appropriate KRIs. However, these recommended KRIs number in the hundreds or even thousands, and every firm is seeking the magical minimum number of KRIs that can indicate the operational risk health of the firm.

Firms are participating in collaborative exercises with these and other organizations to compare metrics and seek out possible benchmarking opportunities.

Without industry benchmarking a firm's KRI can be compared only to itself. This can result in a false sense of security in an indicator that is remaining stable, but that may in fact indicate that the control being monitored is operating at below industry standard.

As mentioned earlier, it is good practice to link KRIs to risks and controls that have been identified in the RCSA process and are known to be key to operational risk management. A complete KRI program also requires constant validation and feedback and strong standards.

METRICS EXAMPLES

KRIs could be developed based on the following examples of indicators that can be helpful in an operational risk program.

People Metrics

Some common examples of people metrics are provided in Table 9.1.

TABLE 9.1 Sample People Metrics

Metric	Description	Possible Parameters
Staff turnover	A simple metric that tracks number of staff leaving and joining.	Number of leavers; number of joiners.
Regretted losses	Number of staff who have left the firm not due to downsizing or firing.	Percentage of workforce; percentage of total leavers.
Reason for leaving	Human resources generally tracks the reasons for leaving, and capturing that information may give an indication of morale and other people issues.	Categories could be: compensation, lack of training, lack of opportunities for advancement.
Educational levels	Highest level of education for each employee.	High school, bachelor's, MA, PhD.
Professional level	Professional exams taken and passed.	For example, Series 7, CPEs, CLEs, etc.
Training days	May indicate the level of expertise in the firm and may relate to morale and reasons for leaving.	Average number of days per employee; number of days per department/ business unit.
Staff morale	Firmwide surveys can provide information that can assist with measuring the morale in the firm.	Average morale score; high and low scores; departmental/business unit comparisons; year on year comparisons.
Compensation	Benchmarking compensation can help ensure salaries are competitive.	Comparison with industry benchmarks.

Compliance Metrics

Some common examples of compliance metrics are provided in Table 9.2.

TABLE 9.2 Sample Compliance Metrics

Metric	Description	Possible Parameters
Number of action letters from regulator	Regulators provide investigation notices that require a response by the firm.	Number of letters, number of letters resolved without issue, number of letters requiring remediating actions.
Regulatory fines	This is a subset of loss data that may provide insight into compliance health of the firm.	Number of fines, dollar value of fines, total dollars in fines this month/quarter/year.
Frequency of compliance reviews	Compliance desk reviews are mandatory in some areas.	Frequency or length of time since last review, by division, desk, etc.
Number of open compliance issues	Remediating actions are often required by compliance departments.	Number of actions open, number of actions late, number of high-priority actions open, etc.
Time taken to complete AML	Measures how promptly anti–money laundering checks are made.	Days/hours from request to completion.
Number of new products traded without new-product approval	Products that miss this process may expose the firm to elevated operational risk (as well as market and credit risk).	Number of new products approved by month; number of products identified that missed NPA process.

Technology and Infrastructure Metrics

Some common examples of technology and infrastructure metrics are provided in Table 9.3.

TABLE 9.3 Samples of Technology and Infrastructure Metrics

Metric	Description	Possible Parameters
Average time to resolve support requests	Time between initial request and response or final resolution.	Days/hours/minutes to respond; days/hours/minutes to resolve.
Number of support requests	Number of requests received by the help desk, or production support areas. May indicate issues with the systems. Should be compared to number of support staff and response times.	Number of requests total; number of requests per area; number of requests per time of day, week, month.
Network downtime	Measures resiliency of the network.	Days/hours/minutes down; by process/department/system, etc.
Hardware failure	Measures failed hardware.	Number of incidents; time to resolution or replacement.
Number of software patches	Measures quality of systems and workload of IT.	Number of patches by process/department/system.
Number of security breaches	Number of virus/hacker attacks may indicate stability of the systems and security confidence.	Number of total attacks; number of attacks caught at firewall; number of attacks penetrating security.
System capacity	Measures the redundancy in the systems to ensure they can handle peak requirements.	Percentage of average system capacity per month; percentage of peak system capacity per month.
Password exceptions	Measures how often password attempts are made to monitor security breach attempts.	Number of password breaches; number of authorize exceptions to password resets.
Telecoms failure	Measures failed telecommunications infrastructure.	Number of incidents; time to resolution or replacement.

Business Continuity Metrics

Some common examples of business continuity metrics are provided in Table 9.4.

TABLE 9.4 Sample Business Continuity Metrics

Metric	Description	Possible Parameters
Number of completed business continuity plans	Tracks how many plans are in place, but does not evaluate their quality. Quality may be scored by BCP team.	Number of plans; number of plans scoring as "high"; date since last plan update.
Date since last BCP test	Tracks the age of BCP testing to ensure it does not get stale.	Days/months since last test by process/system/ department/location.

Client Metrics

Some common examples of client metrics are provided in Table 9.5.

TABLE 9.5 Sample Client Metrics

Metric	Description	Possible Parameters
Number of client complaints	Customer satisfaction changes may provide insight into changes in employee practice, product issues, client profile changes.	Number of complaints; types of complaints; by department/region/ product.
Number of new accounts opened	The number of accounts opened may indicate resources constraints.	Number of accounts opened; number of accounts opened with missing data.
Number of client records complete	Measures how many clients have completed reference records. This measure can be used for EDPM, CPBP, and fraud risks.	Percentage of client records that are incomplete.

Trade Execution and Process Management Metrics

Some common examples of trade execution and process management metrics are provided in Table 9.6.

TABLE 9.6 Sample Execution and Process Management Metrics

Metric	Description	Possible Parameters
Volume of transactions	All transactional measures require further insight than mere volumes. They can be considered in relation to each other, e.g., number of fails as percentage of total volume.	Total number of transactions; number per desk/product/department; compared to last day/week/month.
Number of fails		Total number of fails number per desk/product/department; compared to last day/week/month; compared to total volume.
Number of cancel and corrects		Total number of cancel; percentage of corrects; number per desk/product/department; compared to last day/week/month; compared to total volume.
Number of manual wire transfers	An increase in manual wire transfers might increase errors.	Total number or comparison with last week/month; number of erroneous wire transfers per total number of manual transfers.
Downtime of external feeds	Loss of external feeds may affect performance and increase errors.	Days/hours/min downtime of each external fee.

Financial Statement Metrics

Some common examples of financial statement metrics are provided in Table 9.7.

TABLE 9.7 Sample Financial Statement Metrics

Basic Indicator	Description	Possible Parameters
Percentage of SOX controls tested	SOX controls provide evidence that the financials are correct.	Total number tested; percentage tested; percentage tested and failed.
Number of errors in financial statements	The number of erroneous entries and fixes.	Number of entries; percentage of entries requiring fixes; number of fixes; number of unreconciled entries.
Percentage of SOX controls tested	SOX controls provide evidence that the financials are correct.	Total number tested; percentage tested; percentage tested and failed.

KEY POINTS

- KRIs are used to monitor changing risk levels and true KRIs are difficult to identify.
- Metrics may provide the business environment and internal control factors that are required for an advanced measurement approach capital model under Basel II.
- There are many types of metrics including exception monitoring, performance indicators and control indicators.
- A metric might be a lagging, leading, or exception metric.
- SMART principles suggest that a KRI should be specific, measurable, attainable, relevant, and timely.
- It is important to ensure that thresholds are carefully set and monitored.

REVIEW QUESTION

1. An indicator which measures the average time taken to resolve a help desk request would best be described as a:
   a. Key risk indicator
   b. Key performance indicator
   c. Key control indicator
   d. Simple metric

NOTE

1. Quote has been attributed to Albert Einstein (1879–1955), but has also been attributed to William Bruce Cameron's 1963 text, *Informal Sociology: A Casual Introduction to Sociological Thinking*.

CHAPTER 10

Risk and Control Self-Assessments

This chapter explores the role of risk and control self-assessment in the operational risk framework. Various RCSA methods are described and compared and several scoring methodologies are discussed. RCSA challenges and best practices are explained, and the practical considerations that can help ensure the success of an RCSA program are outlined.

THE ROLE OF ASSESSMENTS

Risk and control self-assessments (RCSAs) play a vital role in the operational risk framework.

While operational risk event databases are effective in responding to past events, additional elements are needed in order to identify, assess, monitor, control, and mitigate events that have not yet occurred. A well-designed RCSA program provides insight into risks that exist in the firm, regardless of whether they have occurred before. The RCSA program fits into the operational risk framework as illustrated in Figure 10.1. While loss data allows us to look back at what has already happened, RCSA gives a tool to look forward at what might happen in the future. RCSA results often provide the best leading indicators of where risk needs to be mitigated.

Even if these risks are well understood by their owners, there is rarely a tool outside the operational risk framework that provides consistency and transparency in reporting, mitigating, and escalating these risks. For this reason, risk and control assessments are often the most enthusiastically adopted elements of the program, as they can quickly add value by providing a way for a department to articulate its risks.

However, they are also often the most troublesome elements, as finding the right way to manage the assessments that fits the culture of the firm,

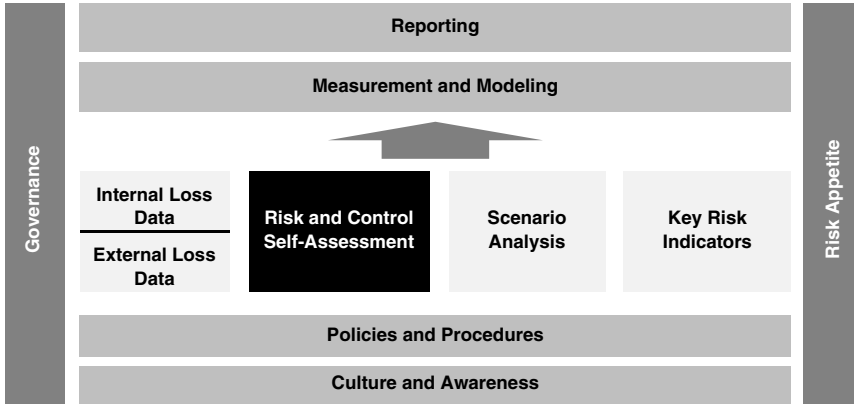

FIGURE 10.1 Risk and Control Self-Assessment in the Operational Risk Framework

meets regulatory requirements, and meets the goals of identifying, assessing, and controlling operational risk can be very difficult.

Many firms have experienced putting tremendous effort into rolling out RCSA programs only to find they are not meeting their needs and have to be redesigned and rolled out again. In fact, many firms have been through RCSA redesigns a few times already and may now be looking yet again at how to get this right.

The challenge is that the effort needed to populate the RCSA with valuable and accurate information can sometimes exceed the business benefit garnered from that information. The business benefit is being able to see your risks with transparency and make informed decisions about them.

The business benefits of an RCSA program are clear, but there may also be regulatory requirements that can be met through RCSAs. For example, Basel II firms that are taking an advanced approach to capital calculation have to show that they are including business environment and internal control factors in their calculation. These factors should reflect an understanding of the underlying business risk factors that are relevant to the firm, and the effectiveness of the internal control environment in managing and mitigating those risks. Key risk indicators (KRIs) can be used to track those indicators, as discussed in Chapter 9. However, RCSA is best suited to identify which indicators are relevant and worthy of monitoring.

In the section on BEICF, Basel II provides a good definition of RCSAs that can be applied to assessments undertaken in any operational risk framework:

> *. . . a bank's firm-wide risk assessment methodology must capture key business environment and internal control factors that can*

> *change its operational risk profile. These factors will make a bank's risk assessments more forward-looking, more directly reflect the quality of the bank's control and operating environments, help align capital assessments with risk management objectives, and recognize both improvements and deterioration in operational risk profiles in a more immediate fashion.*[1]

RCSAs are used by Basel II advanced measurement approach (AMA) firms to gather these factors, and there is further discussion in Chapter 12 on how these are then incorporated into the capital calculation. The same methodologies are applicable to all firms as regardless of regulatory requirements, the firm needs tools to allow them to meet the operational risk management goal of "recognizing both improvements and deterioration in operational risk profiles" to inform its decision making.

Risk and control self-assessment is a term that can refer to many different types of assessment. It should be clearly differentiated from control assessments, and from risk and control assessments, neither of which have the "self" assessment characteristic.

Control Assessments

A simple control assessment is one that tests a control's effectiveness against set criteria and issues a pass/fail or level of effectiveness score. A control assessment is often done *to* the department by a third party, perhaps audit, compliance or the Sarbanes-Oxley team.

Control assessment can produce output that is very useful to the RCSA program. For example, it may provide effectiveness scores for controls that can be leveraged in the RCSA program. Indeed, where a control has been assessed in a Control Assessment it is preferable to avoid reassessing that control. However, while this seems sensible, in practical terms it can prove difficult to leverage scores from other assessment programs unless the firm has adopted a standard taxonomy for controls, processes and organizational structure. Without such taxonomies it can be difficult to map results from one assessment to another.

Risk and Control Assessments

A risk and control assessment is similar to a control assessment, in that it is applied to an area by a third party. However, these do include a risk assessment in addition to a control assessment and so will incorporate several of the elements of the RCSA that will be further described below. As with control assessment, the results of these might be leveraged for the RCSA.

RCSAs

A risk and control *self*-assessment (RCSA) is distinguished from a control assessment and from a risk and control assessment by its subjective nature. While often facilitated by an operational risk manager, an RCSA is conducted by the department or business unit and the scoring of risks and controls reflects not the view of a third party, but the view of the department or business itself.

It is the subjective perspective of the RCSA that presents both its biggest advantages and its strongest challenges.

The advantage of such an approach is that it further embeds the culture of operational risk management. Each department takes ownership of its own risks and controls and assesses the risks that may exist in its area. Empowered with this assessment the department can then prioritize mitigating actions and escalate risks that require higher authority for remediation.

The challenge of such an approach is that a subjective view can be considered as less accurate than an objective view, and there may be some skepticism over the scoring in the assessment. In practice, a well-designed RCSA program can produce accurate and transparent operational risk reporting that can be used effectively in the firm. It is important to never lose sight of the subjective nature of this element however, and to be diligent in applying standards and strong facilitation throughout.

RCSAs should be included in the audit cycle, with each department audited as to its participation in the RCSA program and the reasonableness of their scoring. For example, loss data should be compared to RCSA scores as a check. If losses are high in an area that has been scored as low risk in the RCSA, that would raise a serious question as to the quality of the self-assessment and might result in an audit point. This has been raised by the regulators in recent years under their validation and verification requirements that were discussed in Chapter 4. There are now regulatory requirements that demand that RCSA and loss data be routinely compared to ensure the RCSAs are reflecting the loss experience of the firm.

RCSA METHODS

There are several RCSA methods, and each has its own advantages and disadvantages. The main methods to consider are the questionnaire approach, the workshop approach and the hybrid approach.

Questionnaire Approach

The questionnaire based approach uses a template to present standard risk and control questions to participants. The content of the questionnaire is

designed by the operational risk team, usually after intensive discussions across the firm. Each risk category or business process is analyzed and a list of related risks is prepared. For each risk, expected controls are identified.

The questionnaire is usually distributed to a nominated party in each department, who completes the questionnaire, providing self-assessed scores for each expected control, and risk levels (for example, high, medium, or low) and probabilities for each risk.

The level of complexity of questionnaire based RCSAs content and workflow varies enormously. Some questionnaire RCSAs ask participants to score just the controls (and in this case might be better named a control self-assessment or CSA). Others have several rounds of completion, the first being risk and control identification, the second being control effectiveness scoring by the control owners, and the last being residual risk scoring by the risk owners.

There are several advantages of a questionnaire-based RCSA method. The use of standard risks and controls makes it easier to consolidate reporting and identify cross firm themes and trends. Also, the use of standard risks and controls ensures that a consistent approach is being taken across the firm and ensures that risks and controls that have been identified by the operational risk department are considered by every department.

These characteristics make a questionnaire-based RCSA particularly well suited to a firm that has multiple similar activities. For example, a bank that has many branches that offer the same products and services would be well served by a questionnaire-based RCSA. The results can be collected electronically and the responses compared to identify themes, trends, and areas of potential control weakness or elevated risk.

Another advantage is that this method can take advantage of technology to distribute and collect questionnaires. In the past five years, many software providers have entered this space with tools that provide good workflow functionality. Where firms have found the off-the-shelf solutions do not meet their needs, they have developed their own RCSA workflow tools, with varying degrees of success.

There are also disadvantages to the questionnaire-based RCSA. If a firm does not have standard branches or repeated processes, then a standard RCSA might be more frustrating than it is helpful.

Another disadvantage of the questionnaire-based approach is that it is usually sent to specific nominated parties for completion. For this reason, careful facilitation is required to ensure that a departmental view is being expressed in the assessment and not just one person's opinion.

An additional potential weakness in the questionnaire-based approach is that the original design might be missing a key risk or control, and participants might not have an opportunity to, or may be reluctant to, raise new items.

In fact, a general challenge in any questionnaire-based task is that it can result in a "check all" mentality, where the participants simply check the boxes that are likely to result in the least follow up work, or that express an average score or the middle ground.

A questionnaire-based method is efficient and is highly effective in the right environment, but the supporting training and facilitation should not be underestimated in order to ensure any disadvantages have been effectively overcome.

Workshop Approach

A workshop method RCSA is discussed in a group setting, with facilitation from the operational risk department. Each risk is discussed, and related controls are scored for effectiveness. Once the controls have been scored, the residual risk is scored, often on a high-medium-low scale, along with related probabilities. Alternatively, the exposure might be expressed in financial terms. Some workshops also collect other impact data, such as possible client impact, legal or regulatory impact, reputational impact, and life safety impact.

Workshops often run for two to three hours, and perhaps more than one session is needed for each RCSA. As such, they are time consuming for all involved and require a strong commitment from both the participants and the facilitators.

Preparation for the workshop is usually extensive, involving the review of past losses, audit, compliance, and Sarbanes-Oxley reports and interviews with business managers and support areas. There are several advantages to a workshop-based RCSA. Perhaps mostly important, it provides a forum for an in-depth discussion of the operational risks in the firm. For this reason, it can be effective in embedding operational risk management.

The group approach to scoring ensures that there has been full participation in the scoring, rather than a single view. However, reaching a true consensus can be challenging and requires strong facilitation skills.

The workshop session often results in new risks and controls being identified and so contributes to the richness of the operational risk framework.

Workshop-based approaches are generally more appropriate for firms that do not have consistent branches or processes, and that need more flexibility than can be offered in a questionnaire-based approach. For example, a financial services firm that does not have retail branches, but has fixed income, equity, and asset management divisions, might be better suited to a workshop-based approach so that the unique risks and controls in each area can be appropriately assessed.

However, as with the questionnaire approach, there are several disadvantages to the workshop approach. The flexibility can also result in inconsistency as risks and controls might be newly raised in several areas, perhaps with different terminology. Also, consolidating the results can be challenging as each workshop output might look very different to the others.

Another disadvantage is that the roll out of a workshop-based approach is extremely burdensome on the operational risk department, and on the firm. Many people will be involved in the sessions and the preparation and facilitation can use up a large proportion of an operational risk department's resources.

Hybrid RCSA Methods

As the operational risk framework matures and evolves, RCSA design will also mature and evolve. In the meantime, some firms use both the questionnaire and workshop approaches in order to get the most out of their RCSA program. For example, a firm that used the workshop approach in its first year might then use the output from that workshop to design a questionnaire approach for the subsequent years.

Alternatively, a firm might alternate questionnaire and workshop approaches in order to ensure that new risks and controls are identified and that a full discussion of operational risk is undertaken on a regular basis.

A firm might implement a sophisticated RCSA technology system that supports a flexible and collaborative approach and so decide not to hold workshop RCSAs anymore.

A firm might adopt a questionnaire approach but set certain triggers that will result in a workshop being held for a particular risk category. For example, a trigger might arise if losses escalate in a particular risk category or process, or if a major external event occurs that suggests that a reassessment of that risk would be prudent.

Few firms disclose their assessment methodology in their annual reports, but JPMorgan Chase does describe its assessment approach as a control assessment in its annual report as follows:

> ***Control assessment***
> *In order to evaluate the effectiveness of the control environment in mitigating operational risk, the businesses utilize the Firm's standard self-assessment process and supporting architecture. The goal of the self-assessment process is for each business to identify the key operational risks specific to its environment and assess the*

degree to which it maintains appropriate controls. Action plans are developed for control issues that are identified, and businesses are held accountable for tracking and resolving these issues on a timely basis.[2]

RCSA SCORING METHODS

There are many different ways to produce scores from RCSAs. Most RCSA require some score of the likely impact and probability of an event occurring. Some also require control effectiveness scores that might be entered directly or calculated from control design and performance scores. Some RCSAs might require scores for nonfinancial impacts such as reputational damages, client loss, legal or regulatory exposures, or even life safety impacts.

Scoring Control Effectiveness

A firm that has a Sarbanes-Oxley program in place might well have a control effectiveness scoring methodology in place. This might be leveraged for control scoring requirements in an RCSA. If there is no control scoring method in place, then one can be developed that assesses both the design and the performance of the control. One example of such a scoring method could be as shown in Table 10.1.

TABLE 10.1 Scoring Control Design and Performance

	Low	Medium	High
Design	The design provides only limited protection when used correctly.	The design provides some protection when used correctly.	The design provides excellent protection when used correctly.
Performance	The control is rarely performed.	The control is sometimes performed.	The control is always performed.

The design and performance scores for each control might then be combined to produce an overall effectiveness score as in Figure 10.2.

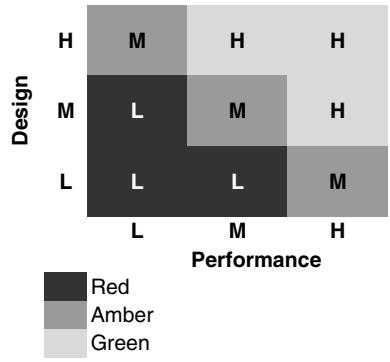

FIGURE 10.2 Control Effectiveness Scoring Matrix

In this example scale, a control that is well designed (H) but poorly performing (L) would have an overall control effectiveness score of low. Often, a red-amber-green or RAG rating will be used in assessments. In this example, controls that had an overall effectiveness that was low would produce a red result. The use of RAG ratings to visually highlight areas of concern can be very effective, but can also produce a strong reaction and so need to be used with caution.

An alternative control scoring method would be to have a list of control attributes for control design and have the overall design calculated or subjectively summarized based on those criteria. For example, a preventative control might be considered to be a stronger safeguard than a detective control and might help raise the score of that control. Similarly, an automated control would be considered stronger than a manual control.

It may also be possible to score control performance using key performance or key control indicators. As the RCSA matures, more and more key performance indicators (KPIs) and key control indicators (KCIs) will be identified, and these can be incorporated into the RCSA to provide more objective scoring for the controls where possible.

Each firm will determine its own appropriate control scoring method. Controls might be scored individually or as a group for each risk.

Risk Impact Scores

Some RCSAs simply require a financial impact score, for example, the maximum loss, the maximum plausible loss, or the likely loss amount.

Other RCSAs also require a score for other impact types, on a scale that is provided. For example, a sample scale that provides high, medium, and low scores for several impact types is provided in Table 10.2.

The impact is usually scored on a residual scale that is the likely impact after all the controls are in place, or after the control effectiveness scores have been determined. Some RCSAs also score the inherent impact; that is the likely impact before controls are considered and this inherent impact score is sometimes used to prioritize the assessment of risks that have a high inherent impact. The inherent impact can be helpful in understanding the relative value of controls. However, some firms do not collect inherent values and focus only on risks that have a high residual impact.

TABLE 10.2 A Risk Impact Scoring Scale That Includes Nonfinancial Impact Categories

Impact Type	Low	Medium	High
Financial	Less than $100k.	Between $100k and $1m.	Over $1m.
Reputational	Negative reputational impact is local.	Negative reputational impact is regional.	Negative reputational impact is global.
Legal or Regulatory	Breach of contractual or regulatory obligations, with no costs.	Breach of contractual or regulatory obligations with some costs or censure.	Breach of contractual or regulatory obligations leading to major litigation, fines, or severe censure.
Clients	Minor service failure to noncritical clients.	Minor service failure to critical client(s) or moderate service failure to noncritical clients.	Moderate service failure to critical clients or major service failure to noncritical clients.
Life Safety	An employee is slightly injured or ill.	More than one employee is injured or ill.	Serious injury or loss of life.

TABLE 10.3 Sample Scoring Method for Frequency or Probability

	Low	Medium	High
Length of time between events	> 5 years	Between 1 and 5 years	< 1 year

Probability or Frequency

An RCSA might require a probability score in terms of the likelihood that the risk event could happen in the next 12 months. For example, if the event is likely to happen 5 times in the next 12 months, the probability would be 5. If it is likely to happen only once in the next 10 years, then the probability would be 0.1.

Alternatively, the probability or frequency might simply be scored as high, medium, or low as shown in Table 10.3.

Risk Severity

Once the impact and frequency have been scored, some RCSAs combine these to give an overall risk severity score. This might be calculated using a combination of the scores as in Figure 10.3.

Using this methodology, a score of low (L) for impact and high (H) for frequency, would give an overall risk severity of medium (M). Once again, a RAG rating that indicates high scores as red, medium scores as amber, and low scores as green can be a powerful tool and should be used with caution.

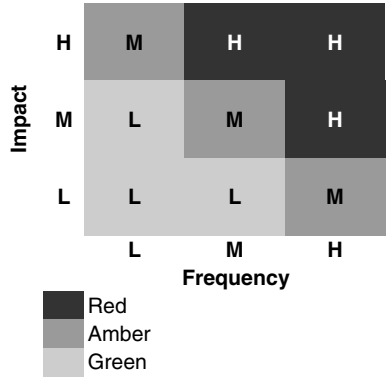

FIGURE 10.3 Risk Severity Scoring Matrix

Scoring scales need to be adapted to meet the risk appetites of the firm. One scoring method might be effective in one firm, but inappropriate in another. For this reason, scoring methods vary greatly from firm to firm.

RCSA BEST PRACTICES

There are several key elements to a successful RCSA program, regardless of approach taken. When designing and implementing an RCSA, it is prudent to consider the following elements.

Interview Participants Beforehand

To ensure that the RCSA is well designed and reflects the business processes and associated risks and controls in each department, it is important to spend time interviewing participants, stakeholders, and support functions prior to launching the RCSA.

Review Available Background Data from Other Functions

There will be valuable information available for preparation purposes in recent audit reports, compliance reviews and Sarbanes-Oxley assessments. A review of these documents can provide insight into existing and recently remediated operational risks.

Review Past RCSAs and Related RCSAs

Once the RCSA program has been running for more than a year, past RCSAs should be reviewed when a department is conducting its next RCSA. There should also be a review of related RCSAs from departments that either provide support services to the department or rely on support from the department. These related RCSAs may have raised risks where the controls are owned by this department, and may have raised risks that the department needs to be aware of.

Review Internal Loss Data

Events that have been captured in the firm's operational risk event database provide a valuable backdrop, and help to identify the risks and control weaknesses that need to be addressed in the RCSA. They also demonstrate the possible impact and frequency of risk events and so can be used to validate assessments made during the RCSA.

Review of External Events

External events are also helpful in informing the discussions around potential risks. The RCSA is designed to consider all possible risks, not just those that have already occurred in the firm, but this can be a difficult task and examples of events in the industry are useful for this purpose.

Carefully Select and Train Participants

The RCSA participant(s) should be selected with care and trained in the RCSA method beforehand. It is helpful to include representatives from areas that support the department that is completing its RCSA, as they will have a (sometimes surprising) view on the effectiveness of the controls that they own. Ensure that control owners participate in scoring their own controls.

It can be helpful to have the head of the department included if it is a workshop-style RCSA, but only if their presence will not intimidate the other participants and so skew the results to just one view.

Document Results

The RCSA output should be consistently and carefully documented with an emphasis on providing evidential support for conclusions and scores whenever possible. Every detail of the discussions need not, and indeed probably should not, be recorded. However, the output must be captured in a way that can be reviewed, analyzed, and acted upon. This might mean that the results are put into a system or simply recorded in a spreadsheet or document, depending on the RCSA method used.

Regulatory expectations regarding the documentation of RCSA results have risen over the past few years and a subjective score is often not considered to be sufficient by the regulator. For this reason, many firms have been looking to adopt more object control scoring methods and have been applying taxonomies for processes, risks, and controls. This is discussed further in this chapter under "Ensure Completeness Using Taxonomies."

Score Appropriately

The RCSA scoring methodology should be appropriate for the firm and each firm should consider whether it might be beneficial to its operational risk management goals to include nonfinancial impacts such as reputational, legal, regulatory, client, and life safety where appropriate.

Identify Mitigating Actions

An RCSA is incomplete without the identification of any actions that have been agreed upon during the assessment. These actions will be undertaken to lower any unacceptable risk levels, either by improving, changing, or adding a control. Generally, a high risk will need to be mitigated, unless the risk is accepted without mitigation. If the risk is accepted, then this should be clearly stated in the assessment. Action items need to be tracked in the operational risk framework, through to their completion.

Implement Appropriate Technology

RCSA technology should be used appropriately to manage the process and to report on the outcome. An RCSA tool should support the methodology and provide access to reporting and analysis of the assessments.

Ensure Completeness Using Taxonomies

RCSAs should cover the entire firm and be complete and comprehensive, indeed national regulatory standards often require this. In recent years, firms have taken this to heart and have been using several methods to demonstrate this.

First, it is important to show that all material areas of the firm have been covered. This can be done by using the organizational hierarchy and checking that all aspects of the hierarchy have participated in an RCSA.

Second, firms are now moving towards developing standard process taxonomies. These process taxonomies can be used by every area in the firm to identify processes that they undertake and to ensure all of those processes are included in their RCSA program.

Third, firms are also moving to developing risk taxonomies. These taxonomies are often built out of the Basel II seven operational risk categories of Internal Fraud; External Fraud; Employment Practices and Workplace Safety; Clients, Products, and Business Practices; Damage to Physical Assets; Business Disruption and System Failures; and Execution, Delivery, and Process Management. It has proven helpful for many firms to develop their own risk taxonomy down to a level three categorization.

Fourth, firms have moved toward developing control or control-type taxonomies.

Finally, all of these elements can be brought together to ensure completeness in the following way. The corporate operational risk function can work with the businesses and support functions to determine which of the risks in the risk taxonomy could arise in each process. They can also determine which of the control types in the control taxonomy could mitigate the risks in the risk taxonomy.

Armed with this information, an RCSA can be designed that captures all the departments, all the processes in each department, all the risks associated with those processes, and all of the expected control types that can mitigate those risks.

This is, not surprisingly, a huge undertaking. Developing the taxonomies alone can require heroic efforts and collaboration across the firms. Even once the taxonomies have been agreed, the size of RCSA that might result could be burdensome and this will mean that a triaging or prioritization procedure will likely be needed. This procedure will need to be well documented and defensible if it is not going to undermine the goal of demonstrating completeness.

Finally, the maintenance of such taxonomies is a large and constant undertaking and needs to be owned by a function that has the capacity and authority to maintain it.

If such taxonomies and their mapping relationships are adopted across the firm by audit, compliance, technology risk, and other assessment functions, then the benefits may well outweigh the burden as they will all then be able to leverage each other's work.

Themes Identified

The whole RCSA program should be reviewed for the identification of firm wide themes that may require escalation. One of the important roles of the operational risk function is to take a step back from the details of the individual RCSAs and deduce where there are firm-wide themes that might need to be addressed. Several local solutions might be less effective than a firm-wide strategy to mitigate a particular risk.

For example, if several areas identified that they had difficulty training their staff in a timely way, and that this was impacting several risk scores, then the appropriate solution might be for the firm to improve its corporate training and development programs, rather than addressing the training differently in each location.

Leverage Existing Assessments

Risks and controls may have been assessed as part of other programs in the firm, such as business continuity planning, or Sarbanes-Oxley. If so, these assessments should be used in the operational risk RCSA, and every effort should be made to avoid repeating an assessment of a risk or of a control. This is important in order to protect the integrity of both the original assessment and the operational risk RCSA. Conflicting scores can cause serious problems, and it is frustrating for all involved if the work is merely

repetitive. This will be discussed in more depth later Chapter 16, under "Governance, Risk, and Compliance."

Schedule Appropriately

Many firms conduct RCSAs on an annual basis. However, each firm should select an appropriate scheduling interval and this might be monthly, quarterly, annually, or ad hoc in response to a certain trigger event.

The schedule should ensure that the information is not stale, and that the burden of collecting the assessment does not outweigh the benefit in responding to the assessments with timely mitigation. Reporting on the remediation efforts generated by RCSA activity should occur more frequently, probably monthly, in order to ensure risks are being mitigated as expected.

Risk and control self-assessments have a unique and powerful role to play in an effective operational risk program. The risk and control scores that are gathered during the RCSA are vital to meeting the goals of identifying, assessing, monitoring, controlling, and mitigating operational risk. RCSAs ensure that there is proactive risk management across the firm, to supplement the reactive risk management that occurs in response to loss events. The challenges with RCSAs are keeping them current, designing them to be relevant and valuable to participants and to senior management, and ensuring that they produce tracked actions.

It is worth spending time planning and piloting RCSA methods before use, and it is important to allow these methods to evolve as experience develops and as the operational risk management function matures.

Backtest or Validate Results

Regulatory expectations now require the validation of RCSA results. The simplest validation method is to compare loss data results with RCSA scores. If loss data suggest that an area produces significant losses in a particular risk category, but the RCSA is indicating low risk severity in that same area, then this should raise concerns. Such contradictions should lead to a review of the RCSA and the justification for the scoring in the RCSA. Backtesting and validation can (and should) be independently undertaken by the second line of defense: the corporate level operational risk function.

KEY POINTS

- RCSAs provide an opportunity to look forward and consider what could occur in the future, whereas loss data focus on what has already occurred in the past.

- RCSAs come in many different forms and an appropriate method needs to be developed at each firm to meet its particular regulatory and business needs.
- RCSAs can be used to collect scores for the effectiveness of controls, the potential size and probability of a risk event's occurring, and the overall risk severity associated with a potential event.
- Workshop method RCSAs focus on group scoring and discussion while questionnaire method RCSAs often use standard templates and automated delivery methods.
- The qualitative nature of many RCSA methods raises challenges in interpreting and applying the results to ensure that appropriate risk management and mitigation activities can be implemented.
- Best practices for RCSA have matured in the past few years and can be leveraged to ensure a successful program is implemented.

REVIEW QUESTION

1. Which of the following best describes how risk and control self-assessments (RCSA) can be used to manage fraud risk for Basel II?
   a. An RCSA can be used to gather business environment and internal control factors that relate to fraud risks.
   b. An RCSA should be used to collect fraud related loss events.
   c. RCSAs are designed primarily to provide estimates of capital for fraud risk exposures.
   d. RCSAs are generally not designed to consider fraud risk.
   e. RCSAs only consider internal fraud risks and not external fraud risks.

NOTES

1. Bank for International Settlements, "International Convergence of Capital Measurement and Capital Standards: A Revised Framework," 2004, section 676.
2. JPMorgan Chase & Co., Annual Report, 2011, p. 166.

CHAPTER 11

Scenario Analysis

Scenario analysis is a challenging element in the operational risk framework. Scenario analysis provides the operational risk framework with a tool to explore the rare but plausible losses that could arise as a result of operational risk. The various methods used for scenario analysis are discussed and the important elements of a robust scenario analysis program are explained.

ROLE OF SCENARIO ANALYSIS

Scenario analysis has become an important element in operational risk management and measurement, and the methods used have evolved rapidly over the past few years. Firms use scenario analysis to evaluate their exposure to high-severity events. Unlike RCSA analysis, scenario analysis focuses on the "fat tail" events, or rare catastrophic events. These types of events can put the firm at serious risk. For this reason, scenario analysis is a required element in calculating operational risk capital requirements under Basel II for any firm undertaking the advanced measurement approach (AMA).

Firms that do not have AMA requirements are also pursing scenario analysis programs as they provide a valuable insight into the major risks faced and also provide the opportunity for an engaging dialogue with the business lines.

The role of scenario analysis in the operational risk framework is illustrated in Figure 11.1.

Scenario analysis is used to derive reasoned assessments of plausible severe losses. The assessments are then used to explore "what-if" cases that may be beyond the current experience of the firm. External data plays a key role in scenario analysis, as it provides insight into what has already occurred in other firms. However, in addition to learning from experiences

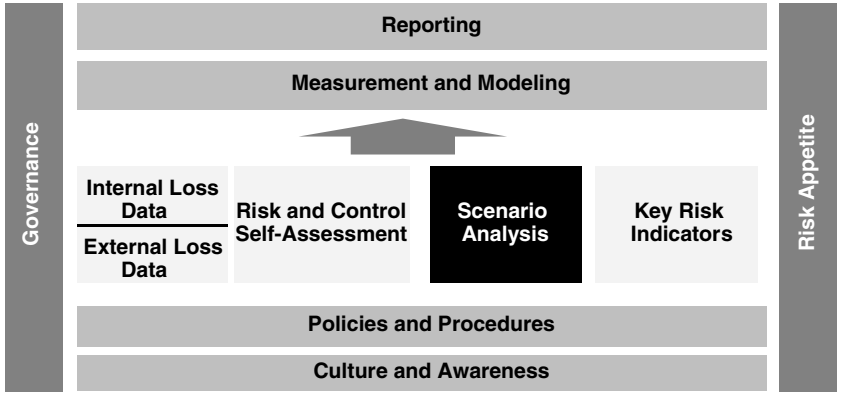

FIGURE 11.1 Scenario Analysis in the Operational Risk Framework

outside the firm, scenario analysis considers events that might not yet have occurred at any firm.

A somewhat helpful definition of scenario analysis and its uses can be found in Basel II. However, highlighted below are the areas of ambiguity that have proven challenging to the industry.

> *A bank must use scenario analysis of expert opinion in conjunction with external data to evaluate its exposure to high-severity events. This approach draws on the knowledge of* ***experienced*** *business managers and risk management experts to derive* ***reasoned*** *assessments of* ***plausible*** *severe losses. For instance, these expert assessments could be expressed as parameters of an assumed statistical loss distribution. In addition, scenario analysis should be used to assess the impact of deviations from the correlation assumptions embedded in the bank's operational risk measurement framework, in particular, to evaluate potential losses arising from multiple simultaneous operational risk loss events. Over time, such assessments need to be validated and re-assessed through comparison to actual loss experience to ensure their reasonableness (emphasis added).*[1]

Finding a process that taps experienced business managers and risk managers, and that produces reasoned assessments of plausible losses is challenging indeed. Who is "experienced"? What constitutes a "reasoned" assessment? What do we mean by "plausible"?

SCENARIO ANALYSIS APPROACHES

There are several different methods that can be used to conduct scenario analysis. Some firms use a workshop approach; some conduct interviews or analyze data in small teams. Some firms conduct many scenario analysis workshops, covering each risk category in each business; some run only a few scenarios at the corporate level. Some firms have standard scenarios for every business line to consider; some prefer that each business line develop their own.

Whatever the approach is, the purpose of the scenario analysis program is to identify those rare but plausible large events that should be incorporated into the operational risk framework. In practice, this means that people will be asked extremely difficult questions such as "How big could such an event be?" or "Could it happen in the next 20 years?"

If the output of scenario analysis is to be used directly in the capital calculation, then it will need to be a particularly robust, repeatable, and well-documented activity. Operational risk capital under an AMA framework is supposed to capture the risk at a 99.9 percent confidence level. In other words, it should be sufficient to cope with a 1/1,000-year event.

Conversations with business managers on whether something could happen in 1,000 years has proved unfruitful, and so most firms have developed ways to get close to the very rare, by considering the rare. For example, a 1-in-10-year event might be easier to discuss, and several data points might be collected to allow for the data collected to be extrapolated out to the rarer event.

The Basel Committee recognized the challenges banks were facing with this element of the framework and provided some further guidance in their 2011 AMA Guidelines as follows:

> *Scenario data provides a forward-looking view of potential operational risk exposures. A robust governance framework surrounding the scenario process is essential to ensure the integrity and consistency of the estimates produced. Supervisors will generally observe the following elements in an established scenario framework:*
>
> *(a) A clearly defined and repeatable process;*
> *(b) Good quality background preparation of the participants in the scenario generation process;*
> *(c) Qualified and experienced facilitators with consistency in the facilitation process;*

(d) The appropriate representatives of the business, subject matter experts and the corporate operational risk management function as participants involved in the process;
(e) A structured process for the selection of data used in developing scenario estimates;
(f) High quality documentation which provides clear reasoning and evidence supporting the scenario output;
(g) A robust independent challenge process and oversight by the corporate operational risk management function to ensure the appropriateness of scenario estimates;
(h) A process that is responsive to changes in both the internal and external environment; and
(i) Mechanisms for mitigating biases inherent in scenario processes. Such biases include anchoring, availability and motivational biases.[2]

We will consider each of these aspects as we explore the variety of methods being used today to meet the challenges of scenario analysis.

(a) A Clearly Defined and Repeatable Process

Scenario analysis contents might vary considerably from one set to another, but the process needs to be consistent. To achieve this it is necessary to develop written procedures and standards that will be applied every time a scenario analysis activity is run.

Experience has shown many firms that their auditors and regulators will pore over these documents and will carefully compare them to the process that actually occurred. It is therefore important to ensure that the defined process is not aspirational, but is achievable over and over again.

A robust scenario analysis process does not need to be, and should not be, overly complex. Rather, it should meet the criteria outlined above, while also providing the maximum benefit and least disruption to the businesses that are involved.

For this reason, much of the scenario analysis process is likely to reside in the corporate operational risk function, in the form of preparation, facilitation, and postscenario documentation and validation.

(b) Background Preparation

Section b of the AMA Guidelines calls for "good quality background preparation of the participants in the scenario generation process."[3]

Interviews Preparation for scenario analysis is very similar to preparation for RCSA workshops and questionnaires. The facilitator or preparation team interviews the key business managers and support managers for the area under consideration. Background documentation from audits, compliance reviews, and Sarbanes-Oxley assessments is reviewed. Internal and external loss events are analyzed.

Internal Loss Data The internal loss data of a firm certainly provides a floor for losses, but it does not show what *could* go wrong, it only shows what *has* gone wrong. The facilitators of a scenario analysis discussion should be aware of the history of losses, but it should not be shared directly with those participating in the discussion as this introduces a hard to overcome anchoring bias, as discussed later.

External Loss Data One of the most important inputs into the scenario analysis process is external loss data.

For example, if a scenario analysis workshop is being conducted on the risk category Internal Fraud, then the firm might have some internal data, but often very little. However, internal fraud as a category includes unauthorized trading, and the industry has several egregious examples of unauthorized trading that have resulted in losses in the many billions of dollars. Information on these external events can be helpful in developing a what-if scenario for the firm.

In scenario analysis, the questions should not be focused so much on why that event *could not* happen at this firm (as most businesses will contend), but rather on how *could* such an event happen at this firm. How many controls would have to fail at once? What sort of positions would the trader have to be able to hold? And so on.

External events provide an excellent opportunity to stimulate discussion on the rare, but plausible risks in this category.

In addition to the story lines from the news, external data from a consortium such as ORX can provide a helpful benchmarking floor. For example, if your firm is a member of ORX and the ORX data show that in the industry firms of your size have experienced losses over $50 million on average once every five years in this risk category, then is there any reason why your firm is different?

RCSA Results Another valuable source of background information is the RCSA program. RCSAs will have identified the high risks in each area and can be used to help populate a straw man of possible scenarios for consideration. However, something that is low risk in the RCSA might still qualify as a scenario as it may be that frequency was the main driver that

was keeping the risk low. If something could generate a very large loss, regardless of frequency, then that is an item for consideration in scenario analysis. Therefore, RCSA results need to be carefully reviewed as part of the background preparation.

Scenario analysis should also feed back into the RCSA program, further enriching the risks library that is constantly evolving in the operational risk framework.

Compliance and Audit Findings Compliance and audit findings can be helpful in challenging claims that a control or a set of controls is working well. These should be carefully reviewed as part of the background preparation and should be on hand for the facilitator to refer to as needed.

Key Metrics and Analysis Some risk categories may lend themselves to preparatory statistical analysis. For example, when discussing scenarios regarding the risk category Damage to Physical Assets, a scenario might be raised concerning a terrorist attack destroying a building. There are sources of data available on the frequency of attacks globally and in the main business cities and the range in impact zone of a single attack. This data can be used alongside the firm's own data on its office locations to develop a model to assist with the estimation of severity and frequency.

The use of such metrics is referred to as factor analysis by some firms and is gaining momentum across the industry. This type of analysis alleviates the difficulties in estimation and seems to be well received by regulators so far. However, according to the AMA guidelines above, the role of the business expert must still exist and so even this type of analysis requires subjective confirmation from the business and risk managers.

Straw Man Scenario List Based on research in all above the elements, a list of possible scenarios can be brought to the participants for their consideration, or a list of scenarios can be determined for an interview based process.

Participants in scenario analysis activities are better equipped to consider scenarios if they are provided with appropriate background resources.

(c) Qualified and Experienced Facilitators with Consistency in the Facilitation Process

The AMA Guidelines call for "qualified and experienced facilitators with consistency in the facilitation process."[4]

If the scenarios are being discussed in a group environment, such as a workshop, then there needs to be a neutral facilitator who not only knows the process completely but is also proficient at managing the conversations to ensure that no one person, or small group, is dominating the discussion and that all ideas are heard.

The skills needed often mean that scenario analysis workshops can be run only one at a time as the facilitation resources are in short supply.

(d) The Appropriate Representatives

The AMA Guidelines call for the involvement of all of "the appropriate representatives of the business, subject matter experts and the corporate operational risk management function as participants involved in the process."[5]

The written procedures for scenario analysis should probably include a list of the required quorum. If the firm has a scenario analysis process that requires each business line to complete a scenario analysis workshop for each risk category, then each category may have a different quorum. For example, for Employment Practice and Workplace Safety would require a representative from the human resources department.

Most scenarios benefit from attendance by representatives from the legal department, compliance, operations, and technology. Some may also benefit from representation from the finance department. The quorum requirements should be set appropriately.

If the quorum is not met, then it may be necessary to cancel and reschedule, or it might be possible to loop the missing participants into the review process afterwards.

(e) A Structured Process for the Selection of Data

The AMA Guidelines call for "a structured process for the selection of data used in developing scenario estimates."[6]

At the heart of scenario analysis activity is the gathering of data to be used to develop the scenario analysis estimates. In a workshop environment, these data include all background preparation data and the estimates that are solicited from the participants during the workshop. While the workshop environment may be a free-flowing conversation, there need to be checkpoints incorporated into the process to ensure that all procedural requirements are being met. For example, a workshop might be designed to gather a worst-case dollar amount for each scenario. If so, there needs to be a defined process by which the worst-case estimates are gathered from the participants in the room and their final consensus reached.

In an interview-based approach, the same challenges exist in ensuring that the way responses are gathered is carefully structured so that it can be clearly documented and is a repeatable process.

To meet this requirement, firms have adopted questionnaires and templates that assist the facilitators in keeping the process in line and ensuring the data is clearly gathered and documented.

Once the data have been gathered, through background preparation and through expert discussion and debate, it can then be used to draw conclusions on the possible severity and frequency for each scenario.

Some firms collect data at the risk category level rather than at the scenario level. For example, there may be five scenarios that have been identified in the Clients, Products, and Business Practices risk category.

Some firms would gather severity and frequency information for all five, and some firms gather severity and frequency for the group of five (e.g., how many of these scenarios could happen in the next ten years in total?).

Conclusions drawn and decisions made need to be clearly documented as discussed below.

(f) High-Quality Documentation Which Provides Clear Reasoning and Evidence Supporting the Scenario Output

The AMA Guidelines require "high-quality documentation which provides clear reasoning and evidence supporting the scenario output."[7]

In the early days of operational risk scenario analysis, there was a reluctance to document the discussions. Sensitive issues are often raised, and there may be disagreements during the discussions before consensus is reached. The idea of documenting all of those details left most firms feeling uncomfortable and their legal departments feeling anxious.

However, in the last few years, the regulatory pressure to ensure that all conclusions are supported by documented reasoning and evidence has led to a more highly documented process despite these concerns.

While the whole conversation does not need to be recorded, there does need to be a well-documented summary at the end of the process that outlines the thought processes, the data and evidence that was weighed and considered and the reason that consensus has been reached on certain conclusions such as severity and frequency.

It is hard for a facilitator to both facilitate the process and document what happens. For this reason, in workshop scenario analysis activities there is often a second neutral participant, perhaps from the corporate operational risk function, whose sole role is to document the proceedings. This is not a court reporter–type activity, but requires a deep understanding of the

process and procedures to ensure that all important aspects are captured in the documentation.

It is difficult to go back afterwards to look for consensus on something that was missed, and a robust documentation template can assist with ensuring that all important data points and rationales have been captured.

(g) Independent Challenge and Oversight

The AMA Guidelines call for a "robust independent challenge process and oversight by the corporate operational risk management function to ensure the appropriateness of scenario estimates."[8]

In a workshop, if the facilitator is provided by the corporate operational risk function, then they can take on the dual role of challenge also. If a third-party facilitator is used, then the corporate operational risk function can be a participant in the workshop and challenge as a member of the quorum.

In all types of scenario analysis, the corporate operational risk function can meet this challenge and oversight requirement by being actively involved in all preparation work, in the scenario analysis activities, and in the review of the documentation.

It is also helpful to establish a formal challenge and review process after the activity. This can consist of a simple e-mail documentation review by all participants or by a follow-up meeting to walk through the final documented conclusions.

(h) A Process That Is Responsive to Changes

The AMA Guidelines require "a process that is responsive to changes in both the internal and external environment."[9]

A scenario analysis activity should capture the current state of the business and control environments and should be designed to ensure that any changes in those environments will trigger a new activity as appropriate.

Many firms revisited their Internal Fraud scenario analysis after the 2012 UBS unauthorized trading event, and external events are helpful triggers for such reassessments. It is also important to revisit scenario analysis when a major business change occurs, such as an acquisition or divestiture. Similarly, a major control change such as a technology infrastructure rollout may trigger a new scenario analysis in impacted business and risk categories.

Regardless of triggers, scenario analysis should be conducted on a timely basis to ensure that it remains up-to-date as regards the current internal and external environment. For this reason, many firms will require them to be updated once a year even if no trigger has arisen.

However, the resource challenge can prove overwhelming and less frequent updates might be practically necessary.

(i) Mechanisms for Mitigating Biases

The AMA Guidelines draw attention to the need for "mechanisms for mitigating biases inherent in scenario processes. Such biases include anchoring, availability and motivational biases."[10]

In all methods there are biases that enter the process and that require careful consideration. While an expert may be knowledgeable on the subject matter of the scenario under discussion, they might not have the statistical background to understand the implications of certain estimates and decisions regarding impact and frequency of events. They are also likely to be untrained in the biases that can arise in such exercises and how to compensate for them.

Therefore, it is important to ensure that scenario analysis workshops and interviews are facilitated by someone who does have that experience or, at the very least, has an appreciation for the dangers of statistical and behavioral bias in the process.

Where possible, the process should avoid the introduction of biases when providing background or supporting data.

The Australian Prudential Regulation Authority produced a working paper in 2007 that addressed the inherent biases that occur in scenario analysis for operational risk and identified two classes of bias: judgmental and motivational.[11] This paper has stood the test of time and still provides strong guidance on how to address bias in scenario analysis today.

Judgmental bias occurs during the estimation process as the experts are swayed by the background data and the form of the questions. An example of judgmental bias is *availability* bias, which occurs when estimates are influenced by the availability of data. For example, past operational risk event data may be supplied to scenario analysis participants in the form of internal and external loss event data.

This data can influence the perception of likely size and frequency of events, and indeed the type of events that can occur. If an expert has recently experienced a particular event, they are more likely to deduce that that event can occur with a higher frequency and with a similar impact. For example, someone who has recently been in a car accident is likely to estimate the frequency of car accidents as higher than someone who has not.

Similarly, if the firm or the industry has recently experienced a large event, the scenario analysis participants are more likely to estimate that that event could occur again soon, and at the same impact level.

Another example of judgmental bias is *anchoring*. Anchoring occurs where participants are offered an initial estimate from which to base their

estimate. For example, internal and external data may anchor the estimates so that likely impacts beyond that size are considered unlikely, and frequencies that differ from the past are discounted as less plausible.

Scenario analysis should provide an opportunity to look forward and consider what could occur in the future, and not only what has already occurred in the past. Therefore, judgmental bias can seriously undermine the process if not carefully considered. For this reason, it may be best not to provide internal loss data and to only use it as a floor. The facilitator can have access to this data and refer to it if the scenario participants are estimating close to that floor.

The careful use of internal and external data, and facilitation by the operational risk department can help to overcome these biases. By addressing these biases up front, the participants can be assisted in resisting these and keeping their estimation processes less constrained to the judgmental influences.

Motivational bias occurs where the estimates of the participants are influenced not by the data presented, but by the personal interest of the participants themselves. More crudely, this can be referred to as "gaming the system." Senior management may be particularly susceptible to this bias, as they may perceive an estimate that suggests a potentially high impact as reflecting poorly on their department's risk management practices.

In addition, if scenario analysis is used as an input into a capital calculation for operational risk capital then participants will be aware that high estimates may result in high capital, and so may resist estimating the fat-tail events effectively.

Overcoming motivation bias is more challenging than overcoming judgmental bias. One way to avoid gaming of the scenario analysis estimates is to ensure that allocation of capital is driven not only by scenario analysis but also by RCSA, KRI, and loss data results. Alternatively, scenario analysis can be done at the top of the house, rather than at the business unit level, and then allocated down to business lines using a combination of operational risk information.

The facilitator of the scenario analysis workshop might also set parameters for the estimates that preclude underestimating. For example, they might set minimum limits at past event levels if they are in fact larger or more frequent than the estimates.

SCENARIO ANALYSIS OUTPUT

Different methods produce different outputs, but the goal of scenario analysis is to produce reasoned assessments of plausible severe losses, and so outputs need to support that goal.

Some scenario analysis methods produce an average loss estimate, a worst-case loss estimate and frequency estimates for each of these

values. Some produce just the worst-case estimate and a single frequency estimate. Others produce a range of loss estimates, with frequency estimates for each loss. Still others produce the latter range plus a maximum loss estimate.

One example of possible scenario analysis output is illustrated in Table 11.1. In this table, the firm has taken an approach where it collects the number of events that might occur in a category, rather than the number of times a single scenario might occur. They are collecting a range of frequencies for each risk category in a selection of severity ranges.

For example, in the Clients, Products, and Business Practices category they have decided upon all the scenarios that apply and are now estimating how many of those scenarios could occur in total.

In the $1 million to $5 million bucket (A), they have agreed that it is plausible that they could experience five events in this category. Hence, they have entered a frequency of five. However, in the greater than $100 million bucket (B), they have agreed that such a large event could occur only once every 10 years. Hence, they have entered a frequency of 0.1.

The total frequency (C) represents how many events could occur in this category in a single year and is simply the sum of the buckets.

The final column (D) contains a maximum loss amount that has been agreed in the scenario analysis workshops.

Some categories do not have any entries (E), as the group has determined that in fact no event could occur at that size. Of course, such an estimation process as is represented in Table 11.1 would have to have be supported by robust procedures, supporting evidence, and well-documented rationale.

The output drives how the scenario analysis information is then used for risk management or for capital calculation purposes, and the model that is applied to calculating capital for the firm. This capital model may have many other elements, and capital calculation methods are considered further in Chapter 12.

While designed to produce fat-tail estimates, scenario analysis is often also responsible for the identification of significant mitigation activities that should be undertaken in order to lessen the risks identified.

This can mean that some overlap occurs between the RCSA program and scenario analysis, particularly if the workshop RCSA method is being used. Indeed, some firms have combined the two elements of the operational risk framework, and at the end of an RCSA workshop they will ask the participants to consider the same risks in an environment where all controls fail. In this way participants can extrapolate from known and relatively well-controlled risks, to extreme but plausible fat-tail events.

TABLE 11.1 Sample Scenario Analysis Output

Risk Category	Frequency/Severity Buckets						Total Annual Frequency	Max Single Loss
	$1 to $5M	$5 to $10M	$10 to $20M	$20 to $50M	$50 to $100M	> $100M		
Clients, Products, and Business Practices	5.0(A)	3.0	1.0	0.5	0.2	0.1(B)	9.8(C)	$600M(D)
Execution, Delivery, and Process Management	10.0	5.0	2.0	0.5	0.2	0.1	17.8	$150M
External Fraud	1.0	0.5	0.2	0.1	–	–	1.8	$45M
Internal Fraud	1.0	0.5	0.1	0.1	0.1	0.1	1.9	$1,000M
Damage to Physical Assets	3.0	1.0	1.0	0.5	0.2	0.1	5.8	$100M
Employee Practices and Workplace Safety	5.0	3.0	2.0	1.0	0.5	–	22.5	$75M
Business Disruption and Systems Failures	6.0	4.0	2.0	1.0	– (E)	–	13	$40M

Most operational risks that have a high impact occur as a result of multiple control failings, and the RCSA process can help with the thought processes behind imagining such events. The risk is identified in an RCSA. The controls are scored for effectiveness and the residual risk assessed. Then the same risk is considered in a situation where all controls fail in order to envisage the fat-tail event.

KEY POINTS

- Firms use scenario analysis to evaluate their exposure to high-severity events by deriving reasoned assessments of plausible severe losses.
- There are several different methods for scenario analysis, including workshops and interviews. A robust scenario analysis process includes:
  - A clearly defined and repeatable process
  - Good-quality background preparation
  - Qualified and experienced facilitators
  - The appropriate quorum of participants
  - A structured process for the selection of data
  - High-quality documentation
  - A robust independent challenge process
  - A process that is responsive to change
  - Bias minimization
- The output from scenario analysis can be used as an input into capital calculations and to inform the firm of potentially catastrophic operational risk losses.

REVIEW QUESTIONS

1. The Basel II definition of scenario analysis requires which of the following elements as part of the process?
   - **I.** Knowledge of experienced business managers
   - **II.** Knowledge of experienced risk management experts
   - **III.** Knowledge of external independent advisers
   - **IV.** Reasoned assessments of plausible severe losses

   a. I, II, and III
   b. I and II only
   c. I, II, and IV only
   d. All of the above

2. During a scenario analysis workshop, a senior manager becomes concerned that an honest but high estimate of plausible losses will reflect badly on her management skills. How might this significantly impact the results? Select the best answer.
   a. The results may reflect a motivational bias.
   b. The results may reflect a judgmental bias.
   c. The results will be unaffected.
   d. The results will reflect the true opinion of the senior manager.

NOTES

1. Bank of International Settlements, Basel Committee on Banking Supervision, "International Convergence of Capital Measurement and Capital Standards: A Revised Framework," Comprehensive Version, 2006, section 675.
2. Basel Committee on Banking Supervision, "Operational Risk—Supervisory Guidelines for the Advanced Measurement Approaches, June 2011. Retrieved from www.bis.org/publ/bcbs196.pdf, section 254.
3. Ibid., (b).
4. Ibid., (c).
5. Ibid., (d).
6. Ibid., (e).
7. Ibid., (f).
8. Ibid., (g).
9. Ibid., (h).
10. Ibid., (i).
11. Emily Watchorn, "Applying a Structured Approach to Operational Risk Scenario Analysis in Australia," APRA Working Paper, September 2007.

CHAPTER 12

Capital Modeling

In this chapter, we will explore the various methods for calculation operational risk capital and the challenges faced in adopting the advanced measurement approach. Different capital modeling methods are discussed and compared and the use importance of correlation and insurance offsets are considered. Finally, the disclosure requirements are introduced.

OPERATIONAL RISK CAPITAL

Firms that are required to, or that choose to calculate operational risk capital can select from several methods.

Basel II provides three main approaches to calculating operational risk capital: the basic approach, the standardized approach, and the advanced Measurement Approach (AMA) (see Figure 12.1).

If an AMA is being used, then calculation will draw on the underlying elements, as is illustrated in Figure 12.2. If a simpler approach is being used, then the underlying elements need not feed into the model.

Under the Basel II rules banks are encouraged to move toward the more sophisticated approaches as they develop their operational risk management tools. Basel II expects international active banks to select either the standardized or advanced measurement approaches. Many national regulators have mandatory requirements that force large financial institutions to adopt the advanced measurement approach for operational risk if they wished to be approved for Basel II overall.

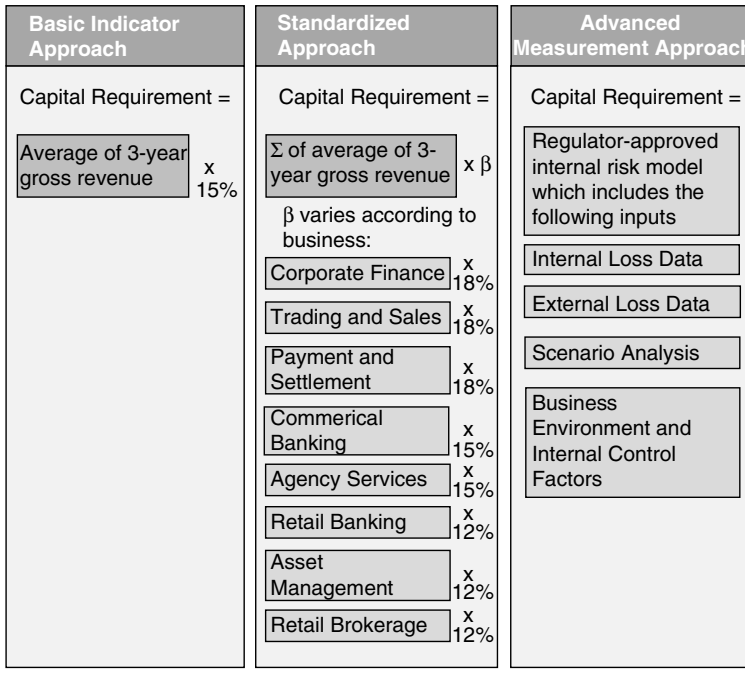

FIGURE 12.1 The Three Basel II Operational Risk Capital Methods

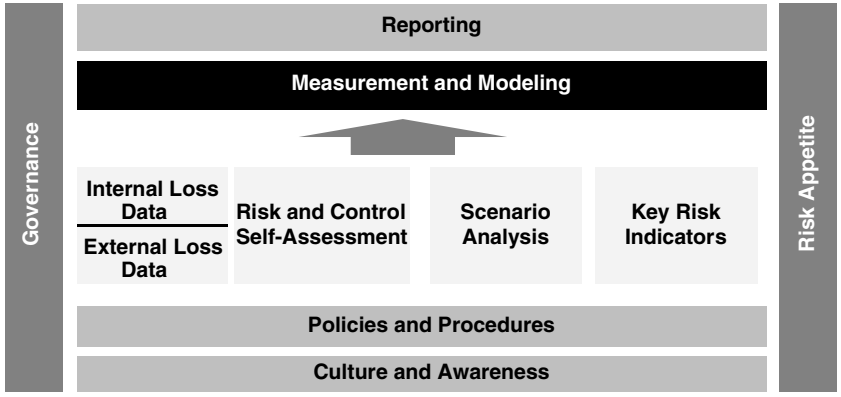

FIGURE 12.2 The Role of Capital Modeling in the Operational Risk Framework

BASIC INDICATOR APPROACH

Under the Basic Indicator Approach (BIA), the capital calculation is arrived at through a simple calculation of the average gross revenue for the past three years, multiplied by 15 percent. Basel II outlines the approach as follows:

> *Banks using the Basic Indicator Approach must hold capital for operational risk equal to the average over the previous three years of a fixed percentage (denoted alpha) of positive annual gross income. Figures for any year in which annual gross income is negative or zero should be excluded from both the numerator and denominator when calculating the average. The charge may be expressed as follows:*

$$K_{BIA} = \left[\left(GI_{1..n} \times \alpha \right) \right] / n$$

where:

K_{BIA} =the capital charge under the Basic Indicator Approach

GI =annual gross income, where positive, over the previous three years

N =number of the previous three years for which gross income is positive

α =15 percent, which is set by the Committee, relating the industry wide level of required capital to the industry wide level of the indicator

> *Gross income is defined as net interest income plus net non-interest income.*[1]

Firms that use this approach are still encouraged to adopt all of the risk management elements that are outlined in the "Sound Practices"[2] document. Therefore, even though loss data, RCSA, scenario analysis, and business environment internal control factors (BEICF) are not needed for the capital calculation, they are needed as part of the operational risk framework to ensure that the firm can adequately identify, assess, monitor and mitigate operational risk as required in the "Sound Practices" document.

If a bank has negative or zero income for any of the three years, then BIA instructs them to remove those years from both the numerator and denominator when calculation the average revenue.

EXAMPLE

Alpha Bank has the following revenue results from the past three years:

	Year One	Year Two	Year Three
Annual Gross Revenue (in $100m)	15	20	25

To calculate the BIA capital charge $K_{BIA} = \left[\left(GI_{1..n} \times \alpha\right)\right]/n$ we insert the values

$$\begin{aligned} GI &= (15 + 20 + 25) \\ N &= 3 \\ \alpha &= 15\% \end{aligned}$$

As follows:

$$K_{BIA} = \frac{\left[(60 \times 0.15)\right]}{3}$$

To give a result:

$$K_{BIA} = 3$$

Therefore, Alpha Bank must hold $300m operational risk capital under Basel II using the Basic Indicator approach.

EXAMPLE

Alpha Bank has the following revenue results from the past three years:

	Year One	Year Two	Year Three
Annual Gross Revenue (in $100m)	15	–20	25

To calculate the BIA capital charge $K_{BIA} = \left[\left(GI_{1..n} \times \alpha\right)\right]/n$ we insert the values

GI = (15 + 25) [year two is not counted]
N = 2 [year two is not counted]
α = 15%

As follows:

$$K_{BIA} = \frac{\left[\left(40 \times 0.15\right)\right]}{2}$$

To give a result:

$$K_{BIA} = 3$$

Therefore, Alpha Bank would still hold $300m operational risk capital under Basel II using the basic indicator approach even though it experienced negative revenue in year two.

The basic approach to capital is certainly simple to adopt but does little to reflect the operational risk in a firm, as it uses only revenue as a driver. A firm that has very strong controls will have the same operational risk requirements as a firm with very poor controls if they have had the same average revenue over the past three years.

Furthermore, a firm will enjoy much lower operational risk capital requirements in years when it is producing lower revenue, even if its controls have not changed at all.

STANDARDIZED APPROACH

The standardized approach is similar to the basic approach, except that different business lines have different multipliers. The standardized approach attempts to capture operational risk factors that are missing in the basic approach by assuming that different types of business activities carry different levels of operational risk. Sales and trading is riskier than retail brokerage, for example. Basel II puts it thus:

> *Within each business line, gross income is a broad indicator that serves as a proxy for the scale of business operations and thus the likely scale of operational risk exposure within each of these business lines.*[3]

As a result, although the calculation method is the same, the multiplier used varies according to the business line. This will result in several separate calculations that are then brought together for the total operational risk capital.

The total capital charge is calculated as the three-year average of the simple summation of the regulatory capital charges across each of the business lines in each year. In any given year, negative capital charges (resulting from negative gross income) in any business line may offset positive capital charges in other business lines without limit.

However, where the aggregate capital charge across all business lines within a given year is negative, then the input to the numerator for that year will be zero. The total capital charge may be expressed as:

$$K_{TSA} = \left\{ \sum_{\text{years } 1-3} max\left[\sum \left(GI_{1-8} \times \beta_{1-8} \right), 0 \right] \right\} / 3$$

where:

K_{TSA} = the capital charge under the standardized approach

$GI_{1\text{-}8}$ = annual gross income in a given year, as defined above in the basic indicator approach, for each of the eight business lines

$\beta_{1\text{-}8}$ = a fixed percentage, set by the Committee, relating the level of required capital to the level of the gross income for each of the eight business lines. The values of the betas are detailed below.

Business Lines	Beta Factors
Corporate finance (β_1)	18%
Trading and sales (β_2)	18%
Retail banking (β_3)	12%
Commercial banking (β_4)	15%
Payment and settlement (β_5)	18%
Agency services (β_6)	15%
Asset management (β_7)	12%
Retail brokerage (β_8)	12%[4]

The TSA calculation of operational risk capital is no more difficult than the BIA, but it does have significantly more steps, as a calculation must be made for all business lines in order to produce the final capital result.

In the example below, Beta Bank has only three lines of business and is using the TSA calculation method for its operational risk capital.

EXAMPLE

Beta Bank has the following revenue in $100m for the past three years for its three lines of business: trading and sales, commercial banking, and asset management.

	Year One	Year Two	Year Three
Trading and sales	15	20	25
Commercial banking	10	5	10
Asset management	5	5	5

To calculate the TSA capital charge $K_{TSA} = \frac{\left\{\sum_{\text{years } 1-3} max\left[\sum\left(GI_{1-8} \times \beta_{1-8}\right), 0\right]\right\}}{3}$ we insert the appropriate β values:

	Year One	Year Two	Year Three
Trading and sales	15 × 18% = 2.7	20 × 18% = 3.6	25 × 18% = 4.5
Commercial banking	10 × 15% = 1.5	5 × 15% = 0.75	10 × 15% = 1.5
Asset management	5 × 12% = 0.6	5 × 12% = 0.6	5 × 12% = 0.6
Total	**4.8**	**4.95**	**6.6**

Entering these totals into the TSA calculation:

$$K_{TSA} = \frac{\{4.8 + 4.95 + 6.6\}}{3}$$

To give a result:

$$K_{TSA} = 5.45$$

Therefore, Beta Bank would hold $545m operational risk capital under Basel II using the standardized approach.

If there is negative or zero income during one of the three prior years, the TSA takes a different treatment approach than that used in the BIA. In the BIA, any years that have negative or zero income are removed from both the denominator and the numerator. However, under the TSA:

> *In any given year, negative capital charges (resulting from negative gross income) in any business line may offset positive capital charges in other business lines without limit. However, where the aggregate capital charge across all business lines within a given year is negative, then the input to the numerator for that year will be zero.*[5]

Note that the denominator in TSA is set at 3.

EXAMPLE

If Beta Bank has negative revenue in any business line, then that can offset the capital charges for that year up to a maximum benefit of zero capital (no negative capital is permitted for a year).

Beta Bank has the following revenue in $100m for the past three years for its two lines of business, corporate finance, and retail banking.

	Year One	Year Two	Year Three
Corporate finance	10	20	30
Retail banking	5	–25	–55

To calculate the TSA capital charge $K_{TSA} = \frac{\left\{\sum_{\text{years } 1-3} max\left[\sum (GI_{1-8} \times \beta_{1-8}), 0\right]\right\}}{3}$ we insert the appropriate β values:

	Year One	Year Two	Year Three
Corporate finance	10 × 18% = 1.8	20 × 18% = 3.6	30 × 18% = 5.4
Retail banking	5 × 12% = 0.6	–25 × 12% = –3	–55 × 12% = –6.6
Total	**2.4**	**0.6**	**–1.2**

As a negative number must not be entered into the calculation, we replace –1.2 in year three with zero. Entering these totals into the TSA calculation:

$$K_{TSA} = \frac{\{2.4 + 0.6 + 0\}}{3}$$

To give a result:

$$K_{TSA} = 1$$

Therefore, Beta Bank would hold $100m operational risk capital under Basel II using the standardized approach.

Alternative Standardized Approach

Basel II allows a national regulator to permit a bank to use an alternative standardized approach (ASA) provided "the bank is able to satisfy its supervisor that this alternative approach provides an improved basis by, for example, avoiding double counting of risks."

Under the ASA, the operational risk capital charge/methodology is the same as for the Standardized Approach except for two business lines—retail banking and commercial banking. For these business lines, loans and advances—multiplied by a fixed factor "m"—replaces gross income as the exposure indicator.

The ASA operational risk capital charge for retail banking (with the same basic formula for commercial banking) can be expressed as:

$$K_{RB} = \beta_{RB} \quad m \quad LA_{RB}$$

where:

K_{RB} = the capital charge for the retail banking business line

β_{RB} = the beta for the retail banking business line

LA_{RB} = total outstanding retail loans and advances (non-risk-weighted and gross of provisions), averaged over the past three years

m = 0.035

For the purposes of the ASA, total loans and advances in the retail banking business line consists of the total drawn amounts in the

following credit portfolios: retail, SMEs treated as retail, and purchased retail receivables. For commercial banking, total loans and advances consists of the drawn amounts in the following credit portfolios: corporate, sovereign, bank, specialized lending, SMEs treated as corporate and purchased corporate receivables. The book value of securities held in the banking book should also be included.

Under the ASA, banks may aggregate retail and commercial banking (if they wish to) using a beta of 15%.

Similarly, those banks that are unable to disaggregate their gross income into the other six business lines can aggregate the total gross income for these six business lines using a beta of 18%, with negative gross income treated as described in paragraph 654.

As under the Standardized Approach, the total capital charge for the ASA is calculated as the simple summation of the regulatory capital charges across each of the eight business lines.[6]

Future of the Basic and Standardized Approaches

The BIA and TSA methodologies can produce an unanticipated result as is demonstrated in the example below.

EXAMPLE

In the prior example Beta Bank had the following revenue in $100m:

	Year One	Year Two	Year Three
Corporate finance	10	20	30
Retail banking	5	–25	–55
Total	**15**	**–5**	**–25**

This resulted in a TSA capital charge of $100m.

If Beta Bank was calculating its capital under the BIA approach to calculate the BIA capital charge $K_{BIA} = \left[\left(GI_{1..n} \times \alpha\right)\right] / n$ we insert the values

$$GI = 15$$
$$N = 1$$

[Years two and three are not counted in the nominator or denominator as they have negative total income]

$$\alpha = 15\%$$

As follows:

$$K_{BIA} = \frac{[15 \quad 0.15]}{1}$$

To give a result:

$$K_{BIA} = 2.25$$

Therefore, Beta Bank would hold $100m operational risk capital under Basel II using the standardized approach, but $225m under the basic indicator approach.

This was likely not the intent of the Basel Committee, and they recognized that making allowances for negative income might produce an inappropriate result.

> *If negative gross income distorts a bank's Pillar 1 capital charge, supervisors will consider appropriate supervisory action under Pillar 2.*[7]

Therefore, if the use of negative income offsets produces an unpalatable or inappropriate result, then a bank may see their regulators adding on capital under the Pillar 2 requirements of Basel II. As discussed in Chapter 2, Pillar 2 provides a mechanism for additional capital requirements to cover any material risks that have not been effectively captured in Pillar 1.

ADVANCED MEASUREMENT APPROACH

The advanced measurement approach (AMA) allows a bank to design its own model for calculating operational risk capital. The Basel Committee recognized that they were allowing significant flexibility for the design of the AMA capital model, although there are three main requirements.

The first was that the model must hold capital for a one-year horizon at 99.9 percent confidence level. In other words, the capital held must be sufficient to cover all operational risk losses in one year with a certainty of 99.9 percent.

This is the equivalent of asking for a bank to hold operational risk capital that will protect it from a one in a thousand year fat-tail event.

AMA soundness standard

Given the continuing evolution of analytical approaches for operational risk, the Committee is not specifying the approach or distributional assumptions used to generate the operational risk measure for regulatory capital purposes. However, a bank must be able to demonstrate that its approach captures potentially severe "tail" loss events. Whatever approach is used, a bank must demonstrate that its operational risk measure meets a soundness standard comparable to that of the internal ratings-based approach for credit risk (i.e., comparable to a one year holding period and a 99.9th percentile confidence interval).[8]

The second requirement is that all four elements of the framework must be included in the model: internal loss data, external loss data, scenario analysis, and business environment internal control factors.

. . . a bank's internal measurement system must reasonably estimate unexpected losses based on the combined use of internal and relevant external loss data, scenario analysis and bank-specific business environment and internal control factors.[9]

The third requirement is that there must be an appropriate method for allocating the capital to the businesses to incent good behavior.

The bank's measurement system must also be capable of supporting an allocation of economic capital for operational risk across business lines in a manner that creates incentives to improve business line operational risk management.[10]

There are then several important quantitative stipulations.

The first stipulation is that the model must represent the operational risk framework as outlined in Basel II.

Any internal operational risk measurement system must be consistent with the scope of operational risk defined by the Committee in paragraph 644 and the loss event types defined in Annex 9.[11]

In effect, this means that calculations should be made for all seven risk categories. Some firms calculate capital at the top of the firm and then

allocate operational risk capital down into the business lines. Others calculate capital at the business line. Table 12.1 shows a matrix for capital calculations using the Basel business lines. However, a firm might have different headings in the first column to better represent their own business line structure.

The second stipulation is that the model must capture all expected and unexpected losses, and may only exclude expected losses under certain strict criteria.

> *Supervisors will require the bank to calculate its regulatory capital requirement as the sum of expected loss (EL) and unexpected loss (UL), unless the bank can demonstrate that it is adequately capturing EL in its internal business practices. That is, to base the minimum regulatory capital requirement on UL alone, the bank must be able to demonstrate to the satisfaction of its national supervisor that it has measured and accounted for its EL exposure.*[12]

TABLE 12.1 Example Capital Calculation Matrix

	Internal Fraud	External Fraud	Clients, Products, and Business Practices	Execution, Delivery, and Process Management	Employment Practices and Workplace Safety	Damage to Physical Assets	Business Disruption and System Failures
Corporate Finance							
Trading and Sales							
Retail Banking							
Commercial Banking							
Payment and Settlement							
Agency and Custody							
Retail Brokerage							
Asset Management							

The third stipulation is that the model must provide sufficient detail and granularity to ensure fat-tail events are captured.

> *A bank's risk measurement system must be sufficiently "granular" to capture the major drivers of operational risk affecting the shape of the tail of the loss estimates.*[13]

The fourth stipulation is that the bank must sum all calculated cells or defend any correlation assumptions that are made in its AMA model.

> *Risk measures for different operational risk estimates must be added for purposes of calculating the regulatory minimum capital requirement. However, the bank may be permitted to use internally determined correlations in operational risk losses across individual operational risk estimates, provided it can demonstrate to the satisfaction of the national supervisor that its systems for determining correlations are sound, implemented with integrity, and take into account the uncertainty surrounding any such correlation estimates (particularly in periods of stress). The bank must validate its correlation assumptions using appropriate quantitative and qualitative techniques.*[14]

The fifth stipulation simply reinforces the requirement that all four elements must be in the model.

> *Any operational risk measurement system must have certain key features to meet the supervisory soundness standard set out in this section. These elements must include the use of internal data, relevant external data, scenario analysis and factors reflecting the business environment and internal control systems.*[15]

Finally, the bank must weight these four elements appropriately.

> *A bank needs to have a credible, transparent, well-documented and verifiable approach for weighting these fundamental elements in its overall operational risk measurement system.*[16]

The Basel rules also provide many qualitative requirements that must be met in order for a bank to qualify for an AMA model for Basel II. Many of these have been discussed in prior chapters, for example the rules regarding the collection and use of loss data, the challenges of scenario analysis and the use of BEICF from RCSA and KRI elements in the operational risk framework.

While the four elements must be considered in the capital calculation methodology, many bank's use some of these elements to allocate capital, to stress test their models or to adjust their models, rather than using them to provide direct inputs into the capital calculation. Regulators have accepted many different models for AMA and the modeling of operational risk capital is developing rapidly as different approaches are tried and tested by the banking industry.

Many firms, however, are still wrestling with their AMA models and continue to seek Basel II approval for them. At the time of writing, no U.S. banks had successfully received Basel II approval. However, such approval requires them to meet many requirements above and beyond operational risk, so it is difficult to judge whether they have successfully completed their operational risk capital models.

In contrast, in Europe many banks have received Basel II approval, and they have used a variety of AMA models in order to meet the operational risk requirements. We will consider some of the modeling options that are available.

Loss Distribution Approach to Modeling Operational Risk Capital

A loss distribution approach (LDA) model relies on internal losses as the mainstay of its design. A simple LDA model uses only internal losses as direct inputs into the model and uses the remaining three elements for stressing or allocation purposes.

A bank must have at least three years of loss data to put into its AMA model, regardless of design as the data may be rich enough to form the basis of a capital model.

> *Internally generated operational risk measures used for regulatory capital purposes must be based on a minimum five-year observation period of internal loss data, whether the internal loss data is used directly to build the loss measure or to validate it. When the bank first moves to the AMA, a three-year historical data window is acceptable.*[17]

Despite this stipulation, regulators are leaning towards requiring all available data to be included, even beyond the five-year requirement. In their recent AMA Guidelines, the Basel Committee noted:

> *The Basel II Framework requires banks to base their internally generated operational risk measures on a minimum historical*

observation period of five years (three years when an institution first moves to an AMA). For certain ORCs with low frequency of events, an observation period greater than five years may be necessary to collect sufficient data to generate reliable operational risk measures and ensure that all material losses are included in the calculation dataset.[18]

The advantage of a loss distribution approach is that the model is based on real historical data that is relevant to the firm.

The disadvantage of a loss distribution approach is that the period of data collection is likely to be relatively short, and so may not have captured the fat-tail events that the capital calculation is supposed to protect the firm from. It certainly will not contain 1,000 years of data, and yet the model is supposed to provide a 99.9 percent confidence level. Some firms also find that they have insufficient loss data on which to build a model even if they have over five years of data.

In addition, historical data does not necessarily reflect the future. The firm may have changed its products, processes, and controls.

Although there is a wide range of AMA modeling practices, even within the LDA approach, there are some standard methods that are worthy of discussion.

Step 1: Modeling Frequency In order to develop a model of expected operational risk losses, the first step is to determine the likely number of events per year. This is the frequency of events.

The most popular distribution selection for modeling frequency is the Poisson distribution. This allows for a fairly simple approach to modeling frequency. In a Poisson distribution there is only a single parameter (λ), which represents the average number of events in a given year. Both the mean and the variance are represented by this single parameter in a Poisson distribution. In more complex cases, a negative binomial distribution may be used, which allows for different values for the mean and variance.

The Poisson distribution works well for a situation where there is a whole number of events and where the probability in one time period is the same as in another time period. The Poisson distribution is built from the use of the average number of events using the following formula.

$$f(n) = \frac{\lambda^N e^{-\lambda}}{n!}$$

Where

n = 0, 1, 2,....

λ = average number of events in a year

In an LDA model, λ can be obtained simply by observing the number of events per year in the internal loss data history and calculating the average.

EXAMPLE

Lambda Bank has been gathering loss data for the past seven years and has observed the following number of events each year.

Year	1	2	3	4	5	6	7
# of loss events	746	810	765	940	780	695	850

λ = (746 + 810 + 765 + 940 + 780 + 695 + 850) / 7 = **798**

The Poisson distribution that is derived from this approach represents the probability of a certain number of events occurring in a single year. As can be seen in the Figure 12.3, lower lambdas produce more skewed and leptokurtic[19] annual loss distributions than higher lambdas.

Step 2: Modeling Severity The next step in modeling expected operational risk losses is to determine the likely size of an event given the fact that an event has occurred. This is the severity of an event.

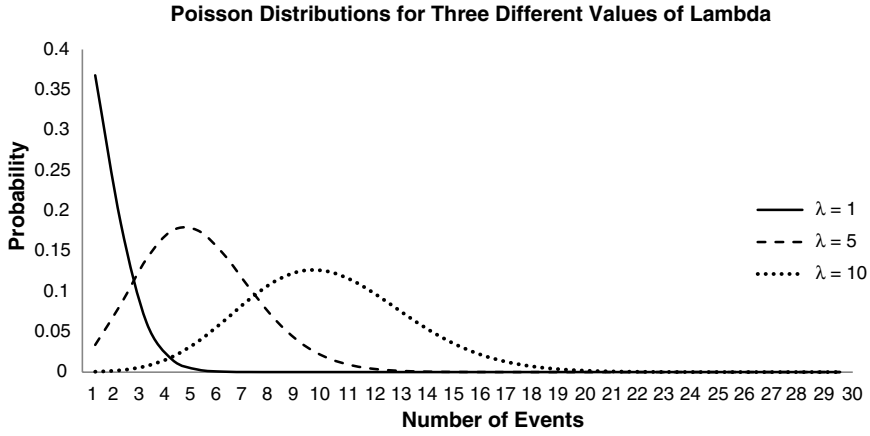

FIGURE 12.3 Comparing Three Different Poisson Distributions

Unlike frequency, severity need not be an integer, but can fall anywhere along a continuum. When a loss occurs it might be $1.50 or it might be $133,892.25 or any other value. The severity distribution establishes the probability of an event occurring over a wide range of values, from zero to very, very large losses.

The most common and least complex approach to modeling severity is to use a lognormal distribution, although low frequency losses may fit better to other options such as Generalized Gamma, Transformed Beta, Generalized Pareto, or Weibull. Regulators take a keen interest in how well the selected distribution demonstrates "goodness of fit"—or in other words, how certain are you that the sample comes from the population with the claimed distribution. When selecting which approach to use, the AMA guidelines also provide the following guidance (emphasis added):

> *The selection of probability distributions should be consistent with all elements of the AMA model. In addition to statistical goodness of fit, Dutta and Perry (2007) have proposed the following criteria for assessing a model's suitability:*
>
> - **realistic** *(e.g., it generates a loss distribution with a realistic capital requirements estimate, without the need to implement "corrective adjustments" such as caps),*
> - **well specified** *(e.g., the characteristics of the fitted data are similar to the loss data and logically consistent),*
> - **flexible** *(e.g., the method is able to reasonably accommodate a wide variety of empirical data) and*
> - **simple** *(e.g., it is easy to implement and it is easy to generate random numbers for the purpose of loss simulation).*
>
> *The process of selecting the probability distribution should be well-documented, verifiable and lead to a clear and consistent choice. To this end, a bank should generally adhere to the following:*
>
> *(a) Exploratory Data Analysis (EDA) for each ORC to better understand the statistical profile of the data and select the most appropriate distribution;*
> *(b) Appropriate techniques for the estimation of the distributional parameters; and*
> *(c) Appropriate diagnostic tools for evaluating the quality of the fit of the distributions to the data, giving preference to those most sensitive to the tail.*[20]

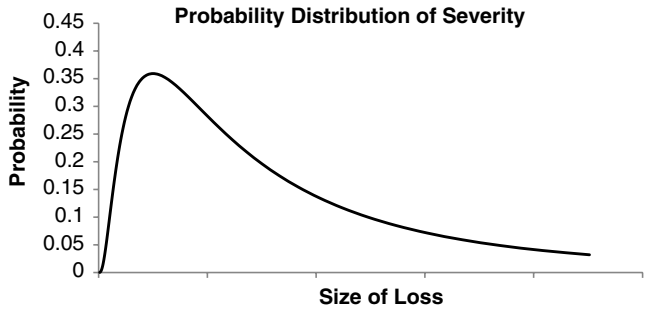

FIGURE 12.4 The Severity Probability Distribution

Whichever distribution is selected, the probability density function for severity will have a fat tail, that is to say that very large events (beyond three standard deviations of the mean) are more likely to occur than in a normal distribution. It will also be skewed to the right, as can be seen in the example in Figure 12.4.

Step 3: Monte Carlo Simulation Once the frequency and severity distributions have been established, the next step is to use these distributions to generate many more data points in order to better estimate the capital needed to ensure with 99.9 percent certainty that likely losses for the next year are covered by appropriate capital.

Monte Carlo simulation provides a method by which frequency and severity distributions can be combined to produce many more data points that have the same characteristics as the observed data points. Excel can handle this process using built in functionality, but often much more powerful statistical modeling tools are used.

First, a data point is selected from the frequency distribution. This gives us the number of events that are predicted to occur in year one. Values nearer the mean of the frequency distribution will be selected more often than values far from the mean. In this example, let us say that the number 50 is selected. Therefore, in year one the model assumes there were 50 events.

Next, the size of each of those 50 events is selected from the severity distribution. Again, values with a higher probability in the severity distribution will be selected more often than values with a lower probability. This will produce 50 losses for year one.

The value of all 50 losses is then added together to give the total value of losses for year one.

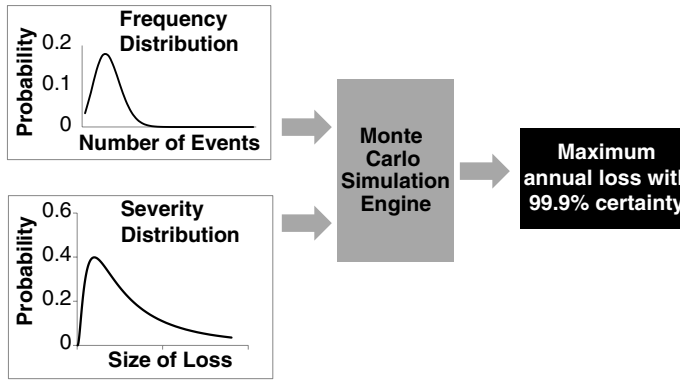

FIGURE 12.5 Using Monte Carlo Simulation

This process is repeated for year two, and then over and over again, a million times, thus giving the modeler many additional years of representative data. The data is then placed in size order, the largest total year loss, to the smallest total year loss.

Finding the 99.9 percent confidence level is simply a case of selecting the one thousandth item in the ordered list. That value represents, with 99.9 percent certainty, the maximum loss that will be experienced in a single year.

This process is represented in Figure 12.5.

Correlation Once all of the cells of the operational risk capital matrix have been populated, with a calculated capital amount for each risk category, and possibly also for every business line, then all of the cells must be simply added together to produce the total capital required. However, firms can take advantage of correlation assumptions between cells if these assumptions can be defended.

> *Risk measures for different operational risk estimates must be added for purposes of calculating the regulatory minimum capital requirement. However, the bank may be permitted to use internally determined correlations in operational risk losses across individual operational risk estimates, provided it can demonstrate to the satisfaction of the national supervisor that its systems for determining correlations are sound, implemented with integrity, and take into account the uncertainty surrounding any such correlation estimates (particularly in periods of stress). The bank must validate its correlation assumptions using appropriate quantitative and qualitative techniques.*[21]

Some firms have found the ORX data useful for this purpose. ORX data contains loss data for all risk categories for all firms that are consortium members. If a correlation matrix can be established for that large pool of data it might be possible to use those same assumptions for the internal AMA model of a member firm. With no correlation assumptions, the additive nature of the model can produce very high capital results. As a result there is an enormous amount of work (internally and with consulting firms) currently under way in the industry, as firms attempt to better support correlation assumptions for use in operational risk capital modeling.

Scenario Analysis Approach to Modeling Operational Risk Capital

A pure scenario analysis approach to modeling uses only scenario analysis data in the model. The other three required elements are used for stress testing, validation, or allocation.

Scenario analysis data is designed to identify fat-tail events, and therefore may provide rich data for the calculation of appropriate operational risk capital.

The advantages of a scenario analysis approach are that the data reflects the future as it is captured in a process that is designed to consider "what if" scenarios. In contrast, an LDA approach is only considering the past.

One of the major disadvantages of a scenario analysis approach is that the data is highly subjective, as it has probably been gathered in an interview or workshop estimation exercise. Also, scenario analysis produces only a few data points and so complex techniques have to be applied to model the data into a full distribution.

While the same methods for frequency and severity distributions and Monte Carlo simulations might be used as in the LDA approach above, the lack of data in scenario analysis output can make the fitting of distributions particularly troublesome. A small change in assumptions can lead to very different results, and therefore the defense of all assumptions must be particularly robust in a scenario analysis approach.

The data for use in the model may look similar to the output example in Chapter 11 and shown again in Table 12.2, or it might be a simple series of maximum loss amounts per risk category, or per scenario.

There are many possible outputs from the many different scenario approaches in use. Whatever scenario analysis method is used, there will likely be a paucity of data points and so a pure scenario analysis approach can be difficult to defend. Indeed, although some scenario-based models may have been approved in Europe, they are generally frowned upon by the regulators in the United States.

TABLE 12.2 Sample Scenario Analysis Output

Risk Category	Frequency/Severity Buckets						Total Annual Frequency	Max Single Loss
	$1 to $5m	$5 to $10m	$10 to $20m	$20 to $50m	$50 to $100m	> $100m		
Clients, Products, and Business Practices	5.0(A)	3.0	1.0	0.5	0.2	0.1(B)	9.8(C)	$600m(D)
Execution, Delivery, and Process Management	10.0	5.0	2.0	0.5	0.2	0.1	17.8	$150m
External Fraud	1.0	0.5	0.2	0.1	—	—	1.8	$45m
Internal Fraud	1.0	0.5	0.1	0.1	0.1	0.1	1.9	$1,000m
Damage to Physical Assets	3.0	1.0	1.0	0.5	0.2	0.1	5.8	$100m
Employee Practices and Workplace Safety	5.0	3.0	2.0	1.0	0.5	—	22.5	$75m
Business Disruption and Systems Failures	6.0	4.0	2.0	1.0	— (E)	—	13	$40m

Certainly, the more reliance there is on scenario analysis, the more robust the scenario analysis program must be.

There may well be cells in the model that rely on a pure scenario analysis model simply because there is little or no loss data available in that cell. It is acceptable to have different modeling techniques in different cells of the model as long as the differences are justified.

Hybrid Approach to Modeling Operational Risk Capital

Many firms have some version of a hybrid approach. In a hybrid approach, the loss data and scenario analysis output are both used to calculate appropriate operational risk capital.

Some firms combine the LDA and scenario analysis approaches by stitching together two distributions, for example, by using LDA for the left end of the distribution, or the expected losses, and scenario analysis for the right end of the distribution, or the fat-tail and unexpected losses. Some firms develop a LDA model and then use scenario analysis to stress the model to produce a more appropriate distribution. Some firms add their scenario analysis data points into their loss data and develop their frequency and severity distributions from the combined data pool.

In a hybrid approach, the advantages and disadvantages of both approaches are present.

INSURANCE

Businesses will often argue that they are not exposed to operational risk in certain risk categories or scenarios because they carry insurance against just such risks arising. However, insurance payments can be slow and contentious and therefore Basel II does not allow for insurance to be used to reduce the gross amount of the loss, except under very narrow circumstances.

Under the AMA, a bank will be allowed to recognize the risk mitigating impact of insurance in the measures of operational risk used for regulatory minimum capital requirements, but only if specific, fairly onerous, criteria are met.

The recognition of insurance mitigation is limited to 20 percent of the total operational risk capital charge calculated under the AMA.

The qualifying criteria are as follows:

> *A bank's ability to take advantage of such risk mitigation will depend on compliance with the following criteria:*

The insurance provider has a minimum claims paying ability rating of A (or equivalent).

- *The insurance policy must have an initial term of no less than one year. For policies with a residual term of less than one year, the bank must make appropriate haircuts reflecting the declining residual term of the policy, up to a full 100% haircut for policies with a residual term of 90 days or less.*
- *The insurance policy has a minimum notice period for cancellation of 90 days.*
- *The insurance policy has no exclusions or limitations triggered by supervisory actions or, in the case of a failed bank, that preclude the bank, receiver or liquidator from recovering for damages suffered or expenses incurred by the bank, except in respect of events occurring after the initiation of receivership or liquidation proceedings in respect of the bank, provided that the insurance policy may exclude any fine, penalty, or punitive damages resulting from supervisory actions.*
- *The risk mitigation calculations must reflect the bank's insurance coverage in a manner that is transparent in its relationship to, and consistent with, the actual likelihood and impact of loss used in the bank's overall determination of its operational risk capital.*
- *The insurance is provided by a third-party entity. In the case of insurance through captives and affiliates, the exposure has to be laid off to an independent third-party entity, for example through re-insurance, that meets the eligibility criteria.*
- *The framework for recognizing insurance is well reasoned and documented.*
- *The bank discloses a description of its use of insurance for the purpose of mitigating operational risk.*

A bank's methodology for recognizing insurance under the AMA also needs to capture the following elements through appropriate discounts or haircuts in the amount of insurance recognition:

- *The residual term of a policy, where less than one year, as noted above;*
- *A policy's cancellation terms, where less than one year; and*
- *The uncertainty of payment as well as mismatches in coverage of insurance policies.*[22]

Operational risk capital may run into many billions of dollars and so it is certainly worth pursuing a 20 percent reduction in that amount and many

firms are exploring how best to take advantage of this opportunity. At the same time, many insurance companies are looking to produce insurance products that can meet the many criteria required. In the following disclosure examples, firms have outlined their approach to the use of insurance to lower their operational risk capital requirements.

DISCLOSURE

Basel II regulators around the world have accepted all types of these modeling approaches in AMA banks to date and the Basel Committee commented in their 2011 AMA Guidelines document on the wide range of practice that they had observed.

Pillar 3 of Basel II requires disclosure of capital calculation results and explanations of methodologies used.

> *Description of the AMA, if used by the bank, including a discussion of relevant internal and external factors considered in the bank's measurement approach.*[23]

No U.S. banks are under the Basel II requirements at the time of writing, but some choose to disclose this information now. Below are extracts from banks' annual reports describing their AMA methods and their operational risk capital amount.

Credit Suisse uses a scenario-based AMA methodology:

> ***Credit Suisse Annual Report 2011***
>
> *The economic capital/AMA methodology is based upon the identification of a number of key risk scenarios that describe the major operational risks that we face. Groups of senior staff review each scenario and discuss the likelihood of occurrence and the potential severity of loss. Internal and external loss data, along with certain business environment and internal control factors, such as self-assessment results and key risk indicators, are considered as part of this process.*
>
> *Based on the output from these meetings, we enter the scenario parameters into an operational risk model that generates a loss distribution from which the level of capital required to cover operational risk is determined. Insurance mitigation is included in the capital assessment where appropriate, by considering the level of insurance coverage for each scenario and incorporating haircuts as appropriate.*[24]

Operational risk increased following the update of scenario parameters to recognize higher litigation risks.[25]

Their Risk Weighted Assets for Operational Risk in CHF Millions was disclosed as 36,088.

In contrast, Deutsche Bank uses a loss data AMA methodology:

Deutsche Bank Annual Report 2011

The economic capital usage for operational risk increased by €1.2 billion, or 32%, to €4.8 billion as of December 31, 2011. The increase is primarily due to the implementation of a new safety margin applied in our AMA model, intended to cover unforeseen legal risks from the current financial crisis.[26]

Our internal AMA capital calculation is based upon the loss distribution approach. Gross losses adjusted for direct recoveries from historical internal and external loss data (Operational Riskdata eXchange Association (ORX) consortium data and external scenarios from a public database), plus internal scenario data are used to estimate the risk profile (that is, a loss frequency and a loss severity distribution). Thereafter, the frequency and severity distributions are combined in a Monte Carlo Simulation to generate losses over a one year time horizon. Finally, the risk mitigating benefits of insurance are applied to each loss generated in the Monte Carlo Simulation. Correlation and diversification benefits are applied to the net losses in a manner compatible with regulatory requirements to arrive at a net loss distribution at the Group level covering expected and unexpected losses. Capital is then allocated to each of the business divisions and both a qualitative adjustment ("QA") and an expected losses deduction are made.

JPMorgan Chase is not yet AMA approved, but chooses to disclose its methodology and operational risk capital amount. They use a hybrid AMA model that uses loss data and adds additional data from scenarios.

JPMorgan Annual Report 2011

Operational risk capital

Capital is allocated to the lines of business for operational risk using a risk-based capital allocation methodology which estimates operational risk on a bottom-up basis. The operational risk capital model is based on actual losses and potential scenario-based stress

losses, with adjustments to the capital calculation to reflect changes in the quality of the control environment or the use of risk-transfer products. The Firm believes its model is consistent with the Basel II Framework.[27]

Their economic capital for Operational Risk was $8.5 billion.

Whatever approach is taken to modeling capital for operational risk, the model must be stress tested and back tested for validity, and it is expected that models will continue to evolve as experience develops. The validity and verification requirements discussed in Chapter 8 must be applied to all modeling activities and a special model validation team is usually established in order to meet those needs.

FUTURE OF CAPITAL REQUIREMENTS

BIS's choice of values for alpha and beta in BIA and TSA were made with little supporting data, and the Basel Committee has recently been reviewing the assumptions that were made when those values were selected. This was always their intention and was clearly stated in Basel II.

The Committee intends to reconsider the calibration of the Basic Indicator and Standardized Approaches when more risk-sensitive data are available to carry out this recalibration. Any such recalibration would not be intended to affect significantly the overall calibration of the operational risk component of the Pillar 1 capital charge.[28]

This reconsideration occurred in 2011–2012, but there has been no formal report on the conclusions drawn. It is generally expected that the alpha and beta values have not stood up to testing now that data is available on business line operational risk losses.

In addition to questions being raised about the alpha and beta values of the BIA and TSA, there have been concerns raised about the range of practice found in the implementation of AMA calculations. In Basel II, the Basel Committee stated:

Supervisors will review the capital requirement produced by the operational risk approach used by a bank (whether Basic Indicator Approach, Standardized Approach or AMA) for general credibility, especially in relation to a firm's peers. In the event that credibility is lacking, appropriate supervisory action under Pillar 2 will be considered.[29]

Therefore, while the industry continues to refine their models, the rules may well change and it is possible that the Basel Committee will issue new operational risk capital requirements and guidance on permitted modeling methodologies at some point in the future.

KEY POINTS

- Basel II provides three main approaches to calculating operational risk capital: the basic approach, the standardized approach, and the advanced measurement approach.
- Firms that are required to, or choose to, calculate operational risk capital using AMA can select from several methods. They may base their calculations on loss distribution approach (LDA), on scenario analysis, or on a combination of the two.
- A model is generally built through the combination of a frequency distribution and a severity distribution using Monte Carlo simulation.
- A calculation must be done for each risk category.
- Capital must be allocated to the business lines appropriately.
- Correlation assumptions must be strongly defended.
- The use of insurance to mitigate capital is limited.
- The model must be validated.
- Capital amounts and the factors used must be disclosed under Pillar 3 of Basel II.

REVIEW QUESTION

1. Basel II provides three main approaches to calculating operational risk capital which are:
   I. The basic approach
   II. The standardized approach
   III. The advanced measurement approach
   IV. The loss distribution approach
      a. I, II, and III
      b. I, II, and IV
      c. II, III, and IV
      d. I, III, and IV

NOTES

1. Bank for International Settlements, "International Convergence of Capital Measurement and Capital Standards: A Revised Framework," 2004, sections 649–650.
2. Basel Committee on Banking Supervision, Risk Management Group, "Sound Practices for the Management and Supervision of Operational Risk," 2011. Retrieved from www.bis.org/publ/bcbs195.pdf.
3. See note 1, section 653.
4. Ibid., section 654.
5. Ibid.
6. Ibid., footnote 104.
7. Ibid., footnote 99.
8. Ibid., section 667.
9. Ibid., section 665.
10. Ibid., section 655.
11. Ibid., section 669(a).
12. Ibid., section 669(b).
13. Ibid., section 669(c).
14. Ibid., section 699(d).
15. Ibid., section 699(e).
16. Ibid., section 699(f).
17. Ibid., section 672.
18. "Operational Risk—Supervisory Guidelines for the Advanced Measurement Approaches," 2011. Retrieved from www.bis.org/publ/bcbs196.pdf, section 180.
19. A leptokurtic distribution is more concentrated around the mean than would be observed in a normal curve.
20. See note 19, sections 195–196.
21. See note 1, section 670(d).
22. Ibid., sections 678–679.
23. Ibid., p. 241, Table 12.
24. Credit Suisse Annual Report 2011, p. 134.
25. Ibid., p. 99.
26. Deutsche Bank Financial Report 2011, p. 43.
27. JPMorgan Annual Report 2011, p. 123.
28. See note 1, footnote 103.
29. See note 1, footnote 98.

CHAPTER 13

Reporting

In this chapter, we investigate reporting tools that empower the operational risk function with the opportunity to contribute to the business decision making at the firm. We consider loss data reporting in some depth and also discuss reporting on the other elements in the framework including risk and control self-assessment, key risk indicators, and scenario analysis. Examples of fictional data will be used to demonstrate how risk analysis can be applied to raw data in order to provide relevant reporting conclusions that can drive business decision making.

ROLE OF REPORTING

An operational risk framework is designed to identify, assess, monitor, control, and mitigate operational risk. All of the elements of the framework contribute to these goals, but without effective reporting even the best of programs will be ineffective in changing the risk culture of the firm. The place of reporting in the operational risk framework is illustrated in Figure 13.1.

The reporting of operational risk is key to the program's success. There are many ways to ensure that the reporting of each element drives action, and to protect against the danger of producing reporting that receives a "so what?" response.

Generally, an operational risk department will be looking to report on several things, including:

- Loss data for the last period
- Remediation action being taken
- KRIs
- Results of RCSA

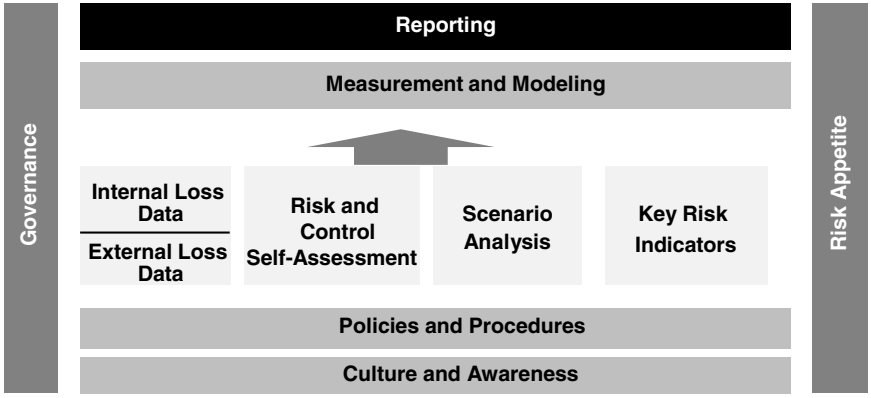

FIGURE 13.1 The Role of Reporting in the Operational Risk Framework

- Results of scenario analysis
- Capital calculation
- Whether the operational risk department is on track with its deliverables

However, the chief risk officer (CRO), risk committee, or other executive management may have different expectations, and they are more likely to be looking for reporting that addresses:

- Where is our risk?
- What action do we need to take?
- Who is under control?
- Who is not?
- Are we meeting our regulatory requirements?

Effective reporting is presented in a way that demonstrates the risks analyst role of the operational risk department. Just as market and credit risk specialists are focused on risk analysis, so too should operational risk specialists be risk analysts. Market risk and credit analysts:

- Analyze raw data
- Analyze trends and predictors
- Follow news articles
- Present opinions
- Present capital at risk (value at risk [VaR], and stressed VaR)
- Recommend action and hedging strategies

In the same way, operational risk managers should take on the same responsibilities for operational risk and should not be just data gatherers but should also:

- Analyze raw data
- Analyze trends and predictors (KRIs)
- Follow news articles
- Present opinions
- Present capital at risk
- Recommend action and mitigating strategies

LOSS DATA REPORTING

Loss data reporting is often the central reporting activity in an operational risk function. Loss data can be a mine of vital information that can contribute to effective operational risk management and measurement. However, it can also be dead data if it is not properly presented in a way that can drive decision making.

Internal loss data reporting typically looks something like the fictional example seen in Table 13.1.

While these data are somewhat self-explanatory, the method of collection and underlying assumptions might lead to a misinterpretation of the data. Therefore, it is important to ensure that the recipients of the event data reporting understand the background.

Impact of Gains on Internal Event Reporting

For example, in Table 13.1 the data may actually contain gains as well as losses. It may be an operational risk *event* report, rather than a *losses* report. Table 13.1 shows that there were eight events in Investment Banking in December 2012 and that the net value of events was $10,000. However, there is no more detail provided on the nature of those eight events, and there may be significant information that is being masked from view.

An example of the underlying data for investment banking is seen in Table 13.2.

From the underlying data it is clear that one of the events was a gain of $12,500, and this gain is skewing the net events so that they total $10,000, when in fact operational risk losses totaled $22,500 if gains are excluded. The amount at risk might actually be $35,000—the absolute value of the events, as it was probably only luck that the seventh event was a gain instead of a loss.

TABLE 13.1 Example Operational Risk Event Data Table

	Dec 2012						12-Month Total		
Business Line	Absolute $ Value of Events	# Events	Gross $ Value of Events	$ Recovery	Net $ Value of Events	Trend	# Events	Gross $ Value of Events	Net $ Value of Events
Fixed income	150,000	10	(65,000)	5,000	(60,000)	⟷	185	(650,000)	(350,000)
Investment banking	35,000	8	(10,000)		(10,000)	⟷	65	(435,000)	(400,000)
Equities	250,000	65	(208,000)	55,000	(153,000)	↑	450	(8,500,000)	(2,500,000)
Asset management	120,000	28	(120,000)	25,000	(95,000)	⟷	235	(11,350,000)	(5,500,000)
Private wealth management	70,000	35	(70,000)		(70,000)	↓	625	(12,560,000)	(2,000,000)
Total	**625,000**	**146**	**(473,000)**	**85,000**	**(388,000)**		**1,560**	**(33,495,000)**	**(10,750,000)**

TABLE 13.2 Example Investment Banking Operational Risk Event Detail

Investment Banking Events in $, December 2012					
	Absolute	Gross	Recovery	Net	Total Net Loss
Event 1	2,000	(2,000)	0	(2,000)	(2,000)
Event 2	2,000	(2,000)	0	(2,000)	(2,000)
Event 3	4,000	(4,000)	0	(4,000)	(4,000)
Event 4	2,000	(2,000)	0	(2,000)	(2,000)
Event 5	5,000	(5,000)	0	(5,000)	(5,000)
Event 6	2,000	(2,000)	0	(2,000)	(2,000)
Event 7	12,500	12,500	0	12,500	0
Event 8	5,500	(5,500)	0	(5,500)	(5,500)
Total	**35,000**	**(10,000)**	**0**	**(10,000)**	**(22,500)**

Therefore, it is important to ensure that the recipients of a report such as Table 13.1 are aware if gains are being netted against losses. Perhaps this nuance would be lost on the audience. If so, absolute dollar value of the events might be a better indicator of operational risk and the report might be changed to reflect that.

Trends in Internal Losses

The fictional operational risk data Table 13.1 includes a trend column. This trend needs more explanation in order to be informative. The presenter of the report will need to clarify whether the trend relates to month on month changes, changes relative to the average over the past year, or some other benchmark. The trend also could relate to any of the previous columns, and so clarification is needed as to whether it relates to the number of events or to the dollar amount of the absolute, gross, or net amount.

Trends can be helpful as they can indicate a changing risk environment that may require action. Trends of loss size against number of events might provide insight into improving or worsening control environments. An example of a use of trends to compare events and net losses is provided in Figure 13.2.

It can also be helpful to compare trends in business lines and in risk categories to see where the risks are elevated. This information is

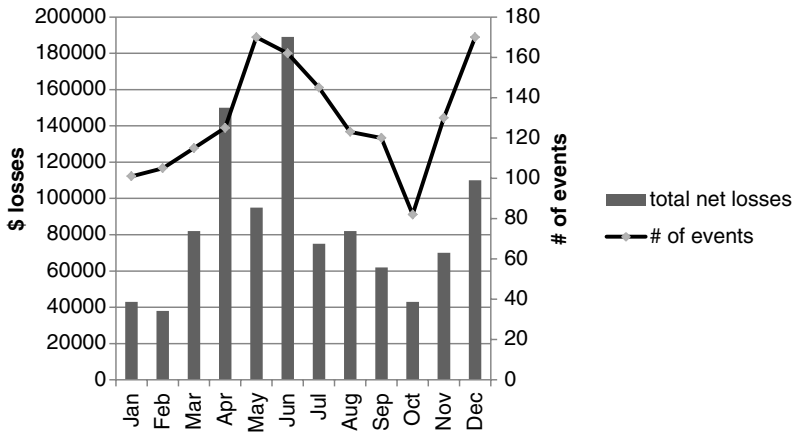

FIGURE 13.2 Trending Loss Amount vs. Number of Events

particularly helpful when considering entering into a new business. Trends and history from similar business lines can be used to help with the assessment of the likely operational risk exposures that may arise in this new business line.

Risk Analysis of Table 13.1

There may be a story behind the raw numbers which is not apparent without explanation and analysis from the operational risk department. Looking again at fictional operational risk event Table 13.1, it is clear that there is a large difference between the total gross amount of losses ($33,495,000) and the total net amount ($10,750,000) of losses for the past 12 months.

This difference begs for analysis and explanation and suggests that this firm is very good at recovering amounts lost in operational risk events. Recoveries are usually achieved through expert employees who intervene and recover some, or all, of the initial loss amount. Recoveries are more often driven by people than by automated systems, suggesting that the excellent recovery rate reflected in this data is dependent on experienced personnel.

This analysis takes on significance if the firm is currently downsizing. An operational risk manager could use this loss data to alert senior management that they might experience an increase in net losses due to weaker recovery rates as a result of the current downsizing strategy of the firm.

The recovery rate might also be used to drive a discussion about what efforts could be made to further improve the recovery rates, and what the cost benefit might be of such initiatives.

This type of analysis, linking operational risk data to the business activities and strategies of the firm, demonstrates the relevance and importance of the operational risk function, and properly provides increased transparency into operational risk exposures.

Internal Losses by Risk Category

The same operational risk event data can also be presented by risk category rather than by business line as follows. The fictional data in Table 13.1 provides a view into how each business is doing compared to the other business lines. There may be opportunities for more analysis if the data are cut differently, by risk category, as in Table 13.3.

Risk Analysis of Table 13.3 Several stories can be told from this cut of the data. It is clear that most of the events occur in the Execution, Delivery, and Process Management category as it has experienced 1,100 events over the past 12 months—significantly higher than any other category.

However, the highest loss amounts occur in the Clients, Products, and Business Practices category, which has the lion's share of the dollar value of the losses at $18.5 million over the past year. This suggests that the latter are more prone to fat-tail events.

The firm will want to confirm whether this pattern of losses is to be expected, and it can be helpful to compare risk category data to external benchmarks. This can be compared to benchmarks from sources such as the IBM Algo FIRST database and the ORX consortium data discussed in Chapter 8.

Further analysis of these data shows that this firm has a good experience with recoveries from fraud events. They have experienced 32 internal events and two external events, but the net losses are small compared to the gross losses, indicating that there have been successful recoveries in these cases.

Timeliness

A report that tracks the timeliness of reporting of internal loss data events can be a powerful tool in driving culture change within a firm. Transparent reporting of loss reporting behavior can be very effective in inspiring better behavior and can drive reporting times down.

TABLE 13.3 Example Operational Risk Event Data Cut by Risk Category

	Dec 2012						12-Month Total		
Risk Category	Absolute $ Value of Events	# Events	Gross $ Value of Events	$ Recovery	Net $ Value of Events	Trend	# Events	Gross $ Value of Events	Net $ Value of Events
Business Disruption and System Failure	5,000	8	(5,000)	$5,000	0	⟷	45	(650,000)	(150,000)
Clients, Products, and Business Practices	265,000	28	(158,000)	0	(158,000)	⟷	88	(18,500,000)	(7,450,000)
Execution, Delivery, and Process Management	190,000	97	(145,000)	80,000	(65,000)	↑	1,100	(6,540,000)	(2,400,000)
Damage to Physical Assets	20,000	10	(20,000)	0	(20,000)	⟷	235	(1,200,000)	(200,000)
Employment Practices and Workplace Safety	120,000	2	(120,000)	0	(120,000)	↓	56	(3,450,000)	(500,000)
Internal Fraud	25,000	1	(25,000)	0	(25,000)	⟷	32	(2,655,000)	(50,000)
External Fraud	0	0	0	0	0	⟷	4	(500,000)	0
Total	**625,000**	**146**	**(473,000)**	**85,000**	**(388,000)**		**1,560**	**(33,495,000)**	**(10,750,000)**

If loss data is being reported late, it not only exposes the firm to unmitigated risks, but it may also impact the capital calculation if the firms has an AMA approach that uses loss data as a direct input into the model.

Timeliness can be tracked in several ways:

- Time from occurrence to identification
- Time from identification to entry in the loss database
- Time from entry to sign off

It should be noted that legal losses often have a long time lag between occurrence and identification, and this needs to be handled thoughtfully when tracking timeliness of loss data. Any combination of the above criteria can be used to drive better reporting behavior. Timeliness can often be adversely impacted due the slow response of another department, and this can also be reflected in reporting statistics. For example, the front office areas might complain that the finance department is very slow to complete their portion of the data when accounting issues are involved. By tracking the timeliness of all events that have finance as an impacted department, this can be made transparent and encourage more efficiencies in the finance area.

External Loss Data Reporting

Operational risk reporting often includes a summary and analysis of relevant external events over the past reporting period. These should be reviewed for relevance and lessons learned. It is always more popular to discuss bad things that have happened to competitors than it is to talk about bad things that have happened at the firm. However, significant external events offer an opportunity to consider "could it happen here?"

Senior management are often very engaged in such discussions, and they can lead to proactive operational risk mitigation activities that can be led by the operational risk function or kicked off and tracked by that function.

Any emerging trends, such as an increase in regulatory fines in a particular area, should be compared to the firm's internal experience and current risk and control environment.

For example, if external data indicate that there has been an increase in the levying of regulatory fines for breaches in the Foreign Corrupt Practices Act (FCPA), then the operational risk manager might propose a review of the firms current FCPA training and awareness to ensure that these controls are functioning at peak levels of effectiveness.

If the firm is a member of a consortium of loss data, then the internal loss results should be compared to the benchmarking results that the consortium makes available. Comparisons between external and internal

data should always be treated with caution, as there may be significant differences in the business models, products and control environments which could lead to incorrect conclusions.

However, as discussed above, external data can provide helpful awareness of risks that may not yet have occurred at the firm, but which should be seriously addressed.

RISK AND CONTROL SELF-ASSESSMENT REPORTING

The output from RCSAs is generally reported in detail to the participating department, and in summary or thematic form to senior management. While the full RCSA output demonstrates that analysis and recommendations are based on strong underlying data, the details themselves are rarely of interest to the risk committee or CRO.

Instead, the operational risk department can analyze the RCSA output and identify areas that require escalation and raise themes that are best addressed on a firm-wide basis.

For example, if multiple departments have identified through RCSAs that their employee training is weak, then a firm-wide training and development initiative might be a more appropriate response than many individual training programs.

The operational risk department might also have noticed underlying themes during their facilitation of the RCSA exercise, such as a lack of awareness of appropriate fraud controls. This might give rise to a firm-wide initiative to raise awareness of appropriate fraud risk mitigation activities.

RCSA thematic data might also be enhanced by regular monitoring of triggers that have been identified as requiring a reassessment of all or part of an RCSA. A large internal or external event might result in a recommendation by the operational risk department that the firm, or one division of the firm, revalidate the risk and control scores for that particular risk. For example, a sudden increase in fines for FCPA breaches might result in the next operational risk report to senior management including a request to reassess all corruption and bribery risks in the firm.

KEY RISK INDICATOR REPORTING

KRIs are particularly well suited to dashboard-type reporting. There are many tools available to present data to management in a way that highlights red flags and allows for drill-down capabilities to review the underlying sources of data.

However, complex and comprehensive KRI reports are often provided to senior management without sufficient analysis and explanation, leaving the audience with the "so what?" question. For this reason, an operational risk department might decide to review all KRI reports with the departments that own the data, and only provide a summary to senior management. Exception reporting of red flags that require escalation might be more valuable than a comprehensive KRI report that shows all KRIs for the firm.

KRI reports are often designed to indicate with color whether there is a concern, with different thresholds for red, yellow, or green.

The dangers with KRI reporting are that a sea of green might give a false sense of security and a sea of red might produce panic, when the underlying KRIs and thresholds have not yet been proven to be indicative of raised or lowered risk.

Careful explanation and analysis must therefore accompany any KRI dashboard reporting that is provided to senior management.

SCENARIO ANALYSIS REPORTING

The results of the scenario analysis program may drive changes to any advanced measurement approach to calculating operational risk capital calculations. They may also produce important mitigating actions that require escalation to senior management.

While the details of the output of scenario analysis are unlikely to be of interest to senior management, the implications of those results and their impact on capital will certainly be of interest. In the same way, any proposed mitigating actions may need to be presented to senior management for approval and funding. Scenario analysis results can also give an organization's senior management a good indication of the firm's "top risks" and help the firm manage against them.

The scenario detail will be of importance to any department that is impacted by the results and should be included in their department-level reporting. The form of scenario analysis reporting will depend on the type of program that is in place.

CAPITAL REPORTING

Operational risk capital will need to be reported to senior management and the Board. They are likely to be very interested in the drivers of capital, and if an AMA model is in place, any reporting of capital will need to be accompanied by a simple, but complete, explanation of the model and

its drivers. As operational risk capital is a direct and sometimes significant driver of risk-weighted assets (RWAs), senior management would benefit from understanding how operational risk capital drives RWAs. Also, firms can do informative peer analysis of operational risk capital by leveraging public information (e.g., Bloomberg) or data provided from a consortium like ORX to create useful peer comparison. Key metrics to compare across the industry can include:

- Op Risk RWA as a percentage of total RWA
- Op Risk RWA as a percentage of Total Revenue

Finally, but importantly, looking at operational risk RWA by business unit can help drive business decisions. If a BIA or TSA approach is being taken to capital calculation then it may be prudent to include a reminder of the method being used also.

ACTION TRACKING REPORTING

There are usually many action items generated by an operational risk management framework. Actions arise from loss events that require actions to ensure a recovery of the lost amount, or to prevent a repeat of the same event. Actions arise during an RCSA as control improvements are identified and mitigating actions are agreed upon. Actions arise during scenario analysis as fat-tail events are discussed and firm-wide mitigating actions proposed.

In addition to all of the action items that arise in the operational risk framework, there are usually other action items that are operational risk related, but that are owned by other areas of the firm. For example, the Sarbanes-Oxley team and the audit department will be tracking their own set of action items, most of which are in fact operational risk related.

Some firms integrate all action tracking into one tool and one business process, and this is discussed further under "Governance, Risk, and Compliance" in Chapter 16. However, most firms do not yet have an integrated action tracking process. This does not prevent the operational risk department from adding value to the organization by bringing the reporting of those action items into one report, so that management can have a clearer view of the operational risk of the firm.

For example, an integrated report could look like something like the example in Table 13.4.

An integrated action table is helpful in assessing which business lines or support areas are managing their risks effectively. The example in Table 13.4 shows

TABLE 13.4 Example of Integrated Action Tracking Reporting

	Operational Risk			Internal Audit		SOX	Total
Business Unit	**Completed**	**Open**	**Past Due**	**Open**	**> 90 Days Past Due**	**Open**	**Open Action Items**
Finance	25	5	2	6	3	8	19
Human Resources	20	2	2	3	0	0	5
Legal	10	0	0	2	2	0	2
Operations	45	5	4	8	3	1	14
Technology	28	8	2	7	1	5	20
Fixed Income	10	2	0	5	1	2	9
Investment Banking	8	1	1	8	1	0	9
Equities	5	1	1	12	2	5	18
Asset Management	14	2	1	12	7	0	14
Private Wealth Management	13	5	5	2	2	1	8
Total	**178**	**31**	**18**	**65**	**22**	**22**	**118**

the output at a firm where there are different action tracking methods in operational risk, in audit and in Sarbanes-Oxley (SOX). Operational risk is tracking all completed open and past due items, audit only tracks past due items once they are more than ninety days late and SOX only tracks whether items are open.

Ideally, all groups will eventually align to one action tracking method, but even while there are different approaches, reporting can still occur and can still be helpful. All departments have action items to track, both support areas and front office business lines. This is unlike loss data reporting, where Table 13.1 showed only the front office business lines, as they own the loss. In loss data reporting, some firms do also track events by cause, and so may have results for support areas also.

Risk Analysis of Table 13.4

As a raw table of data, this report does leave the observer wondering "so what?" Where is there an area of concern or a need for escalation? Further

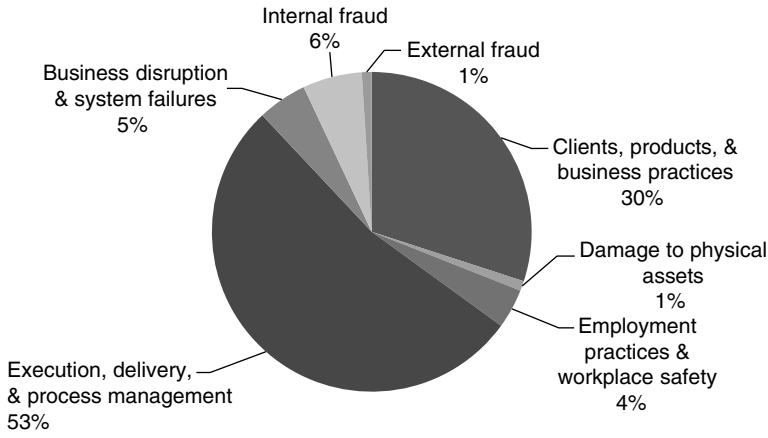

FIGURE 13.3 Fictional Action Open Items by Risk Category, Pie Chart

analysis is helpful to present the information in a way that supports business decision making.

Table 13.4 suggests that the finance, technology, and equities departments need to move more urgently to address the outstanding action items in their areas as they have the highest number of open action items.

If the operational risk department has been successful in partnering with the Sarbanes-Oxley and audit departments to such a degree that all three are categorizing their action items by the same risk categories, then it is also possible to produce a risk category cut of the same data.

Such a cut might produce data that could populate a pie chart such as the one shown in Figure 13.3.

From this view we can see that the majority of open action items in this fictional set are in the Execution, Delivery, and Process Management category. However, perhaps the late action items tell a different and more compelling story, as shown in Figure 13.4.

From this view it is clear that the real concern should be around the resolution of the many late Clients, Products, and Business Practices items, as these relate to a risk category that is prone to fat-tail events.

This demonstrates how analysis and explanation by the operational risk department can lead to decision points for senior management. This chart would best be presented along with a request to follow up on all late Clients, Products, and Business Practices action items in the firm, to ensure they are reprioritized as high priority and addressed as soon as possible.

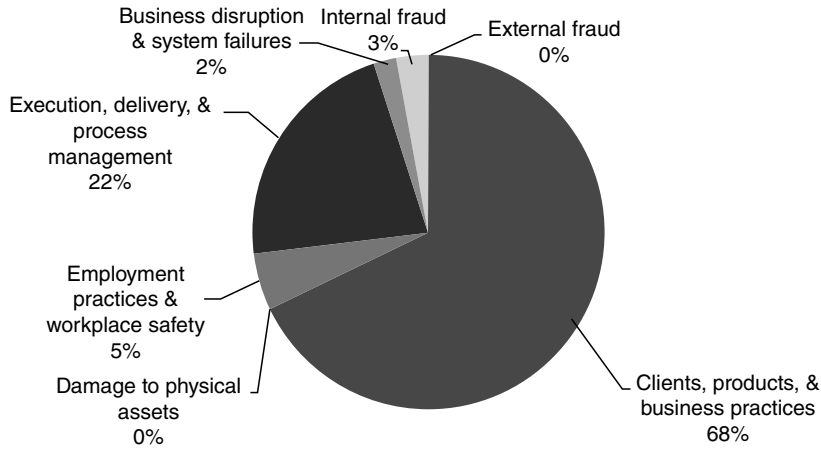

FIGURE 13.4 Fictional Late Action Items by Risk Category, Pie Chart

A CONSOLIDATED VIEW

All of this operational risk data can be brought together into one view, to provide a snapshot of the current overall risk profile for each department. Just one example of how this might be done is shown in Table 13.5. If this report is for the CRO, risk committee, or board, then the overall risk rating should be the *independent view* of the corporate operational risk function, acting in its role as second line of defense.

DASHBOARDS

Some firms bring together all of their reporting into one view, so that the total risk exposure for each department can be clearly seen and compared. There are many sophisticated software solutions for this type of reporting. Some have drill-down capabilities so that an area of interest can be clicked on in order to see the underlying data.

KEY POINTS

- Strong, analytical reporting is fundamental to a successful operational risk framework and provides the opportunity to drive business decision making.

TABLE 13.5 Consolidated View of Operational Risk Outputs to Produce a Risk Profile

Dec 2012 Risk Profile	New Losses $m		RCSA Score							Highest Scenario $m	Late Action Items	Overall Risk Rating
Business Unit	**Owned**	**Caused**	**CPBP**	**EDPM**	**IF**	**EF**	**EPWS**	**DPA**	**BDSF**			
Finance		2.1	H	M	M	M	L	L	L	—	20	M
Human Resources		0.4	L	M	L	L	H	L	L	—	5	M
Legal		1.2	L	L	L	L	L	L	L	—	0	L
Operations		2.1	H	H	M	M	L	L	L	—	16	H
Technology		5.0	L	M	L	H	L	L	L	—	55	H
Fixed Income	11.0	2.0	M	M	M	M	M	L	L	2,000	12	M
Investment Banking	2.5	1.0	L	L	L	L	L	L	L	500	4	L
Equities	2.5	1.0	H	M	L	L	L	L	L	2,500	6	M
Asset Management	0.6	2.0	L	M	L	L	L	L	L	650	18	L
Private Wealth Management	1.2	1.0	L	L	L	L	L	L	L	100	42	L

- Reporting will usually include analysis of internal loss data, external loss data, risk and control self-assessment results, scenario analysis results, and capital.
- Action tracking across the firm can be consolidated under the operational risk framework.
- A risk profile can be subjectively determined from the underlying data.
- Dashboards are readily available today and provide drill-down capabilities for interactive reporting.

REVIEW QUESTION

1. Which of the following is most likely to generate informed business decisions based on operational risk considerations?
   a. A table showing raw operational risk losses data
   b. A table containing the total capital required using the basic indicator approach
   c. A list of themes raised through the RCSA process with proposed mitigating actions
   d. A list of the latest scenario analysis maximum loss estimates

CHAPTER 14

Risk Appetite

In this chapter, we explore the most challenging element of the operational risk framework: risk appetite. The risk appetite element of the framework is the glue that holds the framework together, as it provides context for the risks that are identified and assessed and ensures appropriate escalation and governance of operational risk.

However, there is little guidance on operational risk appetite in the original Basel II documents and firms have struggled with this element in the past few years. Regulators have recently provided further guidance that makes it clear that the board of directors, senior management, and the businesses all have roles to play in setting and managing operational risk appetite. This guidance has proven helpful and firms are now making real progress in addressing this element of the framework, albeit with a wide range of practices.

THE ROLE OF RISK APPETITE

Operational risk management, measurement and capital modeling produce data, scores, and capital numbers that are designed to be used by the firm to identify, assess, monitor, control, and mitigate operational risk. All of these activities rely on an underlying understanding of the risk appetite of the firm.

Assessment of risk assumes that there is a gauge against which that assessment is measured. However, finding and expressing an operational risk appetite can prove to be very challenging. Unlike other risk categories, operational risk is inherent in the very existence of the firm. As such, a risk appetite of zero operational risk is untenable. What then is the appropriate level of operational risk?

Risk appetite usually matures as the operational risk program develops. Once internal loss event data is gathered, then management is able to

determine whether they consider this level of losses to be acceptable or not. As RCSA data is gathered, the participants express whether they feel the risks to be high and in need of mitigation, or whether they are at acceptable levels.

As scenario analysis workshops are conducted, participants engage in discussion around the worst possible cases and determine whether there may be mitigating actions required. As KRIs are designed and gathered, thresholds are determined and refined to reflect the risk levels that are considered acceptable.

So the operational risk framework itself supports the evolution of the operational risk appetite of the firm. Thresholds and scores will be adjusted as that appetite is refined or changes.

For that reason, most firms did not attempt to articulate their operational risk appetite until the operational program had had a few years to evolve and mature. The risk appetite is a critical pillar that holds the whole operational risk framework together, as is illustrated in Figure 14.1.

Before examining the rules and approaches that apply to operational risk appetite, it is necessary to establish terminology. Many firms use different terms in this space, referring to risk capacity, risk appetite, risk tolerance, and risk thresholds—often interchangeably and confusingly.

It may help to consider this area of the framework in all four ways, and for the purposes of this chapter we will take the following approach. Risk capacity is the ability of the firm to absorb risk, and is often related to the capital that it holds. Risk appetite is the firm's view on what risks it is willing or unwilling to take. Risk tolerance reflects specific levels of risk that

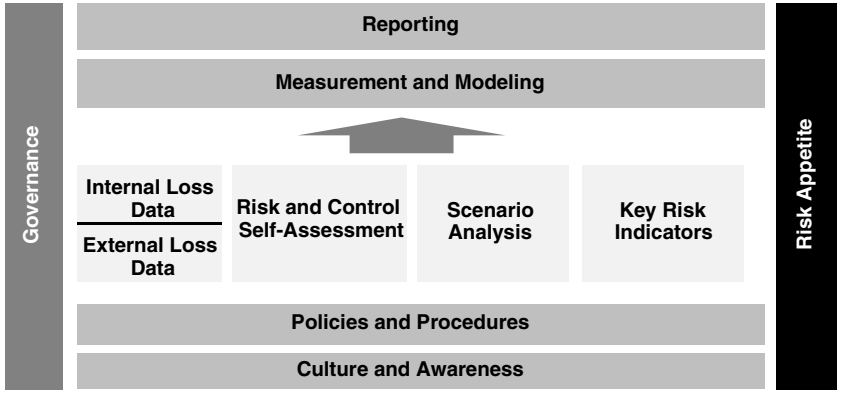

FIGURE 14.1 The Role of Risk Appetite in the Operational Risk Framework

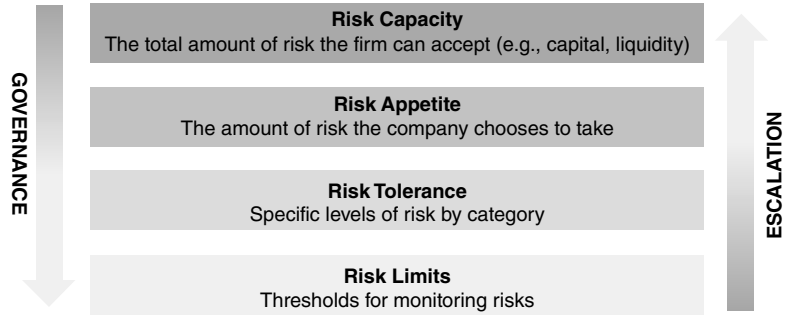

FIGURE 14.2 The Relationship between Risk Capacity, Appetite, Tolerance, and Limits

will be permitted without the need for mitigation. Risk limits are thresholds that are used to monitor measures of risk. The relationship between these is illustrated in Figure 14.2.

In Figure 14.2 it can be seen that the governance flows down from capacity, through appetite and tolerance to limits. It is also clear that the escalation of risk flows upwards from limits up to risk capacity. These flows impact the roles and responsibilities of the board, senior management, and the business lines and limit owners.

REGULATORY EXPECTATIONS

The regulators have evolved their thinking on risk appetite, not just in operational risk, but as an important element in corporate governance. Basel II only mentions the word *appetite* once, in the Pillar 2 section of the rules:

> *The [operational risk] framework should cover the bank's appetite and tolerance for operational risk, as specified through the policies for managing this risk.*[1]

In its 2003 "Sound Practices for the Management and Supervision of Operational Risk" document, the Basel Committee on Banking Supervision (BCBS) did not add much color. They referred to appetite in their principles:

> *Principle 6: Banks should have policies, processes and procedures to control and/or mitigate material operational risks. Banks should periodically review their risk limitation and control strategies and*

should adjust their operational risk profile accordingly using appropriate strategies, in light of their overall risk appetite and profile.[2] *[emphasis added]*

They talked about how the risk appetite should be used in remuneration considerations:

Senior management should also ensure that the bank's remuneration policies are consistent with its appetite for risk.[3]

And they referred to it as a consideration when deciding whether to accept risk or self-insure against certain risks:

In some instances, banks may decide to either retain a certain level of operational risk or self-insure against that risk. Where this is the case and the risk is material, the decision to retain or self-insure the risk should be transparent within the organization and should be consistent with the bank's overall business strategy and appetite for risk.[4] *[emphasis added]*

But there was no Basel guidance provided as to how operational risk appetite could or should be articulated, and initially little pressure from the regulators for banks to get any clear risk appetite statements in place.

However, there was a fundamental change in emphasis in this area when BCBS updated the 2003 "Sound Practices" guidance with the "Principles for the Sound Management of Operational Risk and the Role of Supervision" document in 2011. Instead of 5 mentions of *appetite,* there were now 19, and the bar had been significantly raised.

Perhaps most importantly, under the 2011 guidance the board of directors is now expected to approve and review the operational risk statement, and we have more clues as to what that statement should include:

Principle 4: The board of directors should approve and review a risk appetite and tolerance statement for operational risk that articulates the nature, types, and levels of operational risk that the bank is willing to assume.[5]

The footnote provides additional guidance as to the meaning of *risk appetite* and *risk tolerance* as follows:

"Risk appetite" is a high level determination of how much risk a firm is willing to accept taking into account the risk/return

> *attributes; it is often taken as a forward looking view of risk acceptance. "Risk tolerance" is a more specific determination of the level of variation a bank is willing to accept around business objectives that is often considered to be the amount of risk a bank is prepared to accept. In this document the terms are used synonymously.*[6]

In other words, they do not clearly distinguish between *appetite* and *tolerance,* but they do start to define the concepts for us as *a forward-looking view of risk acceptance*.

The updated "Sound Practices" still require senior management to ensure that the operational risk framework is consistent with the risk appetite of the firm[7] and charges audit to "review the robustness of the process of how [risk appetite and tolerance] limits are set and why and how they are adjusted in response to changing circumstances."[8]

The "Sound Practices" document of 2011 also requires a clear articulation of risk appetite, stating that the framework documents must:

> *… describe the bank's accepted operational risk appetite and tolerance, as well as thresholds or limits for inherent and residual risk, and approved risk mitigation strategies and instruments . . .*[9]

Documenting this description has been a challenge for banks, as they must attempt to articulate a risk appetite for errors occurring due to inadequate or failed processes, people, systems, or external events. The simple answer is, of course, we don't want any mess-ups. But a bank cannot have a risk appetite of zero, as this is not tenable.

Neither the U.S. regulators' AMA guidance nor the Committee of European Banking Supervisors guidelines on operational risk offered any further assistance with these challenges, making little or no mention of risk appetite. The only additional guidance that has been offered out of the Bank of International Settlements is a footnote in their "2012 Core Principles for Effective Banking Supervision":

> *"Risk appetite" reflects the level of aggregate risk that the bank's Board is willing to assume and manage in the pursuit of the bank's business objectives. Risk appetite may include both quantitative and qualitative elements, as appropriate, and encompass a range of measures.*[10]

As a result, a fairly complex, and at times inconsistent, nomenclature has arisen in this element of the framework.

RANGE OF PRACTICE IN RISK APPETITE AND TOLERANCE METHODS

In 2007 the United Kingdom's Financial Services Authority conducted a study[11] into the range of practices being used to define and use operational risk appetite and tolerance within the operational risk frameworks of banks. They identified a very wide range of practices and simply summarized their findings to show the many ways that these terms were being used and thresholds being set.

Figure 14.3 is a reproduction of the diagram that the study used to demonstrate the many ways that risk appetite and tolerance could be managed. In their paper, they refer to operational risk appetite as ORA and note that qualitative and quantitative approaches are being developed across the industry.

This broad range of practices was noted, but not particularly criticized, and many firms continued to take a slow-paced approach to the development of this element of their operational risk framework.

Risk Appetite Pressure Post 2008

However, in 2009, the Senior Supervisors Group (SSG), which includes the major national banking regulators from Europe and the United States, issued a report, "Risk Management Lessons from the Global Banking Crisis of 2008"[12] (the "2009 SSG report"). This report, in their own words "reviewed in depth the funding and liquidity issues central to the crisis and explored critical risk management practices warranting improvement across the financial services industry."[13] Two of the key findings of weakness were

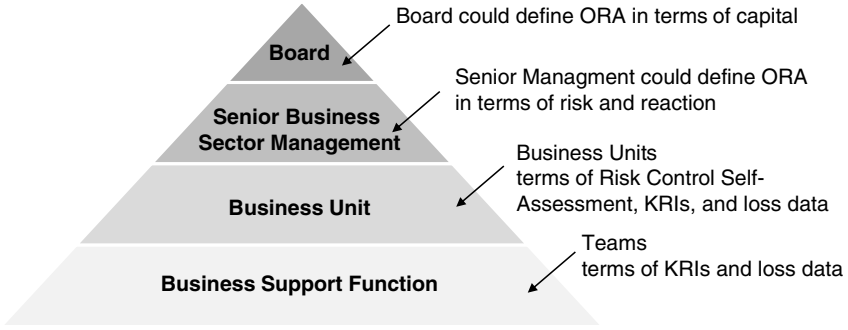

FIGURE 14.3 FSA Findings on How ORA Can Be Defined or Articulated at Several Levels Using Varying Metrics

(1) the lack of robust risk appetite frameworks and (2) weaknesses in information technology (IT) infrastructure and data.

To further address these two items, in 2010 SSG issued "Observations on Development in Risk Appetite Frameworks and IT Infrastructure."[14] Therefore, while Basel remains silent on more guidance on risk appetite, the regulators have now offered their views on their expectations around risk appetite frameworks.

We will therefore adopt the SSG's approach to risk appetite when considering how to implement an effective risk appetite framework. This approach applies to all aspects of the risk framework, not just the operational risk framework.

IMPLEMENTING A RISK APPETITE FRAMEWORK

SSG considered both risk appetite and IT infrastructure in their 2010 report, but for this analysis we will look at just the risk appetite findings and recommendations. It is important to note, however, that a robust and effective IT infrastructure (which produces reliable data) was also considered a critical factor for successful risk management in the future.

The SSG had three key findings regarding risk appetite in 2010:

1. Many firms had made progress in conceptualizing, articulating, and implementing a risk appetite framework (RAF).
2. An effective RAF greatly improves a firm's strategic planning and tactical decision making.
3. Strong and active engagement by a firm's board of directors and senior management plays a central role in ensuring that a RAF has a meaningful impact on the organization.

They also observed three important characteristics that led to a more effective implementation of a risk appetite framework:

1. Strong internal **relationships** at the firm.
2. The board of directors ensures that senior management establishes strong **accountability** for the risk appetite, with clear incentives and constraints for business lines.
3. A common risk appetite **language** is in use across the firm, expressed through qualitative statements and appropriately selected risk metrics.

SSG provided further guidance on implementing a risk appetite framework under the following categories, and we will consider each in turn.

- Background and Approach
- The Risk Appetite Framework as a Strategic Decision-Making Tool
- Risk Appetite Governance: The Board, "C-Suite," and Business Lines
- Promoting a Firmwide Risk Appetite Framework
- Monitoring the Firm's Risk Profile within the Risk Appetite Framework.

Background and Approach

Fourteen firms were studied by the SSG, and none were found to have a risk appetite framework that reflected all of the best practices that they expected to see. In addition, many firms admitted that they had only had a risk appetite framework in place for less than a year. Many were moving forward not as a result of the requirements that they faced under Basel II, but due to requirements that had been published by BCBS in its 2010 "Principles for Enhancing Corporate Governance," which required the board to "approve and oversee the implementation of the bank's overall risk strategy, including its risk tolerance/appetite."[15]

At the time of writing, most firms are actively pursuing improving and refining their risk appetite statements, but they are still adopting a wide range of practices in how they approach their risk appetite framework.

The Risk Appetite Framework as a Strategic Decision-Making Tool

Having a risk appetite framework in place allows for business decisions to be considered in the context of risks being taken relative to the board or senior management's appetite for risk.

For example, a decision to expand a business line should include considerations of how the risk profile may change with that expansion. If that change is well understood and meets with the approval of the senior management, then the expansion will proceed. In contrast, if the risks in an existing business are either beyond the appetite of the firm or are not well understood, then the risk appetite framework can facilitate exiting that business for risk reasons.

Risk appetite discussions often lead to important related discussions on the strategic direction of the firm and its core competencies. Firms have often taken a step back and spent time rearticulating their strategy and business goals before moving forward with linking these to their risk appetites.

Putting a written risk appetite statement down on paper is challenging and usually results in a very high-level statement that expresses the strategic priorities of the firm. SSG refers to the Basel Corporate Governance definition of risk appetite as it tries to provide additional guidance to banks on this:

> *Risk appetite is the level and type of risk a firm is able and willing to assume in its exposures and business activities, given its business objectives and obligations to stakeholders. Risk appetite is generally expressed through both quantitative and qualitative means and should consider extreme conditions, events, and outcomes. In addition, risk appetite should reflect potential impact on earnings, capital, and funding/liquidity.*[16]

A clear risk appetite should be resilient enough to prevent business lines from drifting away from the core strategy of the firm and to assist the firm in staying within its own strategic plans. However, it should also be able to evolve to reflect changing business environments and strategic decisions to move in a new direction.

Appetite Governance: The Board, "C-Suite," and Business Lines

SSG clearly outlined that in order for a risk appetite framework (RAF) to be successfully implemented, the relative roles and responsibilities of the board, senior management, and the business lines should be as follows:

- The board of directors, with input from senior management, sets overarching expectations for the risk profile.
- The CEO, CRO, and CFO translate those expectations into incentives and constraints for business lines, and the board holds the businesses accountable for performance related to the expectations.
- Business lines, in turn, manage within the boundaries of these incentives and constraints, and their performance depends in part on the RAF's performance.[17]

This can be illustrated using an amended appetite triangle, as shown in Figure 14.4.

Successful risk appetite governance relies on a strong and well-informed board, a good partnership among the senior management team and a business strategy and budgeting process that is integrated and transparent.

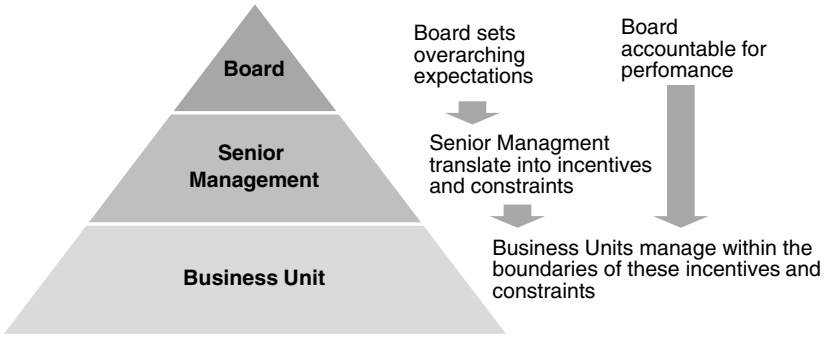

FIGURE 14.4 Risk Appetite Governance

Promoting a Firmwide Risk Appetite Framework

There is still a wide range of practice today in how widely a firm's risk appetite statements and approaches are disseminated across the firm. Some only educate those in senior roles and in business areas where risk is actively managed. Others will run a town hall campaign to ensure that every member of the firm understands the risk appetite of the firm, and how to manage within it.

Operational risk is unique in this area, as every member of the firm does actively manage operational risk in some way. Whether they are a security guard, a bond trader, a controller, an IT programmer, or a client relationship manager, all staff will manage the risk of inadequate or failed people, process, systems, or external events.

For this reason, once an operational risk appetite is stated and an approach is established for the risk appetite framework, it will likely be important to include training and awareness on this subject in any firm-wide operational risk training that is rolled out.

The most effective way to embed the framework is to hold people accountable for remaining within that appetite. In some firms, the consequences of nonadherence to risk principles or appetite statements can lead to loss of compensation, loss of promotion opportunity, or even dismissal from the firm.

Monitoring the Firm's Risk Profile within the Risk Appetite Framework

Setting limits for market and credit risk is a fairly clear-cut process. Limits can be set for traders, for trading desks, for business lines and the

firm. Value at risk (VaR) limits can be set and monitored and business decisions taken with reference to those limits and the current use of the limits. Credit can be denied to counterparties that have credit ratings that are outside the credit risk appetite of the firm. SSG suggests a host of metrics that can be used to monitor behavior against the risk appetite of the firm:

- *capital targets beyond solely regulatory measures (economic capital, tangible common equity, and total leverage) or capital-at-risk amounts;*
- *a variety of liquidity ratios, terms, and survival horizons;*
- *net interest income volatility or earnings-at-risk calculations;*
- *VaR limits;*
- *risk sensitivity limits;*
- *risk concentrations by internal and/or external credit ratings;*
- *expected loss ratios;*
- *the firm's own credit spreads;*
- *asset growth ceilings by business line or exposure type;*
- *performance of internal audit ratings;*
- *economic value added; and*
- *post-stress-test targets for capital, liquidity, and earnings.*[18]

However, few of these apply directly to operational risk. Setting "limits" for operational risk is very challenging. Unlike market and credit risk, in operational risk it is not possible to force people to unwind a transaction to get back under a risk limit. When the operational risk loss is identified, the event has already occurred and the loss is realized. Unwinding a position may not reduce the operational risk. It is not feasible to set a "limit" on how many mistakes you can make.

However, there are mechanisms for monitoring operational risk, other than the use of limits.

MONITORING OPERATIONAL RISK APPETITE

In operational risk, it may be inappropriate to consider having an *appetite* for some risks. For example, should a firm have a set *appetite* for internal fraud? For this reason, it can be helpful to consider risk *tolerance* instead. What level of internal fraud will the firm tolerate, even though its appetite is zero?

Using the language adopted earlier in the chapter, let us consider possible risk capacity, appetite, tolerance, and limit statements for operational risk. See Figure 14.5.

FIGURE 14.5 Operational Risk Appetite Framework

Risk Capacity

The risk capacity is the same as for the firm, as it is the total risk that the firm can withstand, and generally would be expressed in terms of its capital ratios or liquidity.

Operational Risk Appetite

Corporate operational risk appetite statements are likely to be qualitative statements, stating the amount of risk the firm chooses to take, or is willing to take, or that they are not willing to take. In operational risk, these statements are often purposefully broad (vague even) as accepting operational risks as being within the appetite of the board or senior management is generally not palatable. Examples of such statements could be:

- The firm will comply with laws and regulations.
- The firm will avoid business activities that may have adverse reputational impact.
- The business is an equal opportunities employer.
- The firm will invest in a robust infrastructure to support its business.

Operational Risk Tolerance

Many of the regulatory rules interchange the terms appetite and tolerance, but a semantic difference between them is particularly useful in operational risk management. While operational risk appetite statements will need to be necessarily broad, operational risk tolerances can be much more specific

as they can outline specific levels of the risk that the firm is willing to take, in the context of the broader risk appetite statements. For example, some might be black-and-white qualitative statements:

- The firm has zero risk tolerance for internal fraud.

Others might be more quantitative:

- Total annual operational risk losses will not exceed 1 percent of revenue.
- Total annual operational risk losses will not exceed $500 million.
- Employee turnover should not exceed 15 percent.
- High-risk audit items will be resolved within 90 days.
- High residual risks identified in an RCSA will be mitigated or accepted within three months.

Operational Risk Limits/Indicators

While operational risk does not lend itself to limits in the same way that market and credit risk do, it does have many ways in which risk levels can be monitored. The choice of operational risk tolerance statements will drive the tools that are used to monitor risk levels. Each of the four main building blocks of an operational risk framework offer opportunities for articulating and monitoring operational risk appetite.

Losses Tracking operational risk events against tolerance statements can provide a view into the current level of operational risk. While losses are not forward looking, there may be a tolerance statement regarding the number or size of losses and these can be tracked by business line, by risk category and by cause.

If losses are approaching thresholds that may exceed the tolerance statement, then the risk would be escalated to senior management for a decision on any necessary mitigating actions.

For example, a new business might be expected to keep its operational risk loss events below a certain percentage of revenue in order to have approval to continue.

Capital If an AMA approach is being taken to operational risk capital, then the capital levels will move as losses are incurred, scenarios change, and business environment internal control factors change. Some firms set risk

limit statements for their operational risk capital, requiring escalation to senior management if those levels are breached.

RCSA When we explored the use of scoring in RCSAs in Chapter 10, we were in effect building risk tolerance. For example, if a scoring matrix is used for risk impact, then this assumes that the risk tolerance is set at the low, medium, and high levels that are expressed in that matrix. The example scoring matrix can be seen again in Table 14.1.

These qualitative risk impact tolerance statements allow for RCSA reporting that expresses the level of risk as against the risk tolerance of the firm. In Chapter 10, we saw that scoring methods for controls and risk impacts can be developed and combined to produce an overall risk severity score, as in Figure 14.6.

Therefore, RCSA outputs can be used as tool to monitor risk levels against the tolerance of the firm. In this example, if the tolerance statement states that all high risks must be remediated or accepted with a certain time period, then the RCSA is the tool by which that situation can be identified

TABLE 14.1 Impact Scoring Example

Impact Type	Low	Medium	High
Financial	Less than $100k	Between $100k and $1m	Over $1m
Reputational	Negative reputational impact is local.	Negative reputational impact is regional.	Negative reputational impact is global.
Legal or Regulatory	Breach of contractual or regulatory obligations, with no costs.	Breach of contractual or regulatory obligations with some costs or censure.	Breach of contractual or regulatory obligations leading to major litigation, fines, or severe censure.
Clients	Minor service failure to noncritical clients.	Minor service failure to critical client(s) or moderate service failure to noncritical clients.	Moderate service failure to critical clients or major service failure to noncritical clients.
Life Safety	An employee is slightly injured or ill.	More than one employee is injured or ill.	Serious injury or loss of life.

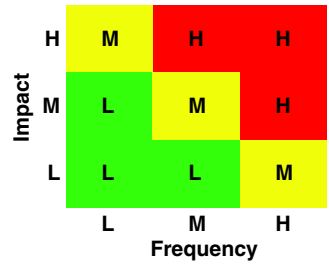

FIGURE 14.6 RCSA Risk Severity Scoring Matrix

and tracked. When a risk reaches a level that breaches the threshold for "high," then necessary action can be taken.

Metrics There are many metrics that can be used to monitor risk levels against risk tolerance statements. Any metrics that are identified as part of the operational risk KRI program should have thresholds set and should be used to produce reporting that allows for escalation of risks that are moving beyond the operational risk tolerance of the firm. As discussed in Chapter 9, the monitoring of business environment and internal control factors is an important element in the operational risk framework.

While RCSA provides monitoring at a fairly high level, metrics allow for monitoring at an individual control level, and sometime, when a true KRI is identified, at the individual risk level. The risk appetite and tolerance of the firm is therefore very important when setting appropriate thresholds for metrics as these metrics can then be used as "limits" for monitoring. The correct threshold will allow for appropriate escalation of rising risks so that business decisions can be made to keep the firm within its operational risk and appetite, and its tolerance in the risk category.

RISK APPETITE TODAY

The regulatory expectation is now established that risk appetite must be articulated, and operational risk needs to be part of that articulation. While it remains a challenging element in the framework, more and more senior management teams and boards are recognizing the benefits of setting appetites and tolerances to help ensure that the firm remains within its chosen strategic path and within its chosen risk boundaries.

KEY POINTS

- Although Basel offered little explanation of operational risk appetite, recent regulatory interpretations require it to be in the operational risk framework.
- There is still a wide range of practice in risk appetite approaches today.
- The board and senior management have responsibilities to set, approve, and monitor risk appetite.
- Risk capacity is the ability of a firm to withstand risk.
- Risk appetite is the firm's willingness to take on risk.
- Risk tolerance expresses specific risk levels that will be acceptable.
- Risk limits/levels set thresholds for indicators above which escalation is required.
- Losses, RCSA, and KRIs all provide ways to monitor risk levels.

REVIEW QUESTION

1. Under Basel II, the board of directors has which of the following responsibilities for the firm's operational risk appetite statement?
   a. Review and approve
   b. Review only
   c. Approve only
   d. Develop, review, and approve

NOTES

1. Bank for International Settlements, "International Convergence of Capital Measurement and Capital Standards: A Revised Framework," 2004, section 737.
2. www.bis.org/publ/bcbs96.pdf, p. 4.
3. Ibid., section 21.
4. Ibid., section 41.
5. www.bis.org/publ/bcbs195.pdf, p. 5.
6. Ibid., p. 6, footnote 12.
7. Ibid., Principle 5, p. 6.
8. Ibid., section 19, p. 5.
9. Ibid., section 27(c).
10. www.bis.org/publ/bcbs230.pdf, footnote 51.

11. Operational Risk Appetite Expert Group, "Operational Risk Appetite." Retrieved from www.fsa.gov.uk/pubs/international/ora_4apr07.pdf.
12. www.financialstabilityboard.org/publications/r_0910a.pdf.
13. www.fsa.gov.uk/pubs/other/ssg_2010.pdf, p. 1.
14. www.fsa.gov.uk/pubs/other/ssg_2010.pdf.
15. www.bis.org/publ/bcbs176.htm, p. 2.
16. Ibid., p. 5.
17. Ibid., p. 6.
18. Ibid., p. 9.

CHAPTER 15

Reputational Risk and Operational Risk

In this chapter we will look more closely at reputational risk and the ways that an operational risk framework can be leveraged to help identify, assess, control, and mitigate reputational risk. Examples from recent headlines will be used to highlight the significant reputational impact of most operational risk events, which often causes severe damage over and above the direct costs of the event. We will explore the causes of reputational risk and the long-term effects that it can have on a firm.

WHAT IS REPUTATIONAL RISK?

It is difficult to find an agreed-upon definition of reputational risk, but the Committee of European Banking Supervisors have offered this following:

> *Reputation risk: the current or prospective risk to earnings and capital arising from adverse perception of the image of the financial institution on the part of customers, counterparties, shareholders, investors or regulators.*[1]

Reputational *risk* may be a misnomer, as it may be more practical to consider reputational *impact*. Any risk event, market, credit, operational, or strategic, can have a reputational impact. For this reason, some firms consider reputational impact in the other aspects of their risk management programs, rather than managing a separate reputational risk activity. Others do consider reputational risk as its own category and manage it using the same tools that are available for operational and strategic risk.

First, let us consider whether there really is such a thing as reputational, or reputation risk. Is this really a risk category or is it simply a type of

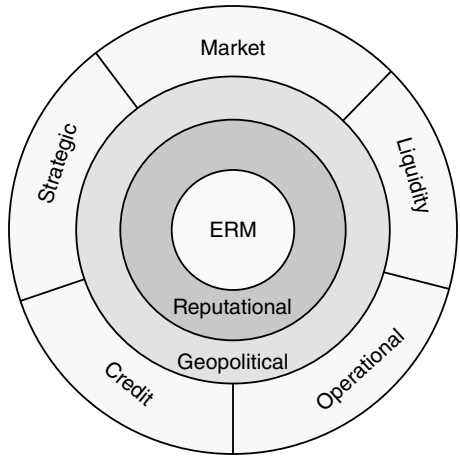

FIGURE 15.1 The Enterprise Risk Management Wheel

impact? In Chapter 10, we looked at the different potential impacts that might occur when an operational risk is identified and assessed in RCSA. There are direct and indirect financial costs, but there also may be client, regulatory, life safety, or reputation impacts.

As discussed in Chapter 1, and shown again in Figure 15.1, reputation risk sits at the heart of the risk wheel. If a risk event occurs in any risk category on the outside spokes of the wheel, it can give rise to reputational impact.

A market risk event, a credit risk event, a strategic risk event, a liquidity risk event, and of course, an operational risk event, can have severe reputational consequences.

It might be better, then, to think of reputational impact, rather than reputational risk. Whatever terminology we adopt, there is no doubt that damage to reputation can have serious consequences.

REPUTATIONAL IMPACT

We can easily identify reputational impacts by looking at two operational risk events that have occurred in recent years: Hurricane Sandy and the London Interbank Offered Rate (LIBOR) scandal.

Hurricane Sandy

In October 2012, the northeast coast of the United States was pounded by a fierce storm: Hurricane Sandy. There was physical damage on a massive scale and extended power outages. There was also tragic loss of life. While

this was an operational risk event of vast proportions, costing many billions of dollars in damaged homes and infrastructure, it was also fraught with reputational impacts for many of those who were directly impacted.

The power companies quickly faced public and local government criticism for not moving quickly enough to restore power. Similarly, phone and cable companies were vulnerable to reputational damage if they were perceived to be reacting too slowly to the event. The quality of customer service in these organizations, and the efficiency of their repair crews, quickly became a hot topic.

Politicians faced the ire of the constituents and political careers may well have been made and broken during the weeks and months following the storm.

This was an operational risk event that was caused by natural disaster, and yet the reputational fallout was severe for all who were impacted.

The LIBOR Scandal

An operational risk event, where the cause is attributed to the internal actions of a bank often gives rise high levels of reputational damage. The LIBOR scandals of 2012 and 2013 tarnished the reputations of many banks.

It was alleged that several major banks had manipulated the LIBOR rate over an extended period, in order to benefit financially from the altered rate. The brush was quickly used to also tarnish other benchmark rates globally and regulators from many nations became engaged in uncovering the breadth and depth of the bad behavior.

Headlines from this period show the reputational wounds that were inflicted on those involved, above and beyond the direct operational risk losses that they suffered in direct fines.

> ***Rigged Rates, Rigged Markets***
>
> *Marcus Agius, the chairman of Barclays, resigned on Monday, saying "the buck stops with me." His was the first departure since the British bank agreed last week to pay $450 million to settle findings that, from 2005 to 2009, it had tried to rig benchmark interest rates to benefit its own bottom line.*
>
> ***New York Times,* July 2, 2012**[2]

> ***RBS Managers Condoned Libor Manipulation***
>
> *Royal Bank of Scotland Group Plc managers condoned and participated in the manipulation of global interest rates.*
>
> ***Bloomberg Business Week,* September 25, 2012**[3]

UBS and LIBOR

Horribly rotten, comically stupid.

***The Economist,* December 19, 2012**[4]

As a result of its role in the alleged LIBOR manipulation, Barclays paid out $450 million in a settlement with the British and U.S. regulators and lost its chief executive officer, Robert E. Diamond Jr.; its chairman, Marcus Agius; and its chief operating officer, Jerry del Missier, along with many other key senior managers.

It then suffered a ratings hit as both Standard and Poor's (S&P) and Moody's rating agencies placed the firm on negative watch:

The abrupt changes alarmed the ratings agencies. Standard & Poor's said in its statement that "the negative outlook reflects our view of the current management flux and near-term strategic uncertainty."

In a separate statement, Moody's said: "The senior resignations at the bank and the consequent uncertainty surrounding the firm's direction are negative for bondholders."[5]

In addition, Barclays, along with many other alleged participants, at the time of writing was facing multiple lawsuits from firms and individuals who allege that the LIBOR manipulation impacted them adversely.

Charles Schwab Sues Banks Over Rate Manipulation

Charles Schwab is seeking unspecified compensatory and punitive damages from the banks. Other defendants include foreign banks like Barclays, Credit Suisse, Deutsche Bank, HSBC Holdings, Royal Bank of Scotland, Lloyds, WestLB and UBS.

***New York Times,* August 25, 2012**[6]

Banks Rigged Libor To Inflate Adjustable-Rate Mortgages: Lawsuit

Homeowners in the U.S. are suing some of the world's biggest banks for fraud–not over any foreclosure issues but over the alleged Libor manipulation scam that they say sparked increases on their adjustable rate mortgages, and resulted in unlawful profits for the banks.

***Forbes,* October 15, 2012**[7]

Finally, the threat of fines and lawsuits across the industry pushed stock prices down.

Barclays Libor Fine Sends Stocks Lower as Probes Widen

Barclays Plc (BARC)'s record $451 million fines for interest rate manipulation sent bank shares plunging as U.S. and U.K. authorities pursue sanctions in a global investigation of more than a dozen lenders.

Bloomberg.com, June 28, 2012[8]

The scandal eventually spread to other banks involved in LIBOR, and at the time of writing, the New York and Connecticut attorneys general had 16 banks under investigation on this issue: Bank of America, Bank of Tokyo Mitsubishi UFJ, Barclays, Citigroup, Credit Suisse, Deutsche Bank, HSBC, JPMorgan Chase, Lloyds Banking Group, Norinchukin Bank, Rabobank, Royal Bank of Canada, Royal Bank of Scotland, Société Générale, UBS, and West LB. In December 2012, UBS agreed to settle with regulators for a huge $1.5 billion in total fines.

All of these banks faced the same reputational damage above and beyond the regulatory dollar fines that they were likely to pay. They faced loss of key personnel (who might also face jail time), credit downgrading, litigation, and stock price devaluation.

A reputational risk event therefore results in multiple impacts occurring, some of which are captured in the operational risk framework, but some might not be. Fines and litigation are captured in an operational risk framework as they meet the definition of operational risk:

Operational risk is defined as the risk of loss resulting from inadequate or failed processes, people and systems or from external events.

This definition includes legal risk, but excludes strategic and reputational risk.[9]

Stock price losses, credit downgrades, and loss of key personnel are not generally considered financial losses within this definition, and reputational risk is expressly excluded. However, this does not mean these risks should remain unmanaged or unmitigated.

While the preceding examples arose out of operational risk events, reputational damage can arise from other events such as market risk and credit risk. Significant losses in either area can lead to serious questions about the ability of the firm to operate effectively in the markets and this can lead to loss of clients, and loss of share value.

In addition to reputational impact arising from other risk types, it can also arise out of activities that are not risky in any other sense. For example, banks are increasingly avoiding investments and funding for

environmentally unpopular or social unacceptable practices. It is common today for banks to issue glowing corporate social responsibility reports that outline their fair, environmental sound, and socially responsible values and practices.

> ***Banks Grow Wary of Environmental Risks***
>
> *After years of legal entanglements arising from environmental messes and increased scrutiny of banks that finance the dirtiest industries, several large commercial lenders are taking a stand on industry practices that they regard as risky to their reputations and bottom lines.*
>
> ***New York Times,* August 30, 2010**[10]

Stock Price Impacts

One of the major drivers for strong reputational risk management is not the direct costs of the event that has occurred, but rather the negative impact on share value. As we saw earlier, the banking sector as a whole took a major stock hit as a result of the widespread LIBOR scandal. Barclays themselves saw an 18 percent slide during the early stages of the news breaking.

In 2005, Perry and de Fontnouvelle completed a study[11] on the market reaction to operational risk announcements. They examined the difference between internal fraud events and other events, on the assumption that internal fraud events carry a much higher reputational impact than, for example, execution errors.

Their research found that losses from internal fraud events resulted in larger impacts to share value than those that were not internal fraud, suggesting reputational impact had real cost.

A similar study was conducted in 2010 by Gillet, Hubner, and Plunus. The authors examined stock market reactions to the announcement of operational losses by financial companies, and attempted to disentangle operational losses from reputational damage. Their results showed:

> *. . . significant, negative abnormal returns at the announcement date of the loss, along with an increase in the volumes of trade. In cases of internal fraud, the loss in market value is greater that the operational loss amount announced, which is interpreted as a sign of reputational damage.*[12]

The apparent reputational impact on stock price can also be seen in the JPMorgan "Whale" case study in Chapter 18.

REGULATORY OVERSIGHT OF REPUTATIONAL RISKS

In September 2012, the Basel Committee on Banking Supervision (BCBS) released updated "Core Principles for Effective Banking Supervision" and listed the following essential criteria as guidance to banking regulators:

> *The supervisor understands and assesses how group-wide risks are managed and takes action when risks arising from the banking group and other entities in the wider group, in particular contagion and* reputation *risks, may jeopardize the safety and soundness of the bank and the banking system. [emphasis added]*[13]

Similarly, in the BCBS 2009 "Principles for Sound Stress Testing Practices and Supervision," they recommend that stress testing should incorporate considerations of reputational damage:

> *Stress tests should feature a range of severities, including events capable of generating the most damage whether through size of loss or through loss of* reputation.
>
> *A bank should enhance its stress testing methodologies to capture the effect of* reputational *risk. [emphasis added]*[14]

In its 2010 update of the "Principles for Enhancing Corporate Governance," BCBS stated that the roles of the board, senior management and the risk committee should include activities concerning reputational risk:

> *… strategies for capital and liquidity management, as well as for credit, market, operational, compliance,* reputational *and other risks of the bank. [emphasis added]*[15]

And that the role of the board and senior management in overseeing risks in certain complex or nontransparent structures should include:

> *Senior management, and the board as appropriate, should note these challenges and take appropriate action to avoid or mitigate them by:*
> - *establishing adequate procedures to identify and manage all material risks arising from these activities. The bank should only approve these operations if the material financial, legal and* reputational *risks can be properly identified, assessed and managed. [emphasis added]*[16]

So the BCBS rules expect a firm to have strategies around its reputational risk, identify, measure and manage its reputational risks and stress test reputational risk impacts to the firm. This sounds very like the requirements for operational risk.

In Basel II itself, although reputational risk is expressly excluded from the Pillar 1 requirements for operational risk, it reemerges in Pillar 2.

> ***Other risks:*** *Although the Committee recognizes that "other" risks, such as reputational and strategic risk, are not easily measurable, it expects industry to further develop techniques for managing all aspects of these risks.*[17]

National regulators have implemented their local rules for the supervision of Pillar 2 under regulations known as ICAAP (Internal Capital Adequacy Assessment Process). In these documents they have included reputational risks as one of the material other risks that need to be captured as part of the bank's exercise to demonstrate that it holds adequate capital overall under Basel II.

Therefore, banks that are under the Basel II rules need to be able to identify, assess, and mitigate reputational risk. Banks who are not under Basel II frequently find that there regulators nevertheless expect Basel II type standards to be in place for risk management.

Apart from the regulatory pressures, it is good business sense to actively manage risks that can seriously harm the firm.

REPUTATIONAL RISK MANAGEMENT FRAMEWORK

Although the Basel II definition of operational risk explicitly excludes reputational risk, some firms adopt an internal definition that expressly includes operational risk. As we saw in Chapter 1, Citi includes reputational risk in their definition of operational risk:

> *Operational risk is the risk of loss resulting from inadequate or failed internal processes, systems or human factors, or from external events. It includes the reputation and franchise risk associated with business practices or market conduct in which Citi is involved.*[18]

The operational risk framework is designed to identify, assess, control and mitigate a hard to manage risk. The elements of the framework are

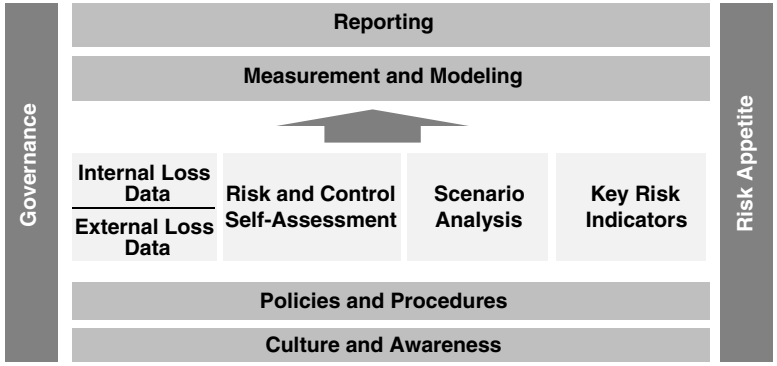

FIGURE 15.2 The Operational Risk Framework Structure Can Simply Be Renamed and Reused as a Reputational Risk Framework

therefore effective in the meeting the similar challenge of managing and measuring reputational risk. Indeed, several of the operational risk elements routinely already consider reputational impacts of operational risks (although not of other risk types such as market, credit, or liquidity risks).

We can adapt the operational risk framework to meet reputational risk needs, and we can leverage existing operational risk activities to include the management and measurement of reputational risks. See Figure 15.2.

Drivers

The drivers for reputational risk management are very similar to the drivers of operational risk management:

- It is sound business management to manage all risks.
- Excellence in reputation risk management provides transparency, foresight, and protection.
- Strong reputational risk management can
  - Lead to potentially fewer (bad) surprises
  - Allows for quicker recovery from events
  - Ensure adequate capital is held to protect the firm from reputation risk events
  - Allow for full assessment of reputation risks prior to business decision making
  - Lead to increased investor/shareholder confidence

Governance

Starting with governance, the same questions apply as for operational risk management: who owns the function, and what should the function own?

Some firms have an individual who is responsible for reputational risk across the firm. That person often resides in the legal department, but it could be argued that they should sit in the risk function in order to ensure that they have the appropriate independence.

There is often a franchise risk or reputation risk committee to which reputational risk issues are escalated. These issues might be raised from the operational risk area, or from other areas where no operational risks are anticipated, and yet reputational risk remains.

For example if a deal is being considered with a counterparty who has a less than stellar reputation, or in an industry where there is strong public protest, such as some mining techniques, then there may be associate reputational risk.

In such cases, the deal can be brought to the franchise committee for consideration. There may be a single global committee, several independent regional committees, or a hierarchy of local and global committees.

The membership of such a committee should probably include:

- Head of corporate social responsibility
- Head of legal
- Head of compliance
- Head of human resources
- Head of risk
- Head of investor relations
- Business heads
- Chief operating officer (COO)
- Chief financial officer (CFO)

Event Data Collection

In the same way that operational risk losses are captured in a database for management and mitigation of the risks, reputational risk events could be captured in a database for the same purpose.

It may be more efficient to leverage the existing operational risk loss database for this purpose. It is certainly fairly simple to add a reputational impact field to an operational risk loss database to ensure that for all operational risk events, the reputational impact is being captured.

TABLE 15.1 Possible Reputational Impact Scoring Method for RCSA

Impact Type	Low	Medium	High
Reputational	Negative reputational impact is local.	Negative reputational impact is regional.	Negative reputational impact is global.

RCSA

As we saw in Chapter 10, it is certainly possible to capture the reputational impact of an operational risk during the RCSA process. The sample reputational risk scale is shown again in Table 15.1.

However, the RCSA could also be leveraged to capture *all* reputational risks, simply by expanding the scope of the RCSA. For example, once all operational risks have been identified, further questions could be asked concerning what reputational risks could also arise in other ways. The reputational impact scoring method could be used to assess the relative priority of those risks.

The use of the RCSA for this purpose would allow for reputational risks that have not yet occurred to be identified, assessed, and controlled and decisions made on whether they need to be mitigated.

An example of such a risk could be "we invest in a company that has environmentally damaging practices."

Key Risk Indicators

In the same way that metrics can be used to help monitor whether operational risks are becoming more or less elevated, metrics can be used to monitor reputational impacts of operational risks. Metrics could also be established to monitor reputational risk indicators that are unique to reputational risk.

For example, how many NGO protest letters has the firm received? How many of the firm's clients are currently under investigation for employing sweat shop labor? What percentage of the United States' mountain-top removal mining is funded by the firm?

The Corporate Social Responsibility department could design and develop these types of metrics for review by the franchise or risk committee on a periodic basis.

Scenario Analysis

The scenario analysis program can be leveraged to meet the stress testing requirements that were outlined above. There is a regulatory expectation

that reputational considerations are included in stress testing when assessing capital adequacy for the firm.

The operational risk function will already have a scenario analysis program that handles the collection of data in the difficult and subjective area of very large operational risk exposures. This program will be well suited to providing the same structured output for reputational risk scenarios.

A scenario analysis program could be run separately for reputational risk, or reputational risk scenarios could be added to the existing operational risk scenario analysis program to improve efficiency.

Reporting

As with operational risk reporting, senior management are likely to be seeking reporting on reputational risk that addresses the following concerns:

- Where is our risk?
- What action do we need to take?
- Who is under control?
- Who is not?
- Are we meeting our regulatory requirements?

Reporting might be designed to go to the risk committee, or to the franchise committee, or to both. It is important that the risk committee and the chief risk officer are aware of all risks in the firm and so some summary and escalation reporting process should be put in place to facilitate that.

As reputational risk issues often arise in the operational risk reporting process, it may be most efficient to combine overall reputational risk reporting with operational risk reporting.

Whatever approach is taken, the owner of reputational risk management at the firm should consider taking a risk analysis approach, and not just a data gathering approach. In other words, they should undertake to provide the following for reputational risk:

- Analyze raw data.
- Analyze trends and predictors (KRIs).
- Follow news articles.
- Present opinions.
- Present capital at risk and stress testing impacts.
- Recommend action and mitigating strategies.

KEY POINTS

- Reputational risk is excluded from the Basel definition of operational risk. However, many firms include it in their internal definition of operational risk.
- The impact of reputational risk on capital occurs through its inclusion as a "material risk" under Pillar 2 of Basel II and as a result of its consideration in stress testing.
- Events that have a reputational impact often result in many knock-on negative impacts including:
  - Litigation
  - Regulatory fines
  - Loss of key personnel
  - Stock price devaluation
- Studies have shown that operational risk events that have a higher reputational impact result in a more pronounced loss in share value.
- The operational risk framework can be leveraged for the effective management of reputational risk.

REVIEW QUESTION

1. Which of the following statements is true
   a. The Basel II definition of operational risk includes reputational risk.
   b. Reputational risk is captured under Pillar 1 of Basel II.
   c. There is no reputational impact in operational risk.
   d. The impact of reputational risk is captured under Pillar 2 of Basel II.

NOTES

1. CEBS Consultation Paper, "Application of the Supervisory Review Process under Pillar 2 (CP03 revised)." 2005.
2. www.nytimes.com/2012/07/03/opinion/rigged-rates-rigged-markets.html.
3. www.businessweek.com/news/2012-09-24/rbs-managers-said-to-condone-manipulation-of-libor-rates.
4. www.economist.com/blogs/schumpeter/2012/12/ubs-and-libor.
5. dealbook.nytimes.com/2012/07/05/attention-turns-to-barclays-future/.
6. dealbook.nytimes.com/2011/08/25/charles-schwab-sues-banks-over-rate-manipulation/.
7. www.forbes.com/sites/halahtouryalai/2012/10/15/banks-rigged-libor-to-inflate-adjustable-rate-mortgages-lawsuit/.

8. www.bloomberg.com/news/2012-06-28/barclays-451-million-libor-fine-paves-the-way-for-competitors.html.
9. Bank for International Settlements, "International Convergence of Capital Measurement and Capital Standards: A Revised Framework," 2004, section 644.
10. www.nytimes.com/2010/08/31/business/energy-environment/31coal.html?_r=0.
11. Jason Perry and Patrick de Fontnouvelle, "Measuring Reputational Risk: The Market Reaction to Operational Loss Announcements," Federal Reserve Bank of Boston, 2005.
12. R. Gillet, G. Hubner, and S. Plunus, "Operational Risk and Reputation in the Financial Industry, 2010. Retrieved from http://dx.doi.org/10.1016/j.jbankfin.2009.07.020.
13. www.bis.org/publ/bcbs230.pdf, p. 36.
14. www.bis.org/publ/bcbs155.pdf, Principles 9 and 14.
15. www.bis.org/publ/bcbs176.pdf, section 52.
16. Ibid., section 122.
17. See note 9, section 742.
18. Citi Annual Report 2011, p. 106.

CHAPTER 16

Operational Risk and Convergence

In this chapter, we explore the growing enthusiasm for convergence, or governance, risk, and compliance (GRC). Both terms refer to the adoption of an integrated approach to managing the various elements of operational risk so that related activities can be leveraged, efficiencies attained and more powerful risk management results achieved. We will consider how a converged approach can be effective in assessment and in metrics and will discuss the powerful reporting possibilities that can result from an integrated approach.

OPERATIONAL RISK AS A CATALYST FOR CONVERGENCE

Operational risk management aims to provide transparency into the operational risk exposures of the firm, by identifying, assessing, monitoring, controlling, and mitigating those risks. The depth and breadth of operational risk in every firm means that the operational risk department needs to take on a unique role. Not only must it build partnerships with all of the underlying operational risk activities, but also attain a governance structure that allows it to influence decision making at every level of the firm. In addition, it often has to facilitate a culture change across the firm so that operational risk management becomes a day-to-day embedded activity in the firm.

The rise of operational risk management has led to the emergence of integration and convergence initiatives and has energized enterprise risk management (ERM) discussions. The qualitative tools of the operational risk framework are being investigated by market, credit, strategic, reputational, and geopolitical risk specialists as the purely quantitative models of the past have revealed weaknesses.

Operational risk management is an art as well as a science, requiring excellent influencing skills, communication skills, facilitation skills, and analytical skills for success.

The future of operational risk is still evolving, but it is certain that it will remain as an important and relevant risk management function in the financial services industry and the discipline is being adopted across many other industries as the benefits of proactive operational risk management are realized.

In addition to its influence on other risk disciplines, the formal operational risk frameworks that have evolved in the past few years have led to improvements and integrations in many related activities. Audit, compliance, Sarbanes-Oxley, information security, business continuity, and many others have similar assessment, metrics, and reporting needs. As the operational risk framework has matured, the overlaps, duplications, and opportunities for leveraging have become more and more clear.

GOVERNANCE, RISK, AND COMPLIANCE (GRC)

There is strong movement toward integrating all operational risk–related activities, and this is often referred to as governance, risk, and compliance (GRC) or convergence. This integration refers to both the activities that are part of the operational risk framework, and the other activities that exist outside that framework but are concerned with operational risk. These other activities include business continuity planning, information security, compliance desk reviews, legal event tracking, audit reports, and Sarbanes-Oxley assessments.

In Chapter 4, we examined the various governance structures that can be used to support an operational risk function. Some of these were more conducive to a GRC strategy at the firm, but it is possible to implement a GRC strategy in any governance structure. A GRC strategy requires senior management support and positive participation from all parties.

Without a GRC approach, there may be a waste of resources, contradictory reporting, incomplete analysis of risks, duplication of effort, and a misperception of risk exposures.

For example, when all operational risk-related functions work independently, they also interact separately with the business and support areas and report separately to management. The separate views of the risks and the separate representation of these views can be confusing and even misleading.

Let us take risk assessment as an example where convergence can be beneficial.

Assessment Convergence

Without an integrated approach, the risk assessment activities in a firm can produce severe assessment fatigue, as business units and support areas are asked to complete a myriad of different assessments, which often rely on the same key individuals in their area.

The first step in integrating risk assessment activities is to understand what the catalog of activities is. Firms are often surprised to discover that they have more than 20 assessments going on each year, all of which touch on subsets of operational risk categories. It can be help to map those activities to see where the overlaps and gaps are. Figure 16.1 illustrates an example mapping of assessment activities in a firm. In this diagram, two businesses units (BU 1 and BU 2) and three support areas (IT, Ops, and Finance) have listed the assessment activities that they are currently engaged in, and where these activities touch on aspects of a Basel II operational risk category. For example, the SOX 404/301 assessment is undertaken by all business units and support areas, and includes areas that are part of the Internal Fraud, Business Disruption and Systems Failures, and the Execution, Delivery, and Process Management risk categories.

In contrast, the anti–money laundering (AML) assessment is only undertaken by the business units and by operations. The AML assessment covers areas that would be under the Clients, Products, and Business Practices risk category.

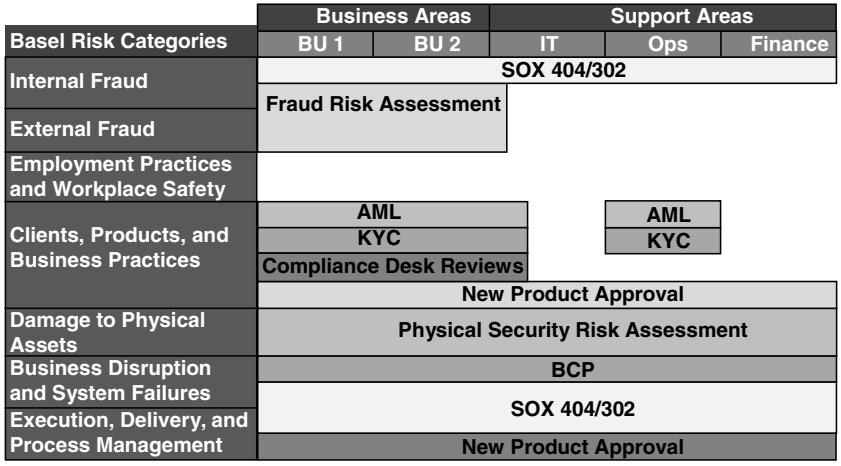

FIGURE 16.1 Map of Existing Assessment Activities Against Operational Risk Categories

Figure 16.1 is a highly simplified version of the mapping that will occur when most firms attempt this exercise. The complexity of assessment activities, the amount of duplication, and the size of some of the gaps is often eye-opening.

However, each of the assessments is likely driven by regulatory requirements or strong business drivers, and so any simplification needs to ensure that the quality and completeness of assessments is not compromised.

The operational risk function will often discover that there are so many gaps in this patchwork, that RCSA is necessary to ensure completeness of risk assessment across all areas of the firm and across all risks that lie within each risk category.

For example, an existing fraud risk assessment might not capture all underlying internal and external fraud risks at level 2 (level 2 risks were discussed in Chapter 7) and it might not capture all departments.

The resulting multitude of necessary activities is often duplicative and burdensome on the firm. Figure 16.2 illustrates a nonconverged model where all owners of risk assessments interact separately with their stakeholders in the firm. In this illustration only a handful of firm wide assessments have been included, but it is easily apparent that there will be inefficiencies and resulting frustrations in this unconverged approach.

This is the model that was in place in many firms in the early stages of the implementation of the operational risk framework. RCSA became an additional assessment burden on the firm, and each assessment was run as a separate activity. To alleviate some of this stress on the firm, some operational risk functions have looked into how to leverage the results of other assessments in the RCSA so that at least that assessment is not unnecessarily duplicative.

For example, why ask questions about risks and controls that have already been assessed by the Sarbanes-Oxley (SOX) program? In fact, it is

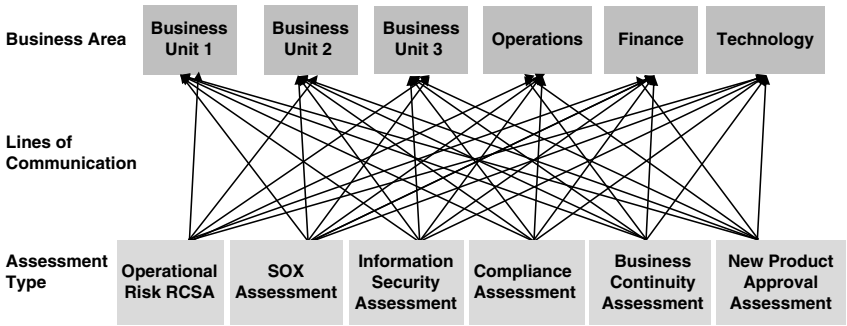

FIGURE 16.2 A Nonconverged Approach to Risk Assessment

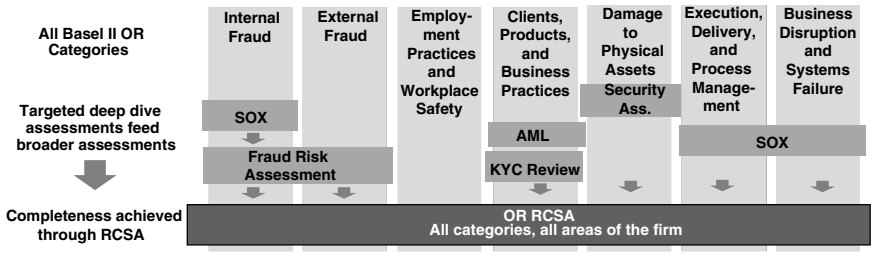

FIGURE 16.3 Leveraging Underlying Assessments in RCSA

dangerous to reassess any SOX risks and controls as it is very important that the SOX certifications are not compromised by any new scoring that does not match the SOX conclusions.

Figure 16.3 illustrates how the RCSA program can leverage deep dive underlying assessments, while ensuring comprehensive cover of all risks in the Basel II operational risk categories.

Figure 16.3 illustrates how the SOX assessment can be leveraged in any fraud risk assessments, and how the fraud risk assessment can then be leveraged in RCSA. By using the results from underlying assessments, the risk and control self-assessment (RCSA) process can avoid duplication and can ensure consistency of reporting among the different assessment teams.

Alternatively, this process could be designed so that the RCSA process now gathers all of the assessment information that is needed by the underlying assessments. For example, the RCSA program could ask for information above and beyond its own requirements so that the underlying assessment needs are met in that one assessment activity. If this approach is taken, then it allows for a highly simplified communication model for assessment at the firm, as is illustrated in Figure 16.4. This leveraging and sharing of assessment data can happen only if the data can be shared among the assessment teams.

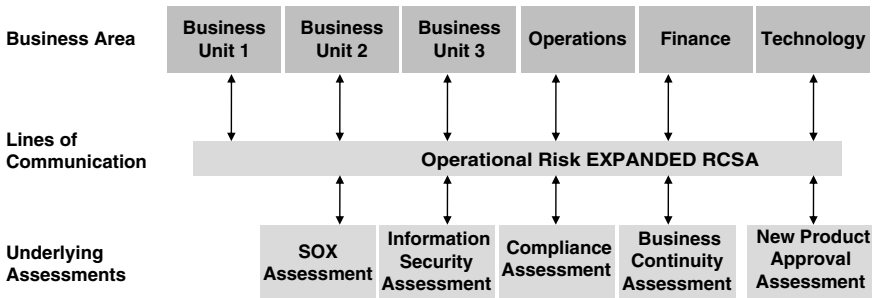

FIGURE 16.4 Simplified Communication Model with Expanded RCSA

Converged Assessment Data The key to an effective GRC program is to provide a central repository for data that can be used by all parties. This is often a challenging undertaking, as each assessment is likely to have different systems, from sophisticated workflow tools, to simple spreadsheets.

However, it is possible to share data without sharing tools. To achieve this, a central "golden source" of data needs to be established and an owner anointed for those data. The operational risk function is uniquely placed to drive such an initiative, as it needs to access all assessments data that relate to operational risk.

For this reason, GRC initiatives are often kicked off by the corporate operational risk function. At the very least, they will be a key stakeholder in such projects, including the data storage.

Assessment Taxonomies Common data requires a convergence of language, to ensure that all parties are using categorizations and definitions in the same way. All risk assessment owners will need to use the same terms when referring to risks and controls. They will likely also need to develop the same language for processes and for organizational hierarchies. Without these common taxonomies it is difficult, or impossible, to leverage data from one assessment for use in another, or to consolidate assessment results meaningfully.

Final converged taxonomies are a desirable end state, but in the meantime it is often possible to simply map different taxonomies to each other to allow for powerful integrated reporting. This can be done using a Rosetta Stone approach—where all libraries map into a central common library of terms.

Developing taxonomy for each of the common elements is a huge task, and should not be underestimated. To get every assessment owner to agree on the language that will be used for process, risk, control, and organizational hierarchy is a complex, political, and practically challenging undertaking.

Assistance can be found in the form of straw man taxonomies for each area. Many consulting firms today offer to provide these straw man taxonomies and to shepherd the organization through the process of engaging all stakeholders and getting agreement on terms for risk, control, process, and hierarchy. Some firms have also developed standard taxonomies for products.

The operational risk department can get the most value from taxonomies if they take the further step of mapping the connections between them. For example, for every process, what are the risks that may exist? A matrix mapping these two is very helpful in ensuring all risks are captured whenever the same process is assessed in a different area of the firm.

In each risk, what are the expected types of controls? A matrix mapping risks to controls is very helpful in developing more standardized scoring methods for the effectiveness of controls. Therefore, using taxonomies and

mapping matrices between them, the operational risk department can identify for an RCSA:

1. Which part of the organization hierarchy is being assessed?
2. Which processes exist in this area?
3. Which risks are associated with those processes?
4. What are the expected controls for those risks?
5. Have any underlying assessments already assessed those risks and controls?

Converged Assessment Tools Figure 16.4 assumes that many fundamental elements are the same for all assessments represented in that model. For example, it assumes that the timing of the RCSA would be appropriate for the compliance assessments, and the sign off requirements would be appropriate for the SOX assessments. However, in practice, this is often not the case. There may be critical deadlines for assessments and different required periods for assessments. In order for an enhanced RCSA to meet all of these requirements it might then need to occur at too broad a scale and too often, with overburdensome sign-off requirements, in order to meet all of the underlying assessment requirements.

A solution to this problem is to move all of the assessments onto a single assessment tool and allow them to conduct their assessments with the business units as needed. The fact that there are multiple assessments being conducted can be invisible to the business unit, if the business only interacts with a single assessment tool. That tool could send out assessment questions each month as needed, and the results parsed to the assessment areas that need them. By using sophisticated workflow tools, sign-off and scoring can all be built into the tool. In this way, assessment will have a standardized look and feel to the business unit, and duplication will be removed as the tool would provide recent results to the assessment teams, and exclude them from this month's list of assessment questions for the business.

There are many such tools on the market today, but many firms are also selecting to build them in house. They rely on robust taxonomies, excellent workflow capabilities, and centralized data.

A possible ideal end-state for such an approach is illustrated in Figure 16.5.

At its most robust, a converged, or GRC assessment strategy results in an integrated reporting platform that allows management to review assessment data from all sources across the firm.

Convergence of Metrics

The need for metrics has grown exponentially in recent years. Metrics are gathered by risk assessment areas, control functions, and business

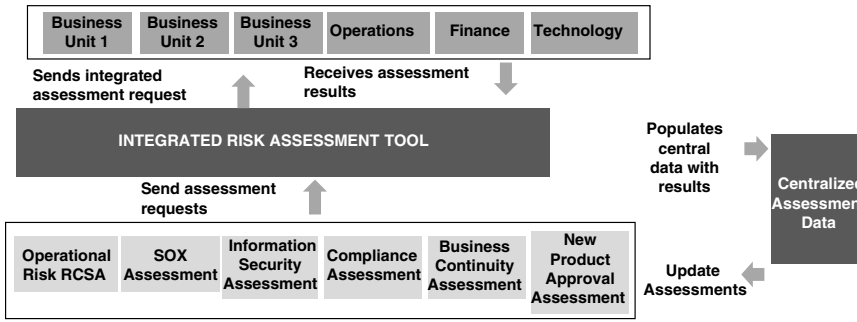

FIGURE 16.5 Communication Flows Using an Integrated Risk Assessment Tool

departments. Some are used to measure efficiencies, some are used to monitor risk, and some are used to measure performance against strategic goals. As a result, many firms have found themselves entangled in multiple metrics initiatives that use communication and data gathering models similar to the confused communications illustrated in Figure 16.2. The technological complexities of having multiple metrics databases accessing the same metrics data can cause serious headaches in the information technology (IT) department and frustrations from the data owners.

Figure 16.6 illustrates the complexity of a nonconverged approach to metrics. In this illustration, the requests for metrics data are made by all areas of the firm. A business unit might requests data from operations, operations may requests data from technology, and technology may request data from finance. Each area of the firm has unique metrics needs and uses, and this often results in every area receiving multiple similar but slightly different requests for metrics data.

If standardized taxonomies have been developed for the firm, then a converged approach can also be taken to metrics gathering and usage. This approach generally looks very similar to a converged approach to assessment as a centralized data repository for metrics data is accessed by all metrics users and providers. Figure 16.7 illustrates how such an approach limits the data requests received by each area of the firm and allows users of metrics to access one location for all of their data needs.

There are many advantages to such a centralized metrics data approach:

- Consistent data quality standards can be applied.
- Consistent metrics reporting is ensured.
- "Golden sources" of data can be identified.
- Duplicate sources of data can be eliminated.

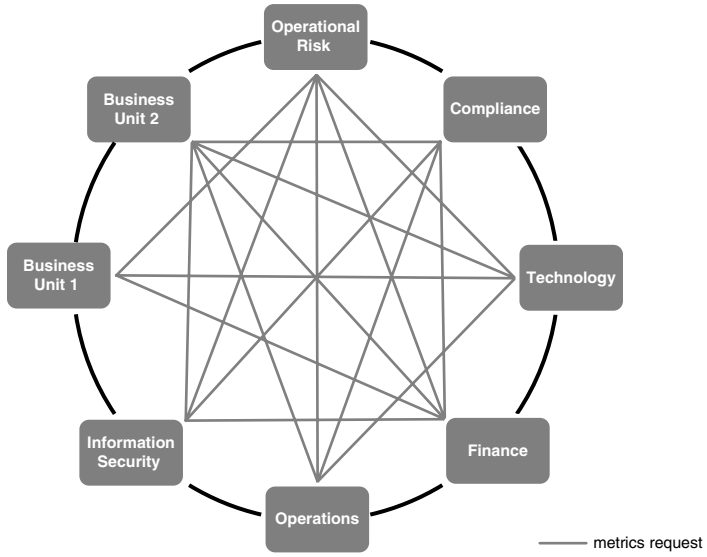

FIGURE 16.6 A Nonconverged Approach to Metrics Results in Multiple Data Requests

- Only one connection or "pipe" is needed to each source of data.
- Efficiency savings.
- Best practices are leveraged.

Metrics initiatives in banks in the past were often doomed to failure. They often relied on the enthusiasm and support of a small number (sometimes one) senior manager and the cost and effort involved in producing useful results was often considered prohibitive. When cost-cutting cycles came along, the metrics initiative often was one of the first initiatives to be axed.

Today, metrics are considered to be an essential element in a well-managed bank. Regulators, boards, and executive management teams demand metrics to evidence the current state of controls, risks, performance, and efficiencies. As the permanence of metrics is now become evident, more and more firms are looking at the current complexities of their many metrics programs and are exploring initiatives to converge those programs, using a robust central data strategy.

This improved data management and warehousing approach also fits within the second major recommendation made by the Senior Supervisors Group in its "2010 Observations on Development in Risk Appetite Frameworks and IT Infrastructure."[1] The risk appetite elements of this

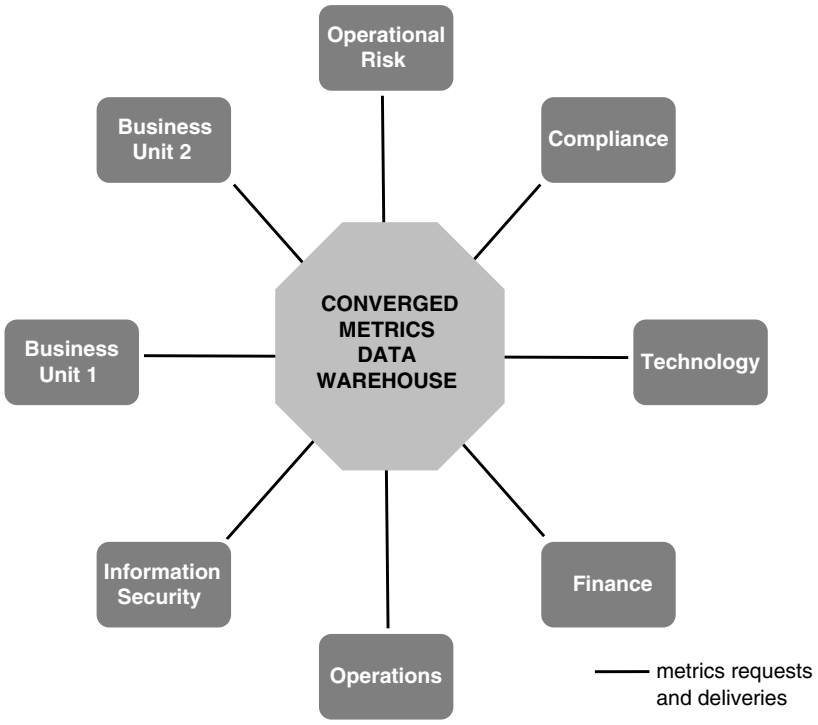

FIGURE 16.7 A Converged Approach to Metrics Data Warehousing

report were discussed in Chapter 14, but the second major recommendation was that banks make fundamental improvements in the quality of their data and the processes that surround that data.

CONVERGED OR GRC REPORTING

In addition to having assessment and metrics data mapped to standard taxonomies, and held in centralized data repositories, many firms are now looking at taking the same approach to their event data and their action tracking processes.

For example, all operational risk loss events, all audit items, and all regulatory exam results could be housed in one database. By housing all of these items in one location, mapped against standard taxonomies, it is now possible to also house all related action tracking in one location also. This fully integrated approach is referred to as a GRC approach.

GRC Tools

The level of interest in a GRC approach has led to many software firms developing off-the-shelf and configurable tools that promise to do some or all of the following:

- Provide workflow for many different assessments.
- Manage the capture and storage of loss event data.
- Manage the capture and storage of audit items.
- Manage the capture and storage of compliance items.
- Manage SOX processes and sign-off.
- Warehouse metrics for all operational risk-related functions.
- Provide taxonomy warehouses for process, risk, control, organizational hierarchies, and products.
- Support matrixed relationships between taxonomies.
- Provide all underlying data in dashboard and hard copy reporting.

Many firms have also decided to develop their own GRC tools and are linking them to other management information systems that they have in place. When firms have achieved this impressive end state of convergence and are able to mine the data they will be able to ask profound and powerful operational risk questions. For example, if the operational risk department has recently learned of a major external event in the area of unauthorized trading, they would be able to gather the following information with ease:

- What residual scores do all assessments show against unauthorized trading risks?
- What unauthorized trading loss events have occurred in the past five years?
- What outstanding audit items are there that relate to unauthorized trading?
- What do our KRIs show us regarding controls that are related to unauthorized trading?

Similarly, the head of a business area could use a GRC tool to ask the following questions about his own department:

- What action items are currently outstanding and which are late? (All audit, all compliance, all SOX, and all operational risk actions items would be displayed at once.)
- What process has the weakest-scoring KRIs?
- What process has produced the most loss events and audit items in the past three years?

This type of proactive operational risk management is facilitated by a converged approach to operational risk and its related activities.

KEY POINTS

- Convergence or governance, risk, and compliance (GRC) are terms used to describe an integrated approach to managing operational risk activities and related activities across the firm.
- Assessment integration can lessen the assessment burden on a firm.
- Metrics convergence can result in higher quality data practices and lessen the data request burdens on the firm.
- GRC reporting allows for powerful operational risk management reporting, including dashboard and management information systems that facilitate proactive operational risk management questions.
- Successful convergence requires the development and implementation of standard taxonomies for process, risk, control, and organizational hierarchy. Product taxonomies are also important in many cases.

REVIEW QUESTION

1. GRC is the common term used for:
   a. Governance, reliance, and content
   b. Global risk convergence
   c. Governance risk and compliance
   d. Global regulatory controls

NOTE

1. www.fsa.gov.uk/pubs/other/ssg_2010.pdf.

CHAPTER 17

Best Practices in Related Risk Management Activities

There are many activities within a firm that manage a specific operational risk or subset of operational risks. Each of these may have existed well before the operational risk corporate function was formed, and may be owned by specialists in that field. In addition to meeting all operational risk regulatory and business requirements, these risk areas often have their own unique regulations and business drivers.

As discussed in Chapter 16, the operational risk department must forge strong relationships with these areas in order to ensure the success of the framework and to ensure consistency in reporting and escalation of operational risks throughout the firm.

In this chapter, we will learn some more about each of these unique areas and their best practices.

NEW-PRODUCT APPROVAL

One of the most effective weapons against Clients, Products, and Business Practices events is a robust new-product approval process. This control should be designed to ensure that all risks are considered when a new product is being proposed. The market and credit risks may be well understood by those involved in proposing the new product, but they may be unaware of the resulting operational risks that may arise. Therefore, a new-product proposal should be reviewed by the legal, compliance, tax, information technology (IT), operations, and finance departments before it is approved. Each of these departments should carefully consider the possible operational risks that may arise in the development, implementation, and maintenance of the new product.

If the operational risks are beyond the appetite of the firm, then they must be mitigated before the product is launched, or if this is not possible, the product proposal must be shelved.

If a product is approved it is important to ensure there is also a mechanism to ensure that it is monitored. Many products that were at the heart of the recent economic crisis did pass through a new-product approval process. However, they then grew at a rate beyond the expectations of all involved, and the risks were not reassessed at any point.

Risk and control self-assessments (RCSAs) can be useful in monitoring operational risks that arise as a product evolves. Key risk indicators (KRIs) can be attached to products to trigger a reassessment when they reach a particular volume.

SUPPLIER AND THIRD-PARTY RISK

The use of vendors or suppliers and third parties raises unique challenges for operational risk management. While activities and controls may be outsourced, operational risks are not. The firm still owns the risk. Therefore, it is necessary to ensure that there is a robust due diligence process to monitor operational risk management outside the firm.

This can be achieved by requiring vendors to complete RCSAs, to deliver KRI data, and to inform the firm of operational risk events that occur. However, it may be difficult to ensure that such data is being collected to the same standards as the firm is applying internally.

Some firms have amended their service-level agreements (SLAs) with vendors and third parties to require them to provide minimum data to assist with monitoring operational risks. Other firms have determined that these risks cannot be accurately monitored and have focused instead on developing robust contingency plans that can be implemented if the vendor fails. Other firms have spread their operational risk exposure by moving away from a single supplier and engaging several vendors where possible.

The regulatory expectations are high in the area of supplier risk management today. The failures of mortgage servicing companies came as a painful reminder to firms that were using those services that they had not reduced their risks, in fact by handing over the controls they may have increased their risks.

Some firms are selecting to move activities back in house where they feel that they cannot get sufficient assurances through an SLA that controls are being well managed and that risk is not rising.

LEGAL RISK MANAGEMENT

There is often a tension between the operational risk department and the legal department as the operational risk department is promoting transparency, while the legal department is focused on protecting the firm from legal risk exposures.

Legal Considerations in the Operational Risk Framework

This can lead to challenges around reporting loss data, RCSA scores, scenario analysis outcomes and KRIs. Each of these elements of the operational risk framework can be responsible for alerting the firm to risks, and the legal department may be wary of the mitigation burden that this might then place on the firm. If a risk is known and is not mitigated, this could present problems in the future if related litigation was to arise.

It is important for the operational risk department to ensure that the policies and procedures surrounding operational risk identification, assessment, monitoring, control, and mitigation clearly state that there is no expectation that all risks can, or will, be mitigated. The legal department will often be eager to review these policies and procedures to ensure they are clearly worded so as to prevent the inadvertent increase in legal risks.

Capturing Legal Risks Using the Operational Risk Framework

There are legal risks that will be captured in the operational risk program. Legal risk is a subset of operational risk, and therefore any losses related to litigation or legal disputes need to be captured in the operational risk event database, and need to be considered in the RCSA and scenario analysis activities.

This raises additional concerns as the contents of the loss database will be subject to the usual rules of discovery, and so might be requested by an adversary during litigation proceedings. For this reason, many firms provide very little information on legal events, restricting them to a simple description such as "pending litigation" and not completing the loss amount until the case has been settled or all appeals have been exhausted.

Recent developments have led to requirements to include reserve amounts in the loss database and special care needs to be taken with those entries to ensure that privilege is not compromised.

REGULATORY RISK MANAGEMENT

The compliance department is sometimes surprised to find that the operational risk department is interested in its processes, procedures, reporting, and assessments. However, the regular monitoring and management of regulatory risks is an important element in operational risk management and a partnership between the two functions is mutually beneficial.

The operational risk function is often able to find strong KRIs that have been monitored regularly by the compliance department for many years, such as training and registration requirements. The compliance department is able to raise any concerns it has regarding regulatory compliance in a central operational risk forum where they may be appreciated as risks that are beyond the risk appetite of the firm.

The governance structures around regulatory risk may need to evolve in order to ensure that the operational risk reporting and escalation processes and the compliance risk escalation processes are aligned.

PEOPLE RISK MANAGEMENT

People risk arises in all areas of operational risk management. Many controls are dependent on manual processes, and there can be some confusion as to how to capture the underlying people risks such as loss of key personnel, inadequate training, or inadequate cross-training.

These risks will often be raised by participants in an RCSA. However, the risk is not that people will leave or be untrained, but rather that this is a cause for other risks arising. Therefore, there may be a place in the operational risk framework for activities to protect the firm from people risks generally.

As a result, operational risk departments often engage with the human resources or training and development departments to develop programs that will help address firm wide people risk themes. These themes may include:

- A need for training in nondiscriminatory behavior.
- A need for skills training in functional areas.
- A need for cross-training for critical activities.
- A staff survey to monitor KRIs regarding morale.
- Compensation surveys to ensure competitiveness.

The human resources department is understandably reluctant to share people-related data, as it can be highly confidential and sensitive. It may take some time before the operational risk department can develop a relationship

with human resources that will support the production of appropriate KRIs and activities that will mitigate people risks.

FRAUD RISK MANAGEMENT

There may be several activities in the firm that are designed to address fraud risks. The Sarbanes-Oxley Act (SOX) requires a firm-wide fraud risk assessment, compliance departments are tasked with monitoring trading to prevent unauthorized trading, and the operational risk department monitors Internal and External Fraud risk categories.

These activities can be combined to meet all needs. The compliance monitoring activities can be used as inputs into the operational risk RCSA program and the SOX requirements can be met by that same RCSA program.

The Société Général event was discussed at length earlier in Chapter 8 and many lessons were learned and controls improved as a result. Since that event, however, there have been many other fraud scandals that were exposed during the economic crisis, and the recent UBS unauthorized trading scandal is discussed in Chapter 18. Hedge fund frauds, Ponzi schemes, insider trading scandals, and simple theft of funds have all occurred in the last few years. As a result, clients and regulators are raising their expectations regarding fraud risk controls and firms are working to ensure that they have addressed internal and external fraud risks.

There are best practices regarding fraud risk mitigation including robust IT security, effective managerial supervision, and careful monitoring of activities. However, in addition to these controls, it is important to ensure that the culture of the firm is such that employees are aware of fraud risk and are comfortable with responding appropriately when faced with suspicious activity.

Whistle-blower hotlines, anonymous intranet sites, and annual training programs help to ensure that the firm's culture is strongly aligned to protect it against fraudulent activity. The operational risk department should work closely with the human resources department and legal and compliance departments to develop a framework for training, monitoring, and reporting that provides transparency and that supports a culture that resists fraudulent activities from within and from outside the firm.

TECHNOLOGY RISK MANAGEMENT

The reliance of the modern firm on technology also exposes it to serious technology risks. The failure of a critical system, the loss of a network

or a programming error in a vital model can result in catastrophic losses to the firm. The recent case of Knight Capital where they suffered a technology glitch that wiped out the value of the firm is discussed in Chapter 18.

The IT department will engage in technology risk management at a detailed level. They often collect metrics that monitor systems capacity, network outages, bug fixes, and security breaches. These metrics can be KRIs in the operational risk management framework and the operational risk department will have a strong interest in understanding the underlying risks in the technology of the firm, as these represent the causes of events in many risk categories.

Technology solutions are often raised as mitigating actions where high residual risks have been identified in an RCSA or where an IT failure or inadequacy has resulted in a risk event. These mitigating actions can range from simple fixes to extensive firm-wide projects. The operational risk department can partner with the IT department to assist them in prioritizing these activities and assessing the cost benefit of large projects. The potential losses that are identified in the operational risk management program can be very helpful in understanding whether a major strategic IT project should be pursued by the firm.

WEATHER RISK

A weather catastrophe can result in significant operational risk losses. The recent hurricane and tsunami disasters have raised awareness of these risks. While weather cannot be controlled, it can be monitored, and the operational risk department should consider weather risks when working on RCSA and scenario analysis activities. The location of a branch or main office of a firm might significantly elevate the risk of a weather related incident, and the assessment of those risks might lead to a residual risk level that requires mitigation or contingency plans.

Weather risks can impact employees as well as office locations, and some firms have travel tracking programs to ensure that they know the location of their employees, or at least their critical employees, at all times. Employees are required to log their business and personal travel plans in a central database.

For example, these systems resulted in some firms being able to quickly arrange for the retrieval of their personnel from Thailand following the tsunami in 2005. Tracking systems can also be used to track whether there are any employees in areas that are subject to civil unrest and that may need to be extracted in an emergency.

PANDEMIC PLANNING

Business continuity planning (BCP) functions were originally designed to provide controls and procedures that would protect the firm from down time in the event of a loss of power, telecommunications, or access to the buildings.

To respond to these risks, BCP plans were designed to provide robust data backup facilities, alternate work sites, and communications protocols to handle events such as a major power outage, terrorist attack, or weather catastrophe.

Over the last few years, concerns have arisen around the potential impact on the financial services industry of a pandemic, initially due to concerns over the avian flu and more recently the swine flu. Traditional BCP contingency plans are often inadequate in a pandemic as they rely heavily on the use of alternate sites. In a pandemic situation, there would be a requirement for "social distancing," where employees would be unable to work together in close proximity. Also, there would be high level of absenteeism in all industries, and disruptions to the infrastructure and social norms as a result.

This has called for a different approach to continuity planning and operational risk departments have been involved in pandemic planning over the past few years. Pandemic flu exercises were held in the United Kingdom and in the U.S. financial services sectors in recent years and the lessons learned from those exercises are being implemented by operational risk teams and BCP teams across the industry.

A pandemic flu would result in a truly global operational risk event, and the operational risk department in each region will need to address global as well as local considerations in its pandemic preparedness planning.

The following pandemic planning considerations are recommended by the U.S. government[1]:

1. Plan for the impact of a pandemic on your business.
2. Plan for the impact of a pandemic on your employees and customers.
3. Establish policies to be implemented during a pandemic.
4. Allocate resources to protect your employees and customers during a pandemic.
5. Communicate to and educate your employees.
6. Coordinate with external organizations and help your community.

In response to these guidelines many firms have developed sick leave, absenteeism, and travel policies that can be implemented should a serious pandemic occur. They have also acquired medical and cleaning supplies that

can be used as needed, including face masks, hand sanitizers and, in some instances, antiviral medications.

The remote computing capabilities of many firms have been upgraded to support remote log-on by all critical personnel, and calling trees and succession plans have been updated. Critical vendors' pandemic plans have been reviewed for completeness and, if they are found to be lacking, alternate vendors identified.

STRATEGIC RISK

Strategic risk is specifically excluded from the Basel II definition of operational risk, but that does not mean that it is excluded from Basel II consideration nor from operational risk management programs. Basel II has three pillars. Pillar 1 concerns the appropriate calculation of capital for market, credit, and operational risk and outlines some qualitative minimum standards for these risk management categories. Pillar 2 concerns the regulatory oversight that should be put in place to ensure compliance with Pillar 1, and also adds additional requirements to ensure that the firm is protected from risks that may not have been captured in Pillar 1. Pillar 3 refers to the disclosure requirements that firms need to adopt; for example, it outlines how to report on risk management practices and capital in the annual report.

Strategic risk is specifically mentioned in Pillar 2:

> *There are three main areas that might be particularly suited to treatment under Pillar 2: risks considered under Pillar 1 that are not fully captured by the Pillar 1 process (e.g. credit concentration risk); those factors not taken into account by the Pillar 1 process (e.g. interest rate risk in the banking book, business and strategic risk); and factors external to the bank (e.g., business cycle effects).*[2]
>
> *Other risks: Although the Committee recognizes that "other" risks, such as reputational and strategic risk, are not easily measurable, it expects industry to further develop techniques for managing all aspects of these risks.*[3] *[emphasis added]*

Therefore, a firm that wishes to meet Basel II standards is required to consider business and strategic risk in its Pillar 2 framework. A weakness in the Pillar 2 framework can lead to capital penalties (or capital charges) from the firm's regulator. For this reason, some operational risk managers also consider business and strategic risks in their framework, so as to be able to demonstrate to regulators that these risks have been included in the risk

management framework. For example, scenario analysis may be used to address both operational and strategic risks.

They may also use tools from the operational risk framework to help quantify appropriate capital additions for strategic risk, so preempting any regulatory suggestions for additions.

It is difficult to find an agreed definition of strategic or business risk, although the Committee of European Banking Supervisors (CEBS) has provided the following:

> ***Strategic risk:*** *the current or prospective risk to earnings and capital arising from changes in the business environment and from adverse business decisions, improper implementation of decisions or lack of responsiveness to changes in the business environment.*[4]

Managing such risks is challenging and requires a qualitative approach. As the operational risk program contains tools that are designed for managing and measuring qualitative as well as quantitative risk exposures, these tools can be very effective for managing and measuring strategic risk also.

KEY POINTS

- Operational risk management often requires partnership with many related areas in the firm including those that own:
  - New-product approval
  - Vendor, supplier, or third-party management
  - Legal risk
  - Regulatory risk
  - People risk
  - Fraud risk
  - Technology risk
  - Weather risk
  - Pandemic risk
  - Strategic risk

REVIEW QUESTION

1. Which of the following is the best description of the Basel II requirements regarding strategic risk?
   a. There is no regulatory requirement to manage or measure strategic risk.

b. Pillar 2 requires firms to manage and measure strategic risk.
c. Pillar 1 includes strategic risk in the definition of operational risk.
d. The only regulations regarding strategic risk are outside of Basel II rules.

NOTES

1. www.pandemicflu.gov.
2. Bank for International Settlements, "International Convergence of Capital Measurement and Capital Standards: A Revised Framework," 2004, section 724.
3. Ibid., section 742.
4. "Application of the Supervisory Review Process under Pillar 2," CEBS Consultation Paper (CP03 revised), 2005.

CHAPTER 18

Case Studies

In this chapter, we dig deeper into four case studies: JPMorgan Whale, UBS Unauthorized Trading, Knight Capital Technology Glitch, and Standard Chartered Anti–Money Laundering Scandal.

JPMORGAN WHALE: RISKY OR FRISKY?

Are large losses at banks always a sign of poor governance, or are they sometimes merely the realization of losses that were expected, and even planned for, in the well-governed risk management of the firm? In May 2012, JPMorgan announced that it had lost $2 billion (possibly much more), on a hedging strategy that was being driven by Bruno Michel Iksil, aka "The London Whale" in its chief investment office. Was this poor governance, or were these losses predictable under JPMorgan's risk management practices? Was this acceptable risky behavior, or was it frisky misbehavior?

You can't win the game all of the time, and for every winner, there is a loser somewhere in the financial system. For each loss event that happens, we should ask the same question: Were these losses within the boundaries of the bank's known risk, or were they out of control?

We have all heard the worn out caveats "investments may go down as well as up," and we all know that the banking industry sometimes makes money on its risk-taking activities and sometimes loses it on those same activities. So why all the noise in the press about these JPMorgan losses?

- "London Whale Harpooned"[1]
- "JPMorgan's 'Whale' Causes a Splash"[2]
- "Beached London Whale"[3]

Anything over a billion dollars still gets our attention, that's true. But even at that size, the steam should have gone out of the story very quickly if

the loss had just been the result of an unfortunate market movement. That would have been a short-lived and dull story about market risk.[4]

So the question is: was it well-managed risk taking that led to these unfortunate losses, or was there "frisky" behavior in a poorly governed trading desk?

This story had frisky written all over it. Both the *Wall Street Journal*[5] and Bloomberg[6] raised concerns about the size of Iksil's trades earlier in April and hedge funds quickly responded and set about taking the other side of his trades, betting that the Whale's position was outsized and unmanageable. Jamie Dimon, CEO and chairman of JPMorgan, made comments that he certainly now regrets, calling the concerns raised "a complete tempest in a teapot."[7] How was it that outsiders were appropriately concerned about the trading strategy, but the firm itself was not?

Jamie Dimon later admitted,

> *"In hindsight, the new strategy was flawed, complex, poorly reviewed, poorly executed, and poorly monitored. The portfolio has proven to be riskier, more volatile, and less effective as an economic hedge than we thought."*[8]

Even JPMorgan's own risk management tools were not working effectively, as Dimon added:

> *"We are also amending a disclosure in the first quarter press release about CIO's VaR, value at risk. We'd shown average VaR at 67. It will now be 129."*[9]

VaR, or value at risk, is the strongest tool in the risk manager's arsenal, providing an indication of the actual current risk taking of the firm measured against its expected levels of risk taking. If it is flawed, then they are flying blind.

These statements made by the senior management team suggested that they might have first learned of the Whale's positions from press reports. A possibility strengthened by the apparent decision to shut down the trading strategy just four days after it hit the press in April—and shutting it down may well have increased the losses as this caused a sudden change in the market profile of those instruments.

The SEC swiftly opened a review[10] into the accounting practices used by JPMorgan and the Justice Department opened a criminal inquiry[11] into the whole affair. Lawsuits[12] have also sprung up among disgruntled JPMorgan shareholders. Jamie Dimon, recently dubbed "The King of Wall Street," is now battling sustained negative sentiment and watched his stock price take a beating every time more information hits the press. In 11 painful days JPM

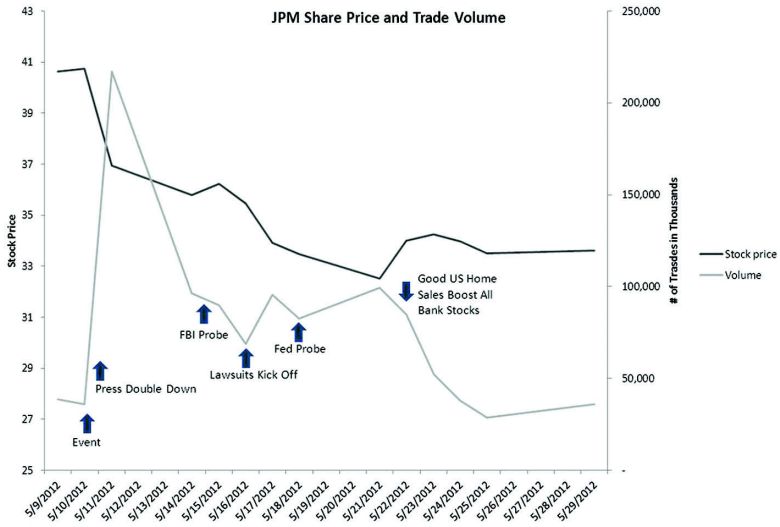

FIGURE 18.1 JPM Share Price and Trade Volume

stock went from 40.64 to 32.51 and only recovered a little when all banks stocks got a boost on news of good U.S. home sales, as shown in Figure 18.1.

Dimon's rhetoric against regulation on Wall Street is now falling on deaf ears as everyone wondered[13] how he let such behavior go unchecked in his own backyard.

Risky or frisky? The positions being taken by the chief information office (CIO) desk were not being accurately captured by the firm's risk management tools, the trading was going on with little or no understanding at the senior management level and the regulators suspect foul play. All this despite the fact that the whole purpose of the CIO desk is to hedge the firm's risk at the highest level and to protect them against large unexpected losses.

This author's verdict: frisky.

JPMorgan released two reports of the event in January, 2102,[14] one by an internal task force, and the other conducted independently by the board. In the task force report, they were transparent about their own failings, as summarized by Bloomberg:

> *In a 129-page report issued yesterday, the bank described an "error prone" risk-modeling system that required employees to cut and paste electronic data to a spreadsheet. Workers inadvertently used the sum of two numbers instead of the average in calculating volatility. The firm also reiterated an assertion that London traders*

initially tried to hide losses that ballooned beyond $6.2 billion in last year's first nine months.[15]

The task force had five key observations:

First, *CIO's judgment, execution and escalation of issues in the first quarter of 2012 were poor, in at least six critical areas:*

(1) CIO management established competing and inconsistent priorities for the Synthetic Credit Portfolio without adequately exploring or understanding how the priorities would be simultaneously addressed;
(2) the trading strategies that were designed in an effort to achieve the various priorities were poorly conceived and not fully understood by CIO management and other CIO personnel who might have been in a position to manage the risks of the Synthetic Credit Portfolio effectively;
(3) CIO management (including CIO's Finance function) failed to obtain robust, detailed reporting on the activity in the Synthetic Credit Portfolio, and/or to otherwise appropriately monitor the traders' activity as closely as they should have;
(4) CIO personnel at all levels failed to adequately respond to and escalate (including to senior Firm management and the Board) concerns that were raised at various points during the trading;
(5) certain of the traders did not show the full extent of the Synthetic Credit Portfolio's losses; and
(6) CIO provided to senior Firm management excessively optimistic and inadequately analyzed estimates of the Synthetic Credit Portfolio's future performance in the days leading up to the April 13 earnings call. …

Second, *the Firm did not ensure that the controls and oversight of CIO evolved commensurately with the increased complexity and risks of CIO's activities. …*

Third, *CIO Risk Management lacked the personnel and structure necessary to manage the risks of the Synthetic Credit Portfolio.*

Fourth, *the risk limits applicable to CIO were not sufficiently granular.*

Fifth, *approval and implementation of the new CIO VaR model for the Synthetic Credit Portfolio in late January 2012 were flawed, and the model as implemented understated the risks presented by the trades in the first quarter of 2012.*[16]

Jamie Dimon, CEO, faced a 50 percent pay cut as a result and many executive team members also saw their compensation significantly impacted.

FIGURE 18.2 ORX Classification of JPMorgan Whale Event

This internal report focuses heavily on what went wrong in the CIO office, but does not clearly state the operational risk categories and causes.

Let us look at the two external data providers that we discussed earlier for their view on this event: ORX News Service[17] (ORX) and IBM Algo FIRST[18] (FIRST). Both provide details on events that have happened in the industry, and offer classifications of the event.

ORX classifies the event as shown in Figure 18.2. They have selected unauthorized trading as the risk category, and inadequate policy/procedure, unauthorized activity and management/control of staff as the three main causes.

FIRST classifies the event as shown in Figure 18.3.

Keywords	
Entity Type	FINANCIAL SERVICES\BANKING\COMMERCIAL/FULL SERVICE BANK
Business Unit Type	TRADING & SALES (BIS)\TRADING
Service/Product Offering Type	DERIVATIVES, STRUCTURED PRODUCTS AND COMMODITIES\DERIVATIVE PRODUCTS\CREDIT DERIVATIVES
Contributory/Control Factors	CORPORATE GOVERNANCE\BOARD OVERSIGHT,CORPORATE/MARKET CONDITIONS\CORPORATE & MARKET CONDITIONS,EMPLOYEE ACTION/INACTION\HUMAN ERRORS,LACK OF CONTROL\FAILURE TO TEST FOR DATA ACCURACY,MANAGEMENT ACTION/INACTION\UNDERTOOK EXCESSIVE RISKS,OMISSIONS\INADEQUATE STRESS TESTING,ORGANIZATIONAL STRUCTURE\ORGANIZATIONAL GAP(S),STAFF SELECTION/COMPENSATION\UNTRAINED/ INEXPERIENCED STAFF,STRATEGY FLAW\STRATEGIC FLAW
Loss Type:	Estimated
Loss Impact	DIRECT LOSS\WRITE-DOWN (BIS)\WRITE-OFFS
Loss Detection Sources	OTHER LOSS DETECTION SOURCES\PRESS DETECTED
Market Focus	INSTITUTIONAL SERVICES
Event Trigger	PROCESS RISK CLASS\TRANSACTIONAL AND BUSINESS PROCESS RISK\INADEQUATE/PROBLEMATIC TRANSACTION EXECUTION
Basel Levels I & II	Execution Delivery and Process Management\Transaction Capture, Execution & Maintenance\Other task misperformance
Basel Business Line	Trading & Sales\Proprietary Positions
Industry Event	
Rules and Regulations	

FIGURE 18.3 FIRST Classification of JPMorgan Whale Event

FIRST has selected execution, delivery, and process management as the risk category, and lists many contributing control factors, also including management, inaction, corporate governance, human errors, and excessive risk taking.

It is important to acknowledge that different interpretations of the Basel II risk categories are common, and external data sources need to be carefully used for this reason.

In the following case studies, you will have an opportunity to read the short descriptions of the event from the perspective of either ORX or FIRST and will determine the appropriate classifications of the risk type and major causes.

REVIEW QUESTIONS

CASE 1: Knight Capital Technology Glitch

Read the ORX description of the Knight Capital technology glitch event below and respond to the questions that follow.

> ***Knight Capital Loses USD 440 Million in Automated Trading System Malfunction***
>
> *Knight Capital Group caused market disruption on 1 August 2012 after a malfunction in newly installed trading software caused the firm to rapidly place millions of erroneous orders into the New York Stock Exchange (NYSE). On 2 August 2012, Knight Capital stated that it had exited the erroneous trading positions, realizing a pre-tax loss of USD 440 million (EUR 361 million) after selling stock it had acquired at inflated prices back into the market at lower prices.*
>
> *The NYSE witnessed high trading volume and large price volatility in around 150 stocks in the first hour after markets opened on 1 August 2012. The NYSE cancelled trades in six of these stocks, reported to be China Cord Blood Corp., American Reprographics, E-House (China) Holdings, Quicksilver Resources, Reaves Utility Income Fund and Wizzard Software.*
>
> *A Knight Capital press release states that following the installation of new trading software, the firm sent "numerous erroneous orders" in equities listed on the NYSE into the market.*
>
> *Large trading volume caused prices of certain stocks to experience very large price fluctuations.*
>
> *Media reports suggest a "rogue" algorithm was to blame for the trades. The Financial Times reports that the trading system at Knight Capital may have executed a large order for a number of stocks over five minutes instead of over a longer period of up to five days. This could have inflated the price of stocks rapidly.*

Knight Capital has said it has removed the new software from its systems and that no clients have been affected.

UPDATE 1 (15 August 2012)—Knight Capital Finds Source of Trading Program Glitch

The trading loss at Knight Capital was caused by disused software which was reactivated after a new program was installed on its system, Bloomberg reports. After being reactivated, a glitch in the out-dated trading system began to multiply stock orders by 1,000. Employees at Knight Capital reportedly looked through eight sets of software before finding what had gone wrong.[19]

1. What level 1 Basel risk category was this event?
2. What was the main cause of this event?
3. What Basel business line did this business event occur in?

CASE 2: Standard Chartered Anti–Money Laundering Scandal

Read the following excerpts from FIRST's record of the Standard Chartered AML event below and respond to the questions that follow.

Short Description[20]

On August 6, 2012, the New York State Department of Finance Services (DFS) filed a court order against Standard Chartered Bank (SCB), alleging that for nine years, from 2001 to 2010, the London-based bank facilitated some 60,000 secret transactions worth $250 billion for Iranian government-controlled entities—including Bank Melli, Bank Saderat, and the Central Bank of Iran/Markazi. The DFS alleged that SCB withheld data from US regulators, falsified its records and wrote an instruction manual for bank staff automating the "stripping" of data from transactions for its Iranian clients. Facing regulatory inquiries, SCB tried to stall US regulators by outsourcing its sanctions-compliance function to Chennai, India. The regulatory complaint cites an email in which SCB personnel warn that the prohibited transactions could cause "catastrophic reputational damage" even as senior management participated in what the regulator terms "flagrantly deceptive actions." The DFS' order asked SCB to show why its New York banking and dollar-clearing licenses should not be revoked. SCB strongly denied the allegations and said that at most $14 million in transactions may have violated regulations in effect at the time. In a settlement announced on August 14, 2012, SCB agreed to pay the DFS $340 million over the Iran transactions, and the

DFS's hearing into the bank's New York license was cancelled. On December 10, 2012, SCB agreed to pay a further $327 million in penalties in a settlement with the US Department of Justice, the Treasury Department's Office of Foreign Assets Control (OFAC) and the Board of Governors of the Federal Reserve System. This brought the total penalties imposed on the bank to $667 million, and ended the federal investigation into SCB's operations in New York, London and Dubai concerning US dollar transactions the bank arranged for Iranian clients as well as other nations under US sanctions restrictions.

Corrective Actions and Management Response

The New York DFS Settlement (August/September 2012).

The New York DFS ordered the bank to show by August 15, 2012, why its New York banking license should not be revoked and its dollar-clearing licenses should not be suspended. The regulator also sought unspecified penalties and asked to have an independent monitor named to supervise the bank's operations in New York. In a statement, SCB said it "strongly rejects the position or the portrayal of facts as set out in the order" and that it was currently reviewing its compliance procedures. The bank said that 99.9% of its Iranian U-turn transactions complied with regulations, and that at most $14 million in transactions may have violated U-turn rules. SCB added that it had never identified any client tied to a terrorist entity or organization, and that it ceased doing business with Iranian customers more than five years earlier. No details on the $14 million in SCB transactions that the bank said may have violated U-Turn rules had been made public as of August 15, 2012.

The DFS' order was apparently brought without any coordination with federal officials, such as the US Treasury or the Department of Justice. The New York regulator's actions also created a strong pushback in London. Mervyn King, Governor of the Bank of England, complained that regulators had not completed their investigations: "I think all the UK authorities would ask is that the various regulatory bodies that are investigating the particular case try to work together and refrain from making too many public statements until the investigation is completed," Mr. King said. Others in London were even more vociferous, some claiming that regulators in the United States were picking fights with British banks.

Peter Sands, the bank's CEO, flew to New York for negotiations with regulators several days before the scheduled fitness hearing

at the DFS. On the afternoon of August 14, 2012, a settlement was announced under which the bank agreed to pay the regulator $340 million over the questionable Iran transactions. The regulator's hearing into the bank's license in New York was cancelled. SCB also agreed to have a monitor named by the DFS at the bank to vet its compliance with AML controls. The DFS' announcement said that: "The parties have agreed that the conduct at issue involved transactions of at least $250 billion." The bank issued a brief statement saying a fuller description of the agreement terms "is expected to be concluded shortly" while the bank "continues to engage constructively with the other relevant U.S. authorities."

Settlement with US Department of Justice, Treasury, Federal Reserve Board (December 2012)

On December 10, 2012, Standard Chartered agreed to pay a further $327 million in penalties in a settlement with several federal regulators, including under US Department of Justice, the Treasury Department's Office of Foreign Assets Control (OFAC) and the Board of Governors of the Federal Reserve System. The New York County District Attorney's office was also a party to the agreement.

Under the deferred prosecution agreement (DPA) with the US Department of Justice, Standard Chartered agreed to forfeit $227 million for violations of the International Emergency Powers Act (IEEPA). The Federal Reserve Board also imposed a $100 million penalty relating to sanctions and AML violations. The Treasury Department's OFAC also issued a statement to the effect that Standard Chartered had agreed to forfeit profits for violations of sanctions orders against regimes in Iran, Sudan, Burma, and Libya. (The sanctions against the last two nations have since been lifted. OFAC also cited eight violations of the Foreign Narcotic Kingpin Sanctions Regulations as being included in the settlement.

Standard Chartered said, "The settlements are the product of an extensive internal investigation that led the bank voluntarily to report its findings concerning past sanctions compliance to these U.S. authorities, and nearly three years of intensive cooperation with regulators and prosecutors."

Lessons Learned

There was a wide discrepancy of scale between the conduct alleged by the DFS – some 60,000 Iranian transactions with a value of $250 billion – and the conduct admitted by Standard Chartered—a few hundred transactions valued at no more than $14 million. On August 15, 2012, the New York Times reported. "The size of the

settlement [$340 million] is puzzling to some officials, including the Justice Department, because there is still widespread disagreement about the extent of the bank's wrongdoing." The amount was "far more than the $5 million the bank had been willing to pay a year earlier," the paper said. For its part, the Wall Street Journal said the penalty was "manageable" given that the bank generated nearly $4 billion in profit in the first half of 2012.

Several press reports saw reputational risk as a key factor in this case, which may have encouraged the bank to settle. Even if the bank's conduct complied with the letter of US regulations in effect at the time, any suggestion that senior personnel condoned the concealment of transactions that should have been reported could be problematic. A former SCB executive who left the bank in 2006 told the Wall Street Journal (August 7, 2012) that US rules in May 2006 were "unclear" and that "many international banks active in Iran were trying to adjust to increased attention from the U.S. There was a lack of clarity over what was and wasn't allowed. The key question was to try and understand exactly what counted as a U-turn transaction," he said.

News of the second Standard Chartered settlement on December 10, 2012 were somewhat overshadowed the next day, when an even larger settlement was announced between federal regulators and another British bank, HSBC (#12045), as well as news of arrests in London in ongoing investigations into the alleged fixing of LIBOR.

4. What Basel risk category does this event fall under?
5. Discuss the actions of the various regulators, do they all seem reasonable?
6. What was the most important lesson learned? Discuss.

Case 3: The UBS Unauthorized Trading Scandal

Read the following excerpts in Figure 18.4 and 18.5 from ORX's and FIRST's records of the UBS event below and respond to the questions that follow.

ORX Record and Description[21]

UPDATE 2 (26 November 2012)—UK FSA Fines UBS Million GBP 29.7 Million

UBS has been fined GBP 29.7 million (USD 47.6 million, EUR 36.7 million) by the Financial Services Authority over the 2011 rogue trading incident. The regulator found ineffective systems and

FIGURE 18.4 ORX Case File on UBS Trading Scandal

controls and inadequate supervision of the synthetic equities desk at UBS allowed Adoboli to cause the unauthorized trading losses.

Though it does not have the power to levy fines, the Swiss Financial Market Supervisory Authority (FINMA) jointly published the findings of its investigation, and has stated it will be appointing an independent investigator to ensure that UBS implements various corrective measures.

On 15 September 2011, UBS reported a loss due to unauthorized trading "in the range of USD 2 billion." This figure was revised to USD 2.3 billion (EUR 1.7 billion) on 18 September 2011 when the bank released a statement providing further details into the rogue trading loss.

The trades were carried out at UBS' Global Synthetic Equity business in the City of London. The losses derived from what the bank called "unauthorized speculative trading" in equity index futures. Whilst the positions taken were within "normal business flow of a large global equity trading house," the trader used fictitious hedges to obscure the fact that risk limits had been violated. The bank stated the positions had been offset with "fictitious, forward-settling, cash ETF positions."

City of London police have arrested and charged trader Kweku Adoboli with fraud by abuse of position and false accounting. UBS stated that the trader had revealed his actions to the bank on 14 September 2011. It has been reported that Adoboli was a market maker in Exchange Traded Funds (ETFs), working on the "Delta 1" trading desk, which replicates stock indices through derivatives such

as swaps, futures and options. This is the same desk as Jérôme Kerviel worked on at Société Générale when he famously lost the bank approximately EUR 4.9 billion through falsely hedging large trades.

Appearing in court on 22 September 2011, Adoboli was also charged with fraud between October 2008 and December 2010. Prosecutors referred to "reckless and inappropriate" trades between these dates.

UBS board member David Sidwell has been appointed to begin an internal investigation into the trading loss. The FSA and its Swiss counterpart FINMA have both stated that they will investigate the loss.

UBS said that no client positions had been affected by the loss.

UPDATE 1 (20 November 2012)—Adoboli Convicted of Fraud

Kweku Adoboli has been sentenced to seven years in prison after being found guilty on two counts of fraud by abuse of position. The jury acquitted Adoboli of four counts of false accounting.

FIRST Record and Excerpts from Description[22]

Keywords	
Entity Type	FINANCIAL SERVICES\BANKING\COMMERCIAL/FULL SERVICE BANK
Business Unit Type	TRADING & SALES (BIS)\TRADING
Service/Product Offering Type	TRADING CATEGORIES\PROPRIETARY TRADING
Contributory/Control Factors	CORPORATE GOVERNANCE\GENERAL CORPORATE GOVERNANCE ISSUES,CORPORATE/MARKET CONDITIONS\CORPORATE & MARKET CONDITIONS,CORPORATE/MARKET CONDITIONS\REGULATORY PRESSURE,EMPLOYEE ACTION/INACTION\EMPLOYEE MISDEEDS,LACK OF CONTROL\FAILURE TO QUESTION ABOVE MARKET RETURNS,LACK OF CONTROL\FAILURE TO TEST FOR P/L ACCURACY,LACK OF CONTROL\LACK OF INTERNAL CONTROLS,LACK OF CONTROL\POOR DOCUMENTATION,LACK OF CONTROL\RULES, REGULATIONS & COMPLIANCE ISSUES,MANAGEMENT ACTION/INACTION\LACK MANAGEMENT ESCALATION PROCESS,MANAGEMENT ACTION/INACTION\POOR EXECUTION,MANAGEMENT ACTION/INACTION\POOR JUDGMENT,OMISSIONS\FAILURE TO COMPLY WITH INTERNAL POLICIES AND PROCEDURES,OMISSIONS\FAILURE TO SET OR ENFORCE PROPER LIMITS,OMISSIONS\FAILURE TO SUPERVISE EMPLOYEES,OMISSIONS\FAILURE TO TEST PRODUCTS OR SYSTEMS,OMISSIONS\INADEQUATE DUE DILIGENCE EFFORTS,OMISSIONS\LACK OF PROPER TRAINING PROCEDURES,OMISSIONS\OMISSIONS & LAPSES,OMISSIONS\OUTSOURCING,ORGANIZATIONAL STRUCTURE\UNCLEAR REPORTING STRUCTURE,STAFF SELECTION/COMPENSATION\UNTRAINED/ INEXPERIENCED STAFF
Loss Type:	Known
Loss Impact	DIRECT LOSS\REGULATORY/COMPLIANCE/TAXATION PENALTY (BIS)\FINES/PENALTIES,DIRECT LOSS\REGULATORY/COMPLIANCE/TAXATION PENALTY (BIS)\REGULATORY-ORDERED CHARGE TO CAPITAL RESERVES,DIRECT LOSS\WRITE-DOWN (BIS)\WRITE-DOWNS,INDIRECT LOSS\MANAGEMENT REMEDIATION,INDIRECT LOSS\REPUTATIONAL (NON-MONETARY),INDIRECT LOSS\SHARE PRICE
Loss Detection Sources	PERIODIC INTERNAL REVIEWS\BACK OFFICE REVIEWS
Market Focus	INSTITUTIONAL SERVICES
Event Trigger	PEOPLE RISK CLASS\TRADING MISDEEDS\UNAUTHORIZED TRADING/ACTIVITY ABOVE LIMITS\UNAUTHORIZED TRADING -- PROPRIETARY ACCOUNTS
Basel Levels I & II	Internal Fraud\Unauthorised Activity\Trans type unauthorized (w/monetary loss)
Basel Business Line	Trading & Sales\Proprietary Positions
Industry Event	
Rules and Regulations	European Jurisdictions\United Kingdom Jurisdiction\Financial Services Authority\The FSA Handbook\High Level Standards\Principles for Businesses\Principle 2 - Skill, care and diligence,European Jurisdictions\United Kingdom Jurisdiction\Financial Services Authority\The FSA Handbook\High Level Standards\Principles for Businesses\Principle 3 - Management and control

FIGURE 18.5 First Summary of UBS Trading Scandal

Control Failings and Contributory Factors

Employee Misdeeds: *A 31-year-old trader in the European Equities Trading Division at UBS' London offices was arrested after the bank discovered he had engaged in unauthorized trades. The employee executed transactions for the bank's account in excess of his defined limits and concealed the risk exposures. Using a variety of methods, he successfully concealed the actual scale of his trading positions and the risk they posed. The methods used included one-sided internal futures positions, the delayed booking of transactions and fictitious deals with deferred settlement dates (T+14).*

Corporate and Market Conditions: *Mr. Adoboli made a series of bets on market indices at times when markets were very volatile, due to concerns about Greek sovereign debt and other economic difficulties. "He managed to change his position always at the wrong time," an unidentified source told the Wall Street Journal (September 20, 2011). Shortly before UBS disclosed the loss, equity markets had been very volatile, due in part to concerns about a possible sovereign default by Greece, a Euro-zone member. To curb what it called "massive overvaluation" of the Swiss Franc, the Swiss National Bank intervened on September 6, 2011 to cap the exchange rate of the CHF against the Euro, a surprise move that led to losses for some hedge funds. Although some have speculated about the possible impact of the SNB's intervention, it is not known whether such externalities contributed to the loss at UBS—or whether it turned a manageable loss into a much larger one.*

Failure to Test for P/L Accuracy; *Lack Management Escalation Process: Profit and loss suspensions to the value of USD $1.6 billion were requested by Adoboli during August 2011. Prior to 18 August 2011, these were accepted without challenge or escalation. The combined factors of unexplained profitability and loss suspensions should have indicated the need for greater scrutiny.*

Lack of Internal Controls: *The front office's monitoring tools established by the line manager responsible for the ETF desk had major deficiencies and were not used properly. The trade capture and processing system had significant flaws, which Adoboli exploited to conceal his unauthorized trading. The system permitted trades to be booked to an internal counterparty without sufficient details; there were no effective methods to detect trades at material off-market prices; and there was a lack of integration between systems. UBS' various control functions did not assemble their information to produce an overall picture. Fulvio Pelli, the party president of the Swiss Liberal Party, commented: "For a bank that has made mistakes in*

the past, it's absolutely unacceptable. I'm absolutely astonished that internal controls didn't work at UBS."

Poor Judgment: *Operational risks were assessed mainly through a yearly self-assessment process by traders and internal controllers. Improvements to this process had been in progress since January 2011, but came completed too late, according to Swiss regulator, the Financial Market Supervisory Authority (FINMA), which was working on an independent investigation of this incident with the FSA.*

Inadequate Due Diligence Efforts: *Untrained/Inexperienced Staff: The regulators found that there was an perception amongst personnel supporting the ETF desk that the Operations Division's main role was that of facilitation. Their focus was on efficiency rather than risk control and they did not sufficiently question the front office about its actions. The control functions had insufficient understanding of the trading activities in question and were therefore unable to challenge the ETF desk's actions. Operations saw its role as providing services to Adoboli and raised no serious questions about his activities. Although reconciliation errors remained unresolved over several weeks, explanations provided were far-fetched, and inconsistencies were seldom escalated, Adoboli's managers and controllers were too quick to accept his explanations. Even at a meeting held on August 24, 2011, managers came to the conclusion that no large amounts of money were at risk. In August 2011, Adoboli once again persuaded Product Control that losses of one billion dollars shown in the trading systems were incorrect. His assurance that he would correct these "booking errors" in the near future was accepted without objection. In fact, Adoboli's objective was to eliminate the bank's losses, at least temporarily, from the books.*

Poor Documentation: *An important control report was not produced at all for a period of several months without anyone noticing. This report is described below, under Outsourcing.*

Lack of Proper Training Procedures: *FINMA found that control personnel "had too little understanding of the trading activities in question and were therefore unable to challenge the ETF desk's actions." Moreover, the various control functions at UBS "did not collate their information to produce an overall picture." This was due in part to the outsourcing of control functions, as well as unclear reporting lines.*

Outsourcing: *The Times of India (November 26, 2012) noted that a key internal control for detecting fraud had been moved to*

India. This function, known as the T+14 report, was maintained by an outsourcing provider, which FINMA did not identify. The T+14 report was designed to identify deferred settlement trades, which posed a greater risk to the firm than trades which settled in three business days (T+3 trades). According to FINMA, the T+14 Report, "was non-operational between May and November 2009, and from November 2010 to September 2011"—shortly before the loss was discovered. If it had been operational it should have flagged the trader's fictitious deals with deferred settlement dates created by Trader X.

Poor Execution: *FINMA found that unclear reporting lines were a key factor: "Line managers were uncertain of their functions and responsibilities" as to who was monitoring the ETF desk. After an internal reorganization in April 2011, the direct line manager for the ETF desk was located in New York, but "no specific arrangements were made for transferring responsibility for monitoring [the desk]." Therefore, warnings did not reach the new direct line manager in New York. They ended up instead with the previous line manager in London, who received and acknowledged them, even though this was no longer his responsibility."*

Unclear Reporting Structure: *At UBS, responsibility for monitoring and controlling the ETF desk was divided between the line managers in the front office and three separate control functions. The Operations unit was charged with ensuring that the ETF desk's trades were correctly logged and processed. Product Control were tasked with ensuring correct reporting and for checking the plausibility of profits and losses, while Risk Control was responsible for monitoring and evaluating the risks from trading activities. Line managers were uncertain of what their functions and responsibilities were as regards monitoring the ETF desk.*

Unclear Reporting Structure (more): *Failure to Question Above Market Returns: FINMA and the FSA determined that the three control functions had failed to properly investigate the many red flags triggered by transactions from the ETF desk. FINMA pointed to one example, where unusually large profits generated by the ETF desk starting in the first quarter of 2011 were not critically scrutinized. The regulator said that the bank failed to examine the underlying reasons for the significant growth in profitability of the ETF desk despite the fact that this could not be explained by reference to the end of day risk positions.*

Failure to Supervise Employees: *At UBS' London offices, the manager of the alleged rogue trader resigned shortly after the trader*

was arrested. Some banks have reportedly urged supervisory staff to be aware of potential risks posed by traders who may have direct knowledge of "back-office" systems and urged them to give those employees heightened supervision. FINMA found that the direct line managers failed to properly monitor the ETF desk in London. Adoboli's relationship with his line manager and the internal control functions relied on trust and not enough on control. The FSA criticized that bank for having inadequate front office supervision. It stated that the supervision arrangements within the Global Synthetic Equities (GSE) trading division, of which the ETF desk was part, were poorly executed and ineffective.

Failure to Set or Enforce Proper Limits: *Although UBS' London trading room was aware that the ETF desk caused many reconciliation errors, often due to late or incorrectly booked transactions, these concerns were not discussed with either the Product Control unit nor with senior management. Starting in June 2011, the reconciliation errors became substantial, with the unexplained amounts sometimes exceeding USD 1 billion. Between June and July 2011, it became clear on at least four occasions that Adobeli had breached his limits. In one case, he revealed to his manager in New York that he had made a profit of USD $6 million by taking a position of more than USD $200 million, far in excess of his approved risk limit. The line manager first congratulated Adoboli on the profit and only later reminded him that he needed permission to exceed his limit. The inadequacy of the controls was also made clear by an incident in August 2011 in which fictitious ETF trades with deferred settlement dates generated irregularities amounting to half a billion dollars. These warning signals were accepted without further investigation. The ETF Desk breached the risk limits set for their desk without being disciplined for doing so. These limits represented a key control and defined the maximum level of risk that the desk could enter into at a given time. This brought about a situation in which unauthorized risk taking was not actively discouraged or penalized by those with supervisory responsibility. According to FINMA, UBS sent out misleading signals by "awarding pay increases and bonuses to a trader who had clearly and repeatedly breached compliance rules, and by accepting him onto a junior management program."*

General Corporate Governance Issues: *Failure to Comply with Internal Policies and Procedures; Staff Selection/Compensation: UBS awarded pay increases and bonuses to Adoboli who had clearly and repeatedly breached compliance rules, and by accepting him onto a junior management scheme.*

Omissions & Lapses; Regulatory Pressure: Reuters reported that the European Union's MiFiD regulations do not currently require the reporting of confirmations from counterparties for over-the-counter (bank-to-bank) ETF transactions until after the settlement date. This would appear to be a major loophole in MiFiD's current reporting requirements.

Failure to Test Products or Systems: *Although ETFs have been in use for a few years, banks are now using them to hedge their own positions. The risks posed by ETFs remain poorly understood, one analyst told Reuters News (September 20, 2011): "There hasn't been the investment in systems to keep up with the complexity of [ETFs]. When new trading products emerge, often the links to risk and credit controls are an afterthought."*

Rules, Regulations and Compliance Issues: *UBS breached FSA Principles 2 (due skill, care and diligence) and 3 (risk management systems and controls) of the FSA's Principles for Businesses.*

7. What lessons had UBS not learned from the Société Générale case from only a few years earlier? Discuss. (See Chapter 8 for a discussion of the Société Générale event.)

NOTES

1. www.forbes.com/sites/nathanvardi/2012/05/16/london-whale-harpooned-iksil-out-at-jpmorgan/.
2. www.ft.com/cms/s/0/fbab63ae-9b72-11e1-b097-00144feabdc0.html#axzz1×77Fp2ct.
3. http://news.yahoo.com/beached-london-whale-loses-2-billion-j-p-213300751–finance.html.
4. For example, www.bloomberg.com/news/2012-06-06/paulson-gold-fund-said-to-extend-slump-with-13-may-loss.html.
5. http://blogs.wsj.com/deals/2012/04/06/deals-of-the-day-meet-j-p-morgans-london-whale/?KEYWORDS=jp+morgan+whale.
6. www.bloomberg.com/news/2012-04-09/london-s-biggest-whale.html.
7. www.reuters.com/article/2012/05/18/us-jpmorgan-crisiscommunications-idUSBRE84H05G20120518.
8. http://blogs.wsj.com/deals/2012/05/10/whale-of-a-call-dimons-best-quotes/.
9. http://i.mktw.net/_newsimages/pdf/jpm-conference-call.pdf.
10. www.nypost.com/p/news/business/jpmorgan_trading_loss_leads_to_us_JYULwjSYhaCot9ZrdoakUM.

11. http://online.wsj.com/article/SB10001424052702304192704577406093989791910.html.
12. http://business.time.com/2012/05/17/jpmorgans-london-whale-loss-rises-to-3-billion-as-lawsuits-fly/.
13. www.investorplace.com/2012/05/so-jamie-dimon-what-do-you-think-of-the-volcker-rule-now/.
14. Report of JPMorgan Chase & Co. Management Task Force Regarding 2012 CIO Losses (JPMorgan Report), January 16, 2012. Available at http://media.bloomberg.com/bb/avfile/rM8QB5s4.Eoc.
15. www.bloomberg.com/news/2013-01-16/jpmorgan-halves-dimon-pay-says-ceo-responsible-for-lapses-1-.html.
16. JPMorgan Report, extracts from pp. 10–13.
17. www.orx.org/orxnews.
18. IBM Algo FIRST for Web Edition on Cloud.
19. ORX News Reference 0734.
20. FIRST Report for Loss Event 11885/OpData Id 17195.
21. ORX News Reference 0012.
22. FIRST Report for Loss Event 11117/OpData Id 15887.

APPENDIX

Answers to Review Questions

CHAPTER 1

1. c
2. a

CHAPTER 2

1. a
2. d

CHAPTER 3

1. c
2. b

CHAPTER 4

1. b
2. b

CHAPTER 5

1. b

CHAPTER 6

1. c

CHAPTER 7

1. c
2. b
3. e
4. d

CHAPTER 8

1. d

CHAPTER 9

1. b

CHAPTER 10

1. a

CHAPTER 11

1. c
2. a

CHAPTER 12

1. a

CHAPTER 13

1. c

CHAPTER 14

1. a

CHAPTER 15

1. d

CHAPTER 16

1. c

CHAPTER 17

1. b

CHAPTER 18

Case 1

ORX classified the event as outlined in Figure A.1:

FIGURE A.1 ORX Classification of Knight Capital Event

1. In the ORX standards, EL0601—Technology and infrastructure failure is a risk that relates to losses arising from disruption of business or system failures. This is equivalent to the Basel II risk category of **Business Disruption and System Failure.**
2. ORX states the main cause as CS0503—**Software—Inadequate Maintenance.**
3. ORX classify the business line as BL0201—Equities, which is a subset of their **Trading and Sales** business line category.

Case 2

FIRST classified the Standard Chartered event as shown in Figure A.2:

Keywords	
Entity Type	FINANCIAL SERVICES\BANKING\COMMERCIAL/FULL SERVICE BANK
Business Unit Type	PAYMENT AND SETTLEMENT (BIS)\PROCESSING/CLEARING SERVICES\CASH CLEARING BUSINESS
Service/Product Offering Type	CLEARING SERVICES\CLEARING SERVICES (MISC.)
Contributory/Control Factors	CORPORATE GOVERNANCE\GENERAL CORPORATE GOVERNANCE ISSUES,CORPORATE/MARKET CONDITIONS\REGULATORY PRESSURE,EMPLOYEE ACTION/INACTION\EMPLOYEE ACTIONS & INACTIONS,LACK OF CONTROL\FAILURE TO DISCLOSE,LACK OF CONTROL\FAILURE TO TEST FOR DATA ACCURACY,LACK OF CONTROL\LACK OF INTERNAL CONTROLS,LACK OF CONTROL\RULES, REGULATIONS & COMPLIANCE ISSUES,MANAGEMENT ACTION/INACTION\LACK MANAGEMENT ESCALATION PROCESS,MANAGEMENT ACTION/INACTION\POOR JUDGMENT,OMISSIONS\OUTSOURCING,ORGANIZATIONAL STRUCTURE\SLOW REACTION TO MANDATE(S)
Loss Type:	Known
Loss Impact	DIRECT LOSS\LEGAL LIABILITY (BIS)\LEGAL JUDGMENTS (CIVIL CHARGES),DIRECT LOSS\LEGAL LIABILITY (BIS)\SETTLEMENTS,DIRECT LOSS\REGULATORY/COMPLIANCE/TAXATION PENALTY (BIS)\FINES/PENALTIES,INDIRECT LOSS\EXTRA EXPENSE,INDIRECT LOSS\REPUTATIONAL (NON-MONETARY),INDIRECT LOSS\SHARE PRICE
Loss Detection Sources	WHISTLE BLOWING\REGULATORY ORIGINATED
Market Focus	INSTITUTIONAL SERVICES
Event Trigger	PEOPLE RISK CLASS\INTERNAL FRAUD\CASH RELATED FRAUD\MONEY LAUNDERING
Basel Levels I & II	Clients Products and Business Practices\Improper Business or Market Practices\Money laundering
Basel Business Line	Payment and Settlement\External Clients

FIGURE A.2 FIRST Classification of Standard Chartered Event

4. FIRST classified this as an Execution, Delivery, and Process Management event.

5/6. FIRST provided helpful details on the event and the lessons learned. The full text of the event in FIRST is significantly longer than the excerpt provided.

Case 3

7. FIRST provides the following suggested lessons learned, many are repeats of exactly the same control failings as were identified in the Société Générale case.

Lessons Learned

The Wall Street Journal on September 16, 2011 said that banks seeking to detect unauthorized trading should supplement their routine electronic surveillance with "an older method of detection: looking out for suspicious behavior." Echoing some findings of the Societe Generale investigation, the WSJ cited several red flags: "traders not taking vacations; traders having a lot of cancelled or amended trades; traders working out of business hours or logging fewer hours on recorded lines; and traders whose trades are questioned by counterparties or exchanges." The size of the loss in this case certainly poses a reputational risk to UBS. In the words of a

Financial Times (September 15, 2011) report, "Hard questions need to be asked about UBS' internal risk controls. It's hard to believe the Swiss bank's view that it cannot identify the area in which the rogue trades were made, or when more information might become available—everything has an electronic audit trail."

The loss amount ($2.3 billion) is the largest rogue trading loss ever by a Swiss bank and the third-largest unauthorized trading loss on record, exceeded only by the January 2008 Societe Generale loss of $6.8 billion (Event #7945) and the 1996 Sumitomo Corporation loss of $2.8 billion (Event #1699). These and other cases can be found using the Unauthorized Trading keyword.

Nor is this the first time that the London offices of UBS have suffered from unauthorized trading. In November 2009, the FSA fined UBS GBP 8 million ($13.3 million)—one of the FSA's biggest fines ever—for weak controls that allowed staff to make as many as 50 unauthorized trades a day on at least 39 client accounts and then conceal the losses. (see Event #9481)

The Wall Street Journal *reported on September 22, 2011, that the FSA was looking into several possible rogue trading cases at other institutions in London. "At least three of those cases involve traders who previously had worked in the bank's 'back-offices' where employees enter and confirm trades, handle accounting issues and transmit payments," the paper said. After the Societe Generale fraud, some banks reportedly began asking supervisors of traders who come from a "back-office" background to enhance their supervision. Since the FSA does not have sufficient staff to monitor trades at large banks however, it is incumbent on banks to be aware of risky trades before large losses are found to have occurred. Traders exceeding their risk limits can (at least in theory) return profits, so banks should pay attention to unexpectedly large profits before they are surprised by unexpectedly large losses.*

One of the key questions to be answered by any investigation is how such a large unauthorized trading loss on the "Delta One" desk went undetected, especially after the highly-publicized Societe Generale fraud. Since it appears that Mr. Adoboli's losses were in market index futures (as was the case with trades executed by Jerome Kerviel) it is as yet unclear why his fictitious hedging positions went unchecked. At the very least banks should require confirmations of ETF trades by counterparties.

At least one online analyst, Paul Amery, argues that lax operational settlement procedures for bank-traded ETFs could prove to be a major factor. Firstly, in London the late settlement of ETF

transactions is not unusual and is not subject to major sanctions. Secondly, many counterparties do not request trade confirmations, especially for OTC transactions. Mr. Amery concludes: "Taken together, these two loopholes may have enabled the creation of fake transactions in UBS's systems. Even if this was the immediate cause of the fraud, the bank's risk controllers seem to have missed other warning signs. High gross trading positions, even if the trader reported his position as hedged, plus what were presumably significant cash outflows in margin as the result of losing futures positions, might together have been expected to flag that something was wrong."

The Financial Times *reporter Gillian Tett noted that trading in ETFs requires yet more attention from regulators, since sales of ETFs—which have been very profitable for banks—could pose conflict-of-interest problems if banks were acting as counterparties in the same funds they sold to customers.*

A few weeks before it disclosed the loss, UBS had announced a plan for 3,500 layoffs—a 5 percent cut in its global work force—half of them in the investment banking arm, in order to meet tougher economic conditions. Press reports said that the loss would also lead to calls from investors and legislators for Swiss banks to reduce their investment banking activities and focus more on private banking and fund management. Regulators could ask for even more stringent capital requirements for investment banking activities, or seek to protect client business from risky proprietary trading.

The Swiss parliament was discussing measures to improve the safety of the biggest Swiss banks (UBS and Credit Suisse) even as the event was disclosed. The "too big- to-fail" banks earlier got taxpayer bailouts after losing large amounts investing in mortgage-backed securities from 2006 to 2008. A representative of the Swiss People's Party (SPP) told Bloomberg News: "There can't be another state bailout. It can't be up to the state and taxpayers to rescue large banks that are involved in risky business." Another SPP member found yet another lesson: "It shows that investment banking is a high-risk field and it's important that we clearly separate systemically important functions from the rest of the banking business." Such concerns have also been echoed elsewhere.

The proposal to "ring-fence" bank activities on their customers' behalf from risky bets in proprietary trading was a feature both of the Volcker rule (enacted as part of the Dodd Frank Act) in the United States, as well as the recent Vickers Report (available here) into banking in the United Kingdom. Proponents of stricter

banking regulation in these and other countries will likely to point to the UBS case to bolster their argument. As Martin Wolf, a columnist for the Financial Times wrote: "Thank you UBS . . . I could not have asked for a better illustration of the unregulatable risks to which investment banks are exposed."

In what may be an emerging trend, the Swiss regulator FINMA noted in its summary report that outsourcing of control functions to India was a contributing factor in UBS' failure to detect unauthorized trading. Such outsourcing has also been mentioned in another high-profile case. In August 2012, the New York Department of Financial Services accused Standard Chartered of involvement in laundering financial transactions (11885). The regulator said the bank's compliance function had been moved to Chennai. The New York regulator cited "no evidence of any oversight or communication between the Chennai and the New York offices" with regard to Standard Chartered's compliance with regulations issued by the Office of Foreign Assets Control (OFAC).

About the Author

Philippa Girling has 18 years' experience in the global securities industry, working in the fields of operational risk, training, project management, and organizational change.

Philippa has held several operational risk leadership roles, including heading the global corporate operational risk functions at Morgan Stanley and Nomura. She is currently the business chief risk officer for Capital One's commercial bank.

She has delivered the Operational Risk Executive Education program at Columbia University, New York City, for the past four years, as well as leading operational risk education sessions for London Business School, Rutgers University, University of Connecticut, and Carnegie Mellon.

Philippa authored *Operational Risk Management,* a textbook for the risk and regulation examination of the Global Association of Risk Professionals in 2009.

She is a regular speaker at global conferences on the topics of Dodd-Frank, systemic risk and regulation, and the evolution of the operational risk discipline, and was selected as one of the Top Fifty Faces of Operational Risk by *Operational Risk and Compliance* magazine.

Philippa holds an English law degree from the University of East Anglia, England, and is a member of the New York Bar. She is a holder of the GARP Financial Risk Manager accreditation and is a doctoral candidate at Rutgers University, her area of study focusing on the development of an industry standard operational risk framework that meets global regulatory expectations and financial services industry business requirements.

Philippa moved from her British homeland to the United States in 1996 and now lives in New Jersey with her husband and daughters.

About the Website

The companion website for this book contains teaching slides and materials and a simple operational risk toolbox. Go to www.wiley.com/go/girling (password: wiley13) for access to the following materials:

- PowerPoint slides to support each chapter.
- A fictional case study with instructions for use as a teaching exercise for groups.

The toolbox contains the following items:

- A PowerPoint training presentation that introduces operational risk concepts and fundamentals.
- A simple risk and control self-assessment Excel worksheet with built-in automatic conditional formatting, drop-down risk category lists, and scoring calculations.
- A basic loss event data collection Excel worksheet with standard fields for data capture and one example event.
- A starter kit of key risk indicators in an Excel worksheet with example metrics for each of the seven Basel risk categories of operational risk.
- A sample reporting deck in PowerPoint with examples of operational risk reporting slides and with supporting sample data in Excel.
- An operational risk policy document in Word.
- A loss data standards document in Word.

The site also features links to all of the reference materials in this book.

Index

S