

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 STUDY⁷

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 'Honey-pot' 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.

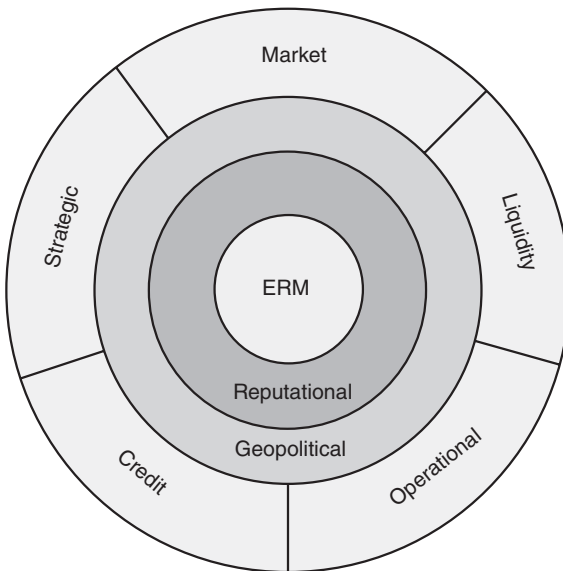


FIGURE 1.1 Enterprise Risk Management Wheel

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-honey-pot-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#11ptQC1VdfjCF9xS.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.