

2026
FRM[®]
Exam Prep

SchweserNotes[™]
Operational Risk and Resilience

Part II | Book 3

KAPLAN[®] **SCHWESER**

Book 3: Operational Risk and Resilience

SchweserNotes™ 2026

FRM Part II

KAPLAN  **SCHWESER**

SCHWESERNOTES™ 2026 FRM® PART II BOOK 3: OPERATIONAL RISK AND RESILIENCE

©2026 Kaplan, Inc. All rights reserved.

Published in 2026 by Kaplan, Inc.

ISBN: 978-1-0788-5489-4

Required Disclaimer: GARP® does not endorse, promote, review, or warrant the accuracy of the products or services offered by Kaplan Schweser of FRM® related information, nor does it endorse any pass rates claimed by the provider. Further, GARP® is not responsible for any fees or costs paid by the user to Kaplan Schweser, nor is GARP® responsible for any fees or costs of any person or entity providing any services to Kaplan Schweser. FRM®, GARP®, and Global Association of Risk Professionals™ are trademarks owned by the Global Association of Risk Professionals, Inc.

These materials may not be copied without written permission from the author. The unauthorized duplication of these notes is a violation of global copyright laws. Your assistance in pursuing potential violators of this law is greatly appreciated.

Disclaimer: The SchweserNotes should be used in conjunction with the original readings as set forth by GARP®. The information contained in these books is based on the original readings and is believed to be accurate. However, their accuracy cannot be guaranteed nor is any warranty conveyed as to your ultimate exam success.

CONTENTS

Readings and Learning Objectives

STUDY SESSION 7—Operational Risk Overview

READING 42

Introduction to Operational Risk and Resilience

Exam Focus

Module 42.1: Operational Risk Categories

Module 42.2: Operational Risk Characteristics

Key Concepts

Answer Key for Module Quizzes

READING 43

Risk Governance

Exam Focus

Module 43.1: Operational Risk Regulation and Governance

Module 43.2: Three Lines of Defense, Risk Appetite, and Risk Culture

Key Concepts

Answer Key for Module Quizzes

READING 44

Risk Identification

Exam Focus

Module 44.1: Identifying Operational Risks

Module 44.2: Operational Risk Taxonomies

Key Concepts

Answer Key for Module Quizzes

READING 45

Risk Measurement and Assessment

Exam Focus

Module 45.1: Operational Loss Data and Qualitative Risk Assessment

Module 45.2: Key Indicators and Quantitative Risk Assessment

Module 45.3: Operational Risk Capital and Resilience

Key Concepts

Answer Key for Module Quizzes

READING 46

Risk Mitigation

Exam Focus

Module 46.1: Risk Mitigation With Internal Controls and Process Design

Module 46.2: Operational Risk Mitigation Measures and Management

Key Concepts

Answer Key for Module Quizzes

READING 47

Risk Reporting

Exam Focus

Module 47.1: Organizational Committees

Module 47.2: Operational Risk Reporting Components

Module 47.3: Operational Risk Reporting Challenges

Module 47.4: External Reporting Best Practices

Key Concepts

Answer Key for Module Quizzes

READING 48

Integrated Risk Management

Exam Focus

Module 48.1: Enterprise Risk Management (ERM)

Module 48.2: Stress Testing

Key Concepts

Answer Key for Module Quizzes

STUDY SESSION 8—Operational Risk Applications and Case Studies

READING 49

Cyber-Resilience: Range of Practices

Exam Focus

Module 49.1: Cyber Risks, Governance, and Supervision

Module 49.2: Cybersecurity Information Sharing Between Institutions and Third-Party Risk

Key Concepts

Answer Key for Module Quizzes

READING 50

Case Study: Cyberthreats and Information Security Risks

Exam Focus

Module 50.1: Information Security Risks and Frameworks

Key Concepts

Answer Key for Module Quiz

READING 51

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

Exam Focus

Module 51.1: Management of Money Laundering and Financial Terrorism Risks

Key Concepts

Answer Key for Module Quiz

READING 52

Case Study: Financial Crime and Fraud

Exam Focus

Module 52.1: Financial Crime and Fraud Risk Management

Key Concepts

Answer Key for Module Quiz

READING 53

Guidance on Managing Outsourcing Risk

Exam Focus

Module 53.1: Managing Outsourcing Risk

Key Concepts

Answer Key for Module Quiz

READING 54

Case Study: Third-Party Risk Management

Exam Focus

Module 54.1: Third-Party Risk Management and Responsibilities

Key Concepts

Answer Key for Module Quiz

READING 55

Case Study: Investor Protection and Compliance Risks in Investment Activities

Exam Focus

Module 55.1: Investor Protection Regulations

Key Concepts

Answer Key for Module Quiz

READING 56

Supervisory Guidance on Model Risk Management

Exam Focus

Module 56.1: Model Risk Management

Module 56.2: Model Validation Process

Key Concepts

Answer Key for Module Quizzes

READING 57

Case Study: Model Risk and Model Validation

Exam Focus

Module 57.1: Model Risk and Model Validation

Key Concepts

Answer Key for Module Quiz

READING 58

Stress Testing Banks

Exam Focus

Module 58.1: Stress Testing

Module 58.2: Challenges in Modeling Losses and Revenues

Key Concepts

Answer Key for Module Quizzes

STUDY SESSION 9—Capital and Regulatory Frameworks

READING 59

Risk Capital Attribution and Risk-Adjusted Performance Measurement

Exam Focus

Module 59.1: Risk-Adjusted Return on Capital

Module 59.2: RAROC, Hurdle Rate, and Adjusted RAROC

Module 59.3: Diversification Benefits and RAROC Best Practices

Key Concepts

Answer Key for Module Quizzes

READING 60

Range of Practices and Issues in Economic Capital Frameworks

Exam Focus

Module 60.1: Risk Measures and Risk Aggregation

Module 60.2: Validation, Dependency, Counterparty Credit Risk, and Interest Rate Risk

Module 60.3: BIS Recommendations, Constraints and Opportunities, and Best Practices
and Concerns

Key Concepts

Answer Key for Module Quizzes

READING 61

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

Exam Focus

Module 61.1: Federal Reserve's Capital Plan Rule

Module 61.2: Capital Adequacy Process
Module 61.3: Assessing the Impact of Capital Adequacy
Key Concepts
Answer Key for Module Quizzes

READING 62

Capital Regulation Before the Global Financial Crisis

Exam Focus
Module 62.1: Basel I Regulations and Revisions
Module 62.2: Basel II Regulations
Key Concepts
Answer Key for Module Quizzes

READING 63

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

Exam Focus
Module 63.1: Stressed VaR, Incremental Risk Capital Charge, and Comprehensive Risk Charge
Module 63.2: Basel III Capital Requirements, Buffers, and Liquidity Risk Management
Module 63.3: Contingent Convertible Bonds and Dodd-Frank Reform
Key Concepts
Answer Key for Module Quizzes

READING 64

High-Level Summary of Basel III Reforms

Exam Focus
Module 64.1: Summary of Basel III Reforms
Key Concepts
Answer Key for Module Quiz

READING 65

Basel III: Finalizing Post-Crisis Reforms

Exam Focus
Module 65.1: Basel III: Post-Crisis Reforms
Key Concepts
Answer Key for Module Quiz

Formulas
Index

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 Publication, 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 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 the frameworks issued 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 of 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 in 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, compliance risk, and on an as-needed basis, 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, specifically senior management in the 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 is 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 are 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 that 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. 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 are correlated with 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 the 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.