2025 FRM®
Exam Prep

SchweserNotes™
Operational Risk and Resilience

Part II Book 3

KAPLAN SCHWESER

Book 3: Operational Risk and Resilience

SchweserNotes™ 2025

FRM Part II

KAPLAN SCHWESER

SCHWESERNOTES™ 2025 FRM® PART II BOOK 3: OPERATIONAL RISK AND RESILIENCE

Published in 2025 by Kaplan, Inc.

ISBN: 978-1-0788-4955-5

CONTENTS

READING 46

Risk Mitigation

READING 47

Risk Reporting

READING 48

Integrated Risk Management

STUDY SESSION 8—Operational Risk Focus Areas

READING 49

Cyber-Resilience: Range of Practices

READING 50

Case Study: Cyberthreats and Information Security Risks

READING 51

Sound Management of Risks Related to Money Laundering and Financing of Terrorism

READING 52

Case Study: Financial Crime and Fraud

READING 53

Guidance on Managing Outsourcing Risk

READING 54

Case Study: Third-Party Risk Management

READING 55

Case Study: Investor Protection and Compliance Risks in Investment Activities

READING 56

READING 61

Capital Planning at Large Bank Holding Companies: Supervisory Expectations and Range of Current Practice

READING 62

Capital Regulation Before the Global Financial Crisis

READING 63

Solvency, Liquidity, and Other Regulation After the Global Financial Crisis

READING 64

High-Level Summary of Basel III Reforms

READING 65

Basel III: Finalizing Post-Crisis Reforms

Formulas

Readings and Learning Objectives

STUDY SESSION 7

42. Introduction to Operational Risk and Resilience

Global Association of Risk Professionals. *Operational Risk and Resilience*. New York, NY: Pearson, 2022. Chapter 1.

After completing this reading, you should be able to:

a. describe an operational risk management framework and assess the types of risks that can fall within the scope of such a framework.
b. describe the seven Basel II event risk categories and identify examples of operational risk events in each category.
c. explain characteristics of operational risk exposures and operational loss events, and challenges that can arise in managing operational risk due to these characteristics.
d. describe operational resilience, identify the elements of an operational resilience framework, and summarize regulatory expectations for operational resilience.

43. Risk Governance

Global Association of Risk Professionals. *Operational Risk and Resilience*. New York, NY: Pearson, 2022. Chapter 2.

After completing this reading, you should be able to:

a. explain the Basel regulatory expectations for the governance of an operational risk management framework.
b. describe and compare the roles of different committees and the board of directors in operational risk governance.
c. describe the "three lines of defense" model for operational risk governance and compare roles and responsibilities for each line of defense.
d. explain best practices and regulatory expectations for the development of a risk appetite for operational risk and for a strong risk culture.

44. Risk Identification

Global Association of Risk Professionals. *Operational Risk and Resilience*. New York, NY: Pearson, 2022. Chapter 3.

After completing this reading, you should be able to:

a. discuss different top-down and bottom-up approaches and tools for identifying operational risks.
b. describe best practices in extreme risk identification for operational risk.
c. describe and apply an operational risk taxonomy and give examples of different taxonomies of operational risks.
d. describe and apply the Level 1, 2, and 3 categories in the Basel operational risk taxonomy.

45. Risk Measurement and Assessment

Global Association of Risk Professionals. *Operational Risk and Resilience*. New York, NY: Pearson, 2022. Chapter 4.

After completing this reading, you should be able to:

a. explain best practices for the collection of operational loss data and reporting of operational loss incidents, including regulatory expectations.
b. explain operational risk-assessment processes and tools, including risk control self-assessments (RCSAs), likelihood assessment scales, and heatmaps.
c. describe the differences among key risk indicators (KRIs), key performance indicators (KPIs), and key control indicators (KCIs).
d. describe the use of factor-based models that quantitatively assess operational risk, and explain the application of the Swiss cheese model and the bowtie tool.
e. estimate operational risk exposures based on the fault tree model given probability assumptions.
f. describe approaches used to determine the level of operational risk capital for economic capital purposes, including their application and limitations.

g. describe and explain the steps to ensure a strong level of operational resilience, and to test the operational resilience of important business services.

46. Risk Mitigation

Global Association of Risk Professionals. *Operational Risk and Resilience*. New York, NY: Pearson, 2022. Chapter 5.

After completing this reading, you should be able to:

a. explain and compare different ways firms address their operational risk exposures.
b. compare different types of internal controls and provide examples of each type of internal control.
c. describe control automation, internal control design, and control testing, including risks and challenges that arise in these processes and ways to make them more effective.
d. describe methods to improve the quality of an operational process and reduce the potential for human error.
e. explain how operational risk can arise with new products, new business initiatives, or mergers and acquisitions, and describe ways to mitigate these risks.
f. identify and describe approaches firms should use to mitigate the impact of operational risk events.
g. describe methods for the transfer of operational risks and the management of reputational risk, and assess their effectiveness in different situations.

47. Risk Reporting

Global Association of Risk Professionals. *Operational Risk and Resilience*. New York, NY: Pearson, 2022. Chapter 6.

After completing this reading, you should be able to:

a. identify roles and responsibilities of different organizational committees, and explain how risk reports should be developed for each committee or business function.
b. describe components of operational risk reports and explain best practices in operational risk reporting.
c. describe challenges to reporting operational risks, including characteristics of operational loss data, and explain ways to overcome these challenges.
d. explain best practices for reporting risk exposures to regulators and external stakeholders.

48. Integrated Risk Management

Global Association of Risk Professionals. *Operational Risk and Resilience*. New York, NY: Pearson, 2022. Chapter 7.

After completing this reading, you should be able to:

a. describe the role of risk governance, risk appetite, and risk culture in the context of an enterprise risk management (ERM) framework.
b. explain and differentiate between regulatory capital and economic capital requirements as prescribed in Basel regulations.
c. describe the elements of a sound stress-testing framework for financial institutions and explain best practices for stress testing.
d. explain challenges and considerations when developing and implementing models used in stress testing operational risk.

STUDY SESSION 8

49. Cyber-Resilience: Range of Practices

"Cyber-Resilience: Range of Practices," (Basel Committee on Banking Supervision Publication, December 2018).

After completing this reading, you should be able to:

a. define cyber-resilience and compare recent regulatory initiatives in the area of cyber-resilience.
b. describe current practices by banks and supervisors in the governance of a cyber-risk management framework, including roles and responsibilities.
c. explain methods for supervising cyber-resilience, testing and incident response approaches, and cybersecurity and resilience metrics.
d. explain and assess current practices for the sharing of cybersecurity information between different types of institutions.

e. describe practices for the governance of risks of interconnected third-party service providers.

50. Case Study: Cyberthreats and Information Security Risks

Global Association of Risk Professionals. *Operational Risk and Resilience*. New York, NY: Pearson, 2022. Chapter 9.

After completing this reading, you should be able to:

a. provide examples of cyber threats and information security risks, and describe frameworks and best practices for managing cyber risks.
b. describe lessons learned from the Equifax case study.

51. Sound Management of Risks Related to Money Laundering and Financing of Terrorism

"Sound Management of Risks Related to Money Laundering and Financing of Terrorism," (Basel Committee on Banking Supervision, July 2020).

After completing this reading, you should be able to:

a. explain best practices recommended by the Basel Committee for the assessment, management, mitigation, and monitoring of money laundering and financing of terrorism (ML/FT) risks.
b. describe recommended practices for the acceptance, verification, and identification of customers at a bank.
c. explain practices for managing ML/FT risks in a group-wide and cross-border context.

52. Case Study: Financial Crime and Fraud

Global Association of Risk Professionals. *Operational Risk and Resilience*. New York, NY: Pearson, 2022. Chapter 11.

After completing this reading, you should be able to:

a. describe elements of a control framework to manage financial fraud risk and money laundering risk.
b. summarize the regulatory findings and describe the lessons learned from the USAA case study.

53. Guidance on Managing Outsourcing Risk

"Guidance on Managing Outsourcing Risk," Board of Governors of the Federal Reserve System, December 2013.

After completing this reading, you should be able to:

a. explain how risks can arise through outsourcing activities to third-party service providers and describe elements of an effective program to manage outsourcing risk.
b. explain how financial institutions should perform due diligence on third-party service providers.
c. describe topics and provisions that should be addressed in a contract with a third-party service provider.

54. Case Study: Third-Party Risk Management

Global Association of Risk Professionals. *Operational Risk and Resilience*. New York, NY: Pearson, 2022. Chapter 13.

After completing this reading, you should be able to:

a. explain how risks related to the use of third parties can arise and describe characteristics of an effective third-party risk management framework.
b. describe the lessons learned from the presented case studies.

55. Case Study: Investor Protection and Compliance Risks in Investment Activities

Global Association of Risk Professionals. *Operational Risk and Resilience*. New York, NY: Pearson, 2022. Chapter 14.

After completing this reading, you should be able to:

a. summarize important regulations designed to protect investors in financial instruments, including MiFID, MiFID II, and Dodd-Frank.
b. describe lessons learned from the case studies involving violations of investor protection or compliance regulations.

56. Supervisory Guidance on Model Risk Management

"Supervisory Guidance on Model Risk Management," Federal Deposit Insurance Corporation, June 7, 2017.

After completing this reading, you should be able to:

a. describe model risk and explain how it can arise in the implementation of a model.
b. describe elements of an effective model risk management process.
c. explain best practices for the development and implementation of models.

d. describe elements of a strong model validation process and challenges to an effective validation process.

57. Case Study: Model Risk and Model Validation

Global Association of Risk Professionals. *Operational Risk and Resilience*. New York, NY: Pearson, 2022. Chapter 16.

After completing this reading, you should be able to:

a. define a model and describe different ways that financial institutions can become exposed to model risk.

b. describe the role of the model risk management function and explain best practices in the model risk management and validation processes.

c. describe lessons learned from the three case studies involving model risk.

58. Stress Testing Banks

Til Schuermann, "Stress Testing Banks," *International Journal of Forecasting* 30, no. 3 (2014): 717–728.

After completing this reading, you should be able to:

a. describe the evolution of the stress testing process and compare the methodologies of historical European Banking Association (EBA), Comprehensive Capital Analysis and Review (CCAR), and Supervisory Capital Assessment Program (SCAP) stress tests.

b. explain challenges in designing stress test scenarios, including the problem of coherence in modeling risk factors.

c. explain challenges in modeling a bank's revenues, losses, and its balance sheet over a stress test horizon period.

STUDY SESSION 9

59. Risk Capital Attribution and Risk-Adjusted Performance Measurement

Michel Crouhy, Dan Galai and Robert Mark, *The Essentials of Risk Management, 2nd Edition* (New York, NY: McGraw-Hill, 2014). Chapter 17.

After completing this reading, you should be able to:

a. define, compare, and contrast risk capital, economic capital, and regulatory capital and explain methods and motivations for using economic capital approaches to allocate risk capital.

b. describe the RAROC (risk-adjusted return on capital) methodology and its use in capital budgeting.

c. calculate and interpret the RAROC for a project, loan, or loan portfolio and use RAROC to compare business unit performance.

d. explain challenges that arise when using RAROC for performance measurement, including choosing a time horizon, measuring default probability, and choosing a confidence level.

e. calculate the hurdle rate and apply this rate in making business decisions using RAROC.

f. calculate the adjusted RAROC for a project to determine its viability.

g. explain challenges in modeling diversification benefits, including aggregating a firm's risk capital and allocating economic capital to different business lines.

h. explain best practices in implementing an approach that uses RAROC to allocate economic capital.

60. Range of Practices and Issues in Economic Capital Frameworks

"Range of Practices and Issues in Economic Capital Frameworks," (Basel Committee on Banking Supervision Publication, March 2009).

After completing this reading, you should be able to:

a. within the economic capital implementation framework, describe the challenges that appear in:

- defining and calculating risk measures
- risk aggregation
- validation of models
- dependency modeling in credit risk
- evaluating counterparty credit risk
- assessing interest rate risk in the banking book

b. describe the recommendations by the Bank for International Settlements (BIS) that supervisors should consider in order to make effective use of internal risk measures, such as economic

capital, that are not designed for regulatory purposes.

c. explain benefits and impacts of using an economic capital framework within the following areas:
   - credit portfolio management
   - risk-based pricing
   - customer profitability analysis
   - management incentives

d. describe best practices and assess key concerns for the governance of an economic capital framework.

61. Capital Planning at Large Bank Holding Companies: Supervisory Expectations and Range of Current Practice

"Capital Planning at Large Bank Holding Companies: Supervisory Expectations and Range of Current Practice," Board of Governors of the Federal Reserve System, August 2013.

After completing this reading, you should be able to:

a. describe the Federal Reserve's Capital Plan Rule and explain the seven principles of an effective capital adequacy process for bank holding companies (BHCs) subject to the Capital Plan Rule.

b. describe practices that can result in a strong and effective capital adequacy process for a BHC in the following areas:
   - risk identification
   - internal controls, including model review and valuation
   - corporate governance
   - capital policy, including setting of goals and targets and contingency planning
   - stress testing and stress scenario design
   - estimating losses, revenues, and expenses, including quantitative and qualitative methodologies
   - assessing the impact of capital adequacy, including risk-weighted asset (RWA) and balance sheet projections

62. Capital Regulation Before the Global Financial Crisis

Mark Carey, "Capital Regulation Before the Global Financial Crisis," GARP Risk Institute, April 2019.

After completing this reading, you should be able to:

a. explain the motivations for introducing the Basel regulations, including key risk exposures addressed, and explain the reasons for revisions to Basel regulations over time.

b. explain the calculation of risk-weighted assets and the capital requirement per the original Basel I guidelines.

c. describe measures introduced in the 1995 and 1996 amendments, including guidelines for netting of credit exposures and methods for calculating market risk capital for assets in the trading book.

d. describe changes to the Basel regulations made as part of Basel II, including the three pillars.

e. compare the standardized internal ratings-based (IRB) approach, the foundation IRB approach, and the advanced IRB approach for the calculation of credit risk capital under Basel II.

f. calculate credit risk capital under Basel II utilizing the IRB approach.

g. compare the basic indicator approach, the standardized approach, and the advanced measurement approach for the calculation of operational risk capital under Basel II.

h. summarize elements of the Solvency II capital framework for insurance companies.

63. Solvency, Liquidity, and Other Regulation After the Global Financial Crisis

Mark Carey, "Solvency, Liquidity, and Other Regulation After the Global Financial Crisis," GARP Risk Institute, April 2019.

After completing this reading, you should be able to:

a. describe and calculate the stressed VaR introduced in Basel 2.5 and calculate the market risk capital charge.

b. explain the process of calculating the incremental risk capital charge for positions held in a bank's trading book.

c. describe the comprehensive risk (CR) capital charge for portfolios of positions that are sensitive to correlations between default risks.

d. define in the context of Basel III and calculate where appropriate:

- Tier 1 capital and its components
- Tier 2 capital and its components
- required Tier 1 equity capital, total Tier 1 capital, and total capital

e. describe the motivations for and calculate the capital conservation buffer and the countercyclical buffer, including special rules for globally systemically important banks (G-SIBs).
f. describe and calculate ratios intended to improve the management of liquidity risk, including the required leverage ratio, the liquidity coverage ratio, and the net stable funding ratio.
g. describe the mechanics of contingent convertible bonds (CoCos) and explain the motivations for banks to issue them.
h. provide examples of legislative and regulatory reforms that were introduced after the 2007–2009 financial crisis.

64. High-Level Summary of Basel III Reforms

"High-Level Summary of Basel III Reforms," (Basel Committee on Banking Supervision Publication, December 2017).

After completing this reading, you should be able to:

a. explain the motivations for revising the Basel III framework and the goals and impacts of the December 2017 reforms to the Basel III framework.
b. summarize the December 2017 revisions to the Basel III framework in the following areas:
   - the standardized approach to credit risk
   - the internal ratings-based (IRB) approaches for credit risk
   - the CVA risk framework
   - the operational risk framework
   - the leverage ratio framework
c. describe the revised output floor introduced as part of the Basel III reforms and approaches to be used when calculating the output floor.

65. Basel III: Finalizing Post-Crisis Reforms

"Basel III: Finalizing Post-Crisis Reforms," (Basel Committee on Banking Supervision Publication, December 2017): 128-136.

After completing this reading, you should be able to:

a. explain the elements of the new standardized approach to measure operational risk capital, including the business indicator, internal loss multiplier, and loss component, and calculate the operational risk capital requirement for a bank using this approach.
b. compare the Standardized Measurement Approach (SMA) to earlier methods of calculating operational risk capital, including the Advanced Measurement Approaches (AMA).
c. describe general and specific criteria recommended by the Basel Committee for the identification, collection, and treatment of operational loss data.

The following is a review of the Operational Risk and Resilience principles designed to address the learning objectives set forth by GARP®. Cross-reference to GARP FRM Part II Operational Risk and Resilience, Chapter 1.

READING 42

INTRODUCTION TO OPERATIONAL RISK AND RESILIENCE

Study Session 7

EXAM FOCUS

This is the first of seven interrelated readings on operational risk management. In this first reading, the concepts of operational risk and resilience are introduced and will be further developed in subsequent readings. The same goes for other concepts such as risk governance, risk identification, risk measurement and assessment, and risk mitigation. For the exam, know the seven operational risk categories and their corresponding examples. Also, understand the five characteristics of operational risk exposures and operational loss events. Finally, be familiar with the regulatory guidance on operational resilience such as those provided by the U.S. Federal Reserve and the Basel Committee on Banking Supervision.

MODULE 42.1: OPERATIONAL RISK CATEGORIES

Operational Risk Management Framework

LO 42.a: Describe an operational risk management framework and assess the types of risks that can fall within the scope of such a framework.

Operational risk has been defined by the Basel Committee on Banking Supervision (BCBS) as "the risk or loss resulting from inadequate or failed internal processes, people, systems, and external events." Operational risk management (ORM) deals with these four specific causes, and an ORM framework is the total of the methods or processes used to control operational risk within a firm.

Within risk management, there are four steps to be taken in an iterative cycle: (1) risk identification, (2) risk assessment, (3) risk mitigation, and (4) risk monitoring.

Risk identification attempts to determine as many relevant risks as possible that could negatively impact the firm's business goals. Group brainstorming activities and interviews with staff might be used in this step.

Risk assessment involves determining the probability and severity of the risks identified as a means of prioritization. It must also be considered that both probability and severity will likely change over time and depend on the situation. Tools such as stress testing and scenario analysis would be used in this step.

Risk mitigation looks to minimize or eliminate risks that have a high probability of occurring or high severity if they occur. Methods such as internal controls, purchasing insurance as protection, or minimizing exposure are commonly used in this step.

Risk monitoring is the final step, and it is meant to verify if the risk management process is operating as expected and if the firm's operations are robust. If not, then the risk management cycle continues again with remedial actions taken in the first three steps before performing another step of risk monitoring and evaluation. Reviewing incident reports and developing key risk indicators would occur in this step.

Event-Driven Risk Categories

LO 42.b: Describe the seven Basel II event risk categories and identify examples of operational risk events in each category.

Basel II provides seven categories of "Level 1" loss events that most firms have adopted to meet their own ORM framework requirements. The seven Basel II event risk categories are intended to capture all potential operational risks. Every loss event should be mapped to the risk event categories outlined in the firm's ORM policies and procedures. However, some loss events may fall under more than one category.

The modeling of loss event data differs for each category. Thus, it is important to make sure every event is placed in the appropriate group. When assigning loss events, consistency is more important than accuracy. Effective ORM requires that similar events are consistently categorized the same way. If mistakes are made classifying risks in past years, it will impact the risk management control process and reporting to regulators. To properly classify risks, it is important for the firm to perform a comprehensive risk-mapping exercise that details every major process of the firm.

The seven Basel II event risk categories are listed as follows. It is important to recognize that the severity and frequency of losses can vary dramatically among the categories.

1. **Internal fraud (IF)**
   - *Examples*: employee defalcation, employees bypassing internal controls (e.g., rogue trading)
   - Low frequency of occurrence and low loss severity
2. **External fraud (EF)**
   - *Examples*: credit card fraud, losses from hacking
   - High frequency of occurrence, but low loss severity
3. **Employment practices and workplace safety (EPWS)**
   - *Examples*: employee termination and discrimination

- Moderate frequency of occurrence, but low loss severity

4. **Clients, products, and business practices (CPBP)**
   - *Examples*: errors resulting in client complaints and requiring compensation, regulatory fines
   - High frequency of occurrence and very high loss severity
5. **Damage to physical assets (DPA)**
   - *Examples*: weather-related events, negligence
   - Low frequency of occurrence and low loss severity
6. **Business disruption and system failures (BDSF)**
   - *Examples*: IT problems, service interruptions
   - Low frequency of occurrence and low loss severity
7. **Execution, delivery, and process management (EDPM)**
   - *Examples*: clerical errors, insufficient documentation
   - High frequency of occurrence and high loss severity

Types of Risks Within the ORM Framework

Stepping back slightly, operational risk includes legal risk and compliance risk, and, on an as-needed basis, it includes strategic risk and reputational risk.

Legal risk refers to the potential losses suffered by a firm due to the enforcement or nonfulfillment of contracts. Most of the legal risks originate from EPWS events (Type 3) and EDPM events (Type 7). Compliance risk is more specific than legal risk, and the former involves adherence to the appropriate policies and procedures. The lack of compliance is seen in CPBP events (Type 4), and the related monetary fines have increased substantially over the past 10 years. As a result, many firms have established internal compliance departments specifically to deal with compliance risk.

Reputational risk can be viewed as a more indirect and subjective type of risk; it is the reputational loss to a firm that arises from a significant operational event. Therefore, reputational loss requires methods to prevent it and to manage it after operational incidents. At the same time, reputational risk can be viewed as a direct risk in certain instances (e.g., product specialization, operating in specific geographic regions) whereby reputational risk is assumed in hopes of leading to greater profitability.

Strategic risk can be broken into two components. First, it could refer to losses occurring because of incorrect or poor strategic decisions. Alternatively, it could refer to losses occurring because of inadequate implementation of a good strategy. The common denominator is personnel, and specifically, senior management in context of a financial institution. Therefore, strategic risk is an important subset of operational risk —especially because strategic performance is greatly impacted by personnel skill and experience, the reliability of information used by personnel, and the strength of the firm's governance processes.

MODULE QUIZ 42.1

1. During which step of the risk management process would scenario analysis most likely be used?
   A. Risk mitigation.
   B. Risk monitoring.
   C. Risk assessment.
   D. Risk identification.

2. Which of the following Basel II event risk categories most likely results in the greatest loss severity for a financial institution?
   A. External fraud (EF).
   B. Client, products, and business practices (CPBP).
   C. Employment practices and workplace safety (EPWS).
   D. Execution, delivery, and process management (EDPM).

MODULE 42.2: OPERATIONAL RISK CHARACTERISTICS

LO 42.c: Explain characteristics of operational risk exposures and operational loss events, and challenges that can arise in managing operational risk due to these characteristics.

Operational risks have five general attributes: (1) heterogeneous, (2) idiosyncratic, (3) heavy tailed, (4) interconnected, and (5) dynamic, each of which presents challenges in managing operational risk.

Heterogeneous

There are a wide range of risks contained under the umbrella of operational risk—for example, anywhere from minor credit card fraud to major loss of physical assets due to weather-related events. Operational risks arise differently, have different implications, and have different loss distributions—and within the major types of operational risks, there are great differences. Consider the various types of errors ranging from minor typos on internal documents with zero losses to transcription errors on large transactions that could result in losses in the millions. Therefore, the heterogeneous nature means that much diligence and thought is necessary to determine and organize operational risk into useful categories.

Idiosyncratic

Operational risk is very diffuse in nature; unlike other financial risks, it cannot be centralized. In practice, operational risk must be managed by each employee in terms of preventing or minimizing errors, for example. To the extent there are robust controls and procedures in place at the firm, much of the operational risk within a firm can be mitigated by employees themselves.

Although significant efforts may be made to avoid, neutralize, or transfer risk using traditional methods, the idiosyncratic nature of operational risk means that there will always be some residual amount of operational risk remaining.

Heavy Tailed

Operational risks tend to result in many minor losses (e.g., service fees, credit card fraud), but with a few major losses (e.g., rogue trading, widespread cyberattack, extended IT service outage)—hence, significant asymmetry and left-tail skew. The major losses are infrequent, but when they occur, they are considerably higher than the median loss.

Because of the wide range, the approach to risk management must be tailored to ensure efficiency. For example, minor operational risks with very low expected losses can often be ignored and treated as a cost of doing business. However, the potential for large losses cannot be ignored—but at the same time, the measurement of such losses is problematic because of the fat tails (excess kurtosis) in the operational loss distribution. The measurement is complicated by the fact that there is often not much precedent in terms of past events, nor is there certainty of recurrence in the future.

Interconnected

Many operational risks have some correlation to each other due to their common causes such as control weaknesses, human error, macroeconomic events, or political events. There are also some links between operational risks and financial risks (e.g., credit and market). For example, trading errors (an operational risk) will probably have market risk impacts in the form of losses. Such risk events are called *boundary events* because they begin as one type of risk but end up affecting another type of risk. In general, operational risks may interact with other risks in unknown and complicated ways that would be problematic to quantify.

Dynamic

Operational risks are, by nature, evolving with changes in business practices within the firm and the industry. For example, the assessed regulatory fines in the financial industry began to increase substantially in recent years, which resulted in unexpectedly significant operational losses for some banks. In addition, the move from manual to electronic banking meant an increase in operational losses due to cyber fraud.

The dynamic nature of operational risks makes them difficult to model or quantify in advance. As a result, in this context, risk managers have to take a more reactive (rather than proactive) approach to managing operational risk.

Operational Resilience

LO 42.d: Describe operational resilience, identify the elements of an operational resilience framework, and summarize regulatory expectations for operational resilience.

Operational resilience refers to how firms and industries deal with business disruptions. It includes activities such as anticipating, reacting to, and recovering from such disruptions. Resilience consists of the following items:

- *Business continuity*. This focuses on minimizing the disruptions to business processes.
- *Key services*. This focuses on determining and ensuring that the absolute, most critical business services can continue with little or no disruption.
- *Impact tolerance levels*. This is similar to the acceptable disruption time of a key service or time needed to recover from an incident.
- *Disruption processes*. This focuses on how to respond to disruptions, retaining the confidence of important stakeholders, and effective communication during disruptions.
- *Feedback*. This focuses on takeaways from past incidents to prevent similar problems from occurring in the future. The goal is to always enhance the ability to deal with unexpected events with high impact.

Regulatory Expectations

Both banks and their regulators have understood that the nature of cyber risks means that there must be a recognition that extreme operational disruptions will occur, but that they will be relatively infrequent. The focus has changed from solely attempting to prevent cyber incidents to managing them as they happen.

UK Regulations

In the United Kingdom, existing ORM regulations were not replaced, but additional regulations were added in 2018 in a collaborative effort by the UK Financial Conduct Authority (FCA), Prudential Regulation Authority (PRA), and the Bank of England (BoE). Regarding the new regulations, the focus on resilience was on the continuity of IT services following a cyber incident. However, with the onset of the COVID-19 pandemic in 2020, further adjustments needed to be made to account for substantially increased work-from-home (WFH) arrangements and for important electronic transactions to be handled in a less secure external/remote environment (instead of a more secure internal environment before the pandemic).

U.S. Regulations

In 2020, the Federal Reserve in the United States published guidance with the conclusion that an effective ORM framework would have operational resilience as the major result. As illustrated in Figure 42.1, the different components of ORM would work together to produce the overall result of operational resilience. With governance as the starting point, ORM is the central element that is accompanied by two key supports: third-party risk management (to ensure supply chain resiliency) and scenario analysis (to anticipate low-probability, high-severity events). The two other key ingredients in operational resiliency are business continuity management and IT systems resiliency. Finally, proper surveillance and monitoring is required to ensure all activities are functioning as expected.

Figure 42.1: Building Blocks of Operational Resilience

Source: Ariane Chapelle, *Operational Risk Management: Best Practices in the Financial Services Industry* (Wiley Finance Series, 2018).

Basel Committee on Banking Supervision (BCBS)

The BCBS issued the following seven principles of operational resilience in 2021:

1. Governance
2. Operational risk management
3. Business continuity planning and testing
4. Mapping interconnections and interdependencies
5. Third-party dependency management
6. Incident management
7. Information and communications technology (ICT), including cybersecurity

With Principles 1 and 2, the underlying premise is that banks account for operational resilience in the wider context of overall risk management within the firm, using their current governance system as a starting point.

Similar to U.S. guidance, business continuity plans must be in use, third-party dependencies must be controlled, and ICT must be developed to maximize its resiliency. Those points are covered in Principles 3, 5, and 7.

Similar to UK guidance, being aware of all interconnections and interdependencies as well as having an established process to manage incidents (response and recovery) are necessary to ensure the continuous provision of key services without unacceptable disruptions. Those points are covered in Principles 4 and 6.

Other Regulators

As of May 2022, the United Kingdom, United States, and BCBS are the key regulators that have provided guidance on operational resilience.

In 2020, the European Central Bank (ECB) issued proposed rules in the form of the Digital Operational Resilience Act (DORA) to promote digital finance, but at the same time, to manage the corresponding risks. DORA will add numerous IT-related requirements for financial institutions under one common regulation to be applied consistently throughout the European Union (EU).

In 2021, the Monetary Authority of Singapore (MAS), together with The Association of Banks in Singapore (ABS), released a publication that deals with operational resiliency

in the context of remote-work settings that arose during the pandemic. The risks involved relate to matters such as operations, IT, fraud, legal, and regulatory. Relevant controls in the context of WFH arrangements and best practices were discussed as well as the need to educate employees in WFH situations to understand their changed work environment and to be constantly alert of the new cyber and fraud risks that abound in the new work environment.

MODULE QUIZ 42.2

1. Which of the following characteristics of operational risk best identifies the concept that operational risk cannot be fully eliminated through traditional methods, such as hedging?
   A. Dynamic.
   B. Idiosyncratic.
   C. Heterogeneous.
   D. Interconnected.

2. To date, which of the following entities is least likely to be considered a key regulator to have issued official guidance for operational resilience?
   A. Bank of England.
   B. U.S. Federal Reserve.
   C. European Central Bank.
   D. Basel Committee on Banking Supervision.

3. Which of the following pairs of resilience principles directly address the issue of providing critical services with minimal or no disruption?
   A. Third-party dependency management; incident management.
   B. Mapping interconnections and interdependencies; incident management.
   C. Business continuity planning and testing; third-party dependency management.
   D. Business continuity planning and testing; mapping interconnections and interdependencies.

KEY CONCEPTS

LO 42.a

Operational risk has been defined as "the risk or loss resulting from inadequate or failed internal processes, people, systems, and external events." Within risk management, there are four steps in an iterative cycle: (1) risk identification, (2) risk assessment, (3) risk mitigation, and (4) risk monitoring. Operational risk includes legal and compliance risk as well as strategic risk and reputational risk.

LO 42.b

There are seven Basel II operational risk event categories:

1. Internal fraud (IF)
2. External fraud (EF)
3. Employment practices and workplace safety (EPWS)
4. Clients, products, and business practices (CPBP)
5. Damage to physical assets (DPA)
6. Business disruption and system failures (BDSF)
7. Execution, delivery, and process management (EDPM)

LO 42.c

Operational risks have five general attributes: (1) heterogeneous, (2) idiosyncratic, (3) heavy tailed, (4) interconnected, and (5) dynamic, each of which presents challenges in managing operational risk.

LO 42.d

Operational resilience consists of the following items:

- Business continuity
- Key services
- Impact tolerance levels
- Disruption processes
- Feedback

Both banks and their regulators have understood that the nature of cyber risks means that there must be a recognition that extreme operational disruptions will occur, but that they will be relatively infrequent. The focus has changed from solely attempting to prevent cyber incidents to managing them as they happen.

The BCBS issued the following seven principles of operational resilience:

1. Governance
2. Operational risk management
3. Business continuity planning and testing
4. Mapping interconnections and interdependencies
5. Third-party dependency management
6. Incident management
7. ICT, including cybersecurity

As of May 2022, the United Kingdom, United States, and BCBS are the key regulators that have provided guidance on operational resilience.

ANSWER KEY FOR MODULE QUIZZES

Module Quiz 42.1

1. **C** Risk assessment involves determining the probability and severity of the risks identified as a means of prioritization. It must also be considered that both probability and severity will likely change over time and depend on the situation. Tools such as stress testing and scenario analysis would be used in this step. (LO 42.a)

2. **B** Based on bank operational loss data for 2014–2019, CPBP accounted for 52% of loss severity (very high loss severity), which was by far the greatest of the seven types. It was followed by EDPM, which accounted for 27% of loss severity (high loss severity). (LO 42.b)

Module Quiz 42.2

1. **B** Idiosyncratic risk refers to the idea that operational risk cannot be fully eliminated through traditional methods such as avoidance, hedging, or insurance and that there will always be some residual risk. (LO 42.c)

2. **C** To date, the United Kingdom (Bank of England, or BoE), the United States (Federal Reserve), and the BCBS are the three key regulators to have provided official guidance regarding operational resilience. (LO 42.d)

3. **B** Both Principle 4 (mapping interconnections and interdependencies) and Principle 6 (incident management) of the BCBS principles on operational resilience are directly concerned with the delivery of critical operations with minimal or no disruption. (LO 42.d)

The following is a review of the Operational Risk and Resilience principles designed to address the learning objectives set forth by GARP®. Cross-reference to GARP FRM Part II Operational Risk and Resilience, Chapter 2.

READING 43

RISK GOVERNANCE

Study Session 7

EXAM FOCUS

This reading reviews the details of an operational risk management framework (ORMF). It builds on basic concepts from the FRM Part I curriculum such as risk regulation, governance, appetite, and culture. This reading applies those concepts in an operational risk context. For the exam, focus on the most testable concepts, such as the calculations in Basel II Pillar 1 (capital for operational risk) as well as the details of the three lines of defense model for controlling operational risk.

MODULE 43.1: OPERATIONAL RISK REGULATION AND GOVERNANCE

LO 43.a: Explain the Basel regulatory expectations for the governance of an operational risk management framework.

Basel II Operational Risk

Basel II includes three pillars for the regulation of operational risk. A brief summary of each is provided here, with a more detailed discussion of Pillar 1 and Pillar 2 to follow.

Pillar 1: Regulatory Capital

- Minimum capital required to meet any unexpected losses from credit, market, and operational risks
- Minimum coverage ratios to manage liquidity risk
- Basel Committee's *Principles for the Sound Management of Operational Risk*

Pillar 2: Supervisory Review Process

- Extra capital requirements on top of Pillar 1 to address regulatory capital for risks not explicitly considered in Pillar 1 (e.g., concentration, compliance, governance risks)
- Voluntary disclosure and self-assessment subject to regulatory review

Pillar 3: Market Discipline

- Required quarterly and annual financial (e.g., balance sheet) and risk disclosures by banks
- Underlying idea is to have greater capital reserves to balance greater risks taken

Pillar 1: Principles for the Sound Management of Operational Risk

Operational risk management cannot exist purely with regulatory capital calculations. It must be balanced with proper operational risk management (ORM). The following 12 principles are the product of numerous past revisions and evolution in risk management by the Basel Committee on Banking Supervision (BCBS) to account for real-life events such as the 2007–2009 financial crisis:

1. Culture directed by the board of directors (board) and put in place by senior management
2. Maintaining a robust ORMF
3. Board analysis and validation of the ORMF
4. Board to regularly assess and sign off on operational risk appetite and operational risk tolerance statements
5. Clear description of senior management's responsibilities regarding ORM policies and systems development and implementation
6. Thorough description and evaluation of operational risk for key business activities
7. Thorough preparation and communication of the change management process
8. Ongoing review of operational risk profile and exposures
9. Secure and stable controls (e.g., internal controls, risk mitigation, training, risk transfer methods)
10. Reliable information and communication technology (ICT) that is consistent with the ORMF
11. Established business continuity plans that are consistent with the ORMF
12. External disclosures on the ORM approach and risk exposures

Pillar 1: Capital Calculation

A revised approach effective as of January 2023 is a single capital measure known as the **standardized approach (SA)**. For this approach, the following general equation is used for operational risk capital (ORC):

ORC = business indicator component (BIC) × internal loss multiplier (ILM)

where:

BIC = percentage of the yearly average business indicator (BI) over the past three years (it is analogous to the concept of gross income)

BI = interest, leases, and dividend component (ILDC) + services component (SC) + financial component (FC)

Business Indicator Component (BIC)

- Within BI, the SC consists of the higher of fee income and fee expenses *plus* the higher of other operating income and operating expense.
- Within BI, the FC consists of the absolute value of the net income/loss of the banking book and the trading book.
- The percentage used to calculate BIC is determined as follows:
  - 12% for less than EUR1 billion (based on BI)
  - 15% for EUR1 billion to EUR30 billion (based on BI)
  - 18% for greater than EUR30 billion (based on BI)
- Given the increased percentages based on size, regulators clearly believe that operational risk has a proportionally larger increase than size. As a result, additional capital is required to account for the greater risk.

Internal Loss Multiplier (ILM)

- Penalizes (helps) banks that have greater (lower) losses than average
- A loss component (LC) is used and is calculated as follows:
  - 15 × annual operational losses incurred over the last 10 consecutive years
- ILM = 1 if LC = BIC; often used by regulators in practice for simplicity
- ILM > 1 if LC > BIC; therefore, more capital is required
- ILM < 1 if LC < BIC; therefore, less capital is required

Pillar 2: Operational Risk Capital

Pillar 2 is a supplement to the Pillar 1 capital requirement. Pillar 2 is meant to be more representative of the specific risk exposure of the given bank. Examples could include excessive geographic or sector concentrations, exceedingly rapid business growth, or weak risk management methods. In such cases, regulators are likely to require additional capital to account for the incremental operational risk.

Within Pillar 2, regulators examine all activities put in place by the bank to meet regulatory requirements. Regulators also pursue additional risks discovered through stress testing. Overall, regulators must be satisfied that the bank has capital reserves that are in line with the risks taken.

Solvency (which is long term in nature) is assessed here, which involves determining significant threats and scenarios for major loss events as well as determining the bank's resilience to sudden events that could negatively impact the bank's operations and profits. Pillar 2 also analyzes the bank's governance processes, values and mission, and the ability of managers to fulfill their roles (e.g., providing thorough and useful risk reporting).

Regulatory Expectations

In assessing an ORMF, there are many core principles required for a proper supervisory system, but five of them are particularly relevant:

- *Principle 8*. Supervisors should formulate and consistently apply a forward-looking assessment of the risk profile of banks in relation to their systemic importance.
- *Principle 14*. Supervisors ensure that banks have strong corporate governance policies and procedures.
- *Principle 15*. Supervisors ensure that banks have a thorough risk management program that is able to determine, quantify, assess, monitor, report, and manage the significant risks faced in a timely manner.
- *Principle 25*. Supervisors ensure that banks have a proper ORMF that considers risk appetite, risk profile, market, and other macroeconomic factors.
- *Principle 26*. Supervisors ensure that sufficient internal controls exist to allow for well-controlled business operations in relation to the bank's risk profile.

Part of *Principles for the Sound Management of Operational Risk* specifically states that supervisors should perform ongoing review of a bank's ORMF, which includes policies, procedures, and IT systems that are associated with operational risk. Any significant deficiencies noted in the reviews would require supervisors to take action to resolve those deficiencies. Finally, the concept of continuous improvement of processes is key here—supervisors should take note of a bank's past improvements plus any ideas for future improvements and assist the bank with continuous improvement.

Regulators expect ORM to go much further than simply a process of compliance. The expectation is that risk management should be integrated as an essential part of business operations with employees involved in making decisions at all hierarchical levels. Regulators should expect to be able to follow a logical decision-making process within the bank and to confirm that decisions always account for the relevant risks.

Operational risk reports assist in evaluating ORMFs. In evaluating a bank's ORMF, regulators should often ask the following:

- Do incident reports account for all significant incidents? Do incident reports determine underlying causes and offer takeaways for improvement? Are "close calls" written up as incident reports?
- Is there a stable and methodical approach to performing risk and control assessments (internal) by qualified staff? Are such assessments subject to cross-examination to ensure they are reliable?
- Has management determined the risk indicators to be appropriate and relevant? How are risk indicators computed, and are they done objectively/without bias? Are risk indicators continuously updated as needed?
- Do scenarios cover a wide enough range, and is there consideration for extreme but potential scenarios? Are scenario assessments fair and detailed?
- Based on available reported information, is the overall ORMF reasonably thorough?
- Is there enough information to make proper decisions? Is the information useful for the given level of management?

Based on experiences, regulators would be happier to receive more sufficient documentation (e.g., meeting minutes) and more thorough reporting to "prove" or provide evidence of solid risk management processes in banks. This is especially the

case with smaller banks, which may not have the robust governance structure to support proper risk management processes.

LO 43.b: Describe and compare the roles of different committees and the board of directors in operational risk governance.

Risk Committee Structure

Risk committees dealing with operational risk will vary in scope based on the size of the bank. A small bank will probably have one operational risk committee with both oversight and reporting duties. A larger bank, on the other hand, will probably have multiple operational risk committees to account for different business lines.

An example and description of an expanded risk committee structure for a large bank could look as follows:

1. Lowest level:
   - Numerous smaller risk committees that are focused on a specific business activity (e.g., personal banking, trading, asset management) or specific countries
   - Such committees will often provide valuable data that is useful to assess firmwide operational risk and may forward crucial issues requiring a second look to be addressed at the middle or top level
2. Middle level:
   - Organization risk committee gathers information and manages the overall level of operational risk for the entire organization
   - Reports that information on a regular basis to the executive risk committee and board risk committee
3. Top level:
   - Board (enterprise) risk committee manages both the middle and lowest levels of operational risk
   - Board (enterprise) risk committee provides recommendations to the board on risk exposures and key decisions involving risk
   - Oversees the evaluation of major operational risk incidents and deals with issues escalated from the first two levels
   - Members must have risk management experience that is pertinent and current

Within a large bank, the term *enterprise risk* is an umbrella term that includes various risk types such as operational, fraud, information security, legal and compliance, credit, and market.

Governance and Risk Documentation

A committee will have a document called the terms of reference (TOR) that provides its mission and objective, membership duties and functions, and meeting frequency.

Committees analyze risk information and reporting to ensure that they are congruent with the risk decisions made. They also analyze and approve the policies and