




2023 FRM[®]

Exam Prep

SchweserNotes[™]

Operational Risk and Resilience



PART II BOOK 3

KAPLAN[®] SCHWESER

Book 3: Operational Risk and Resilience

SchweserNotes™ 2023

FRM Part II



©2023 Kaplan, Inc. All rights reserved.

10 9 8 7 6 5 4 3 2 1

ISBN: 978-1-0788-3120-8

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 35

Introduction to Operational Risk and Resilience

Exam Focus

Module 35.1: Operational Risk Categories

Module 35.2: Operational Risk Characteristics

Key Concepts

Answer Key for Module Quizzes

READING 36

Risk Governance

Exam Focus

Module 36.1: Operational Risk Regulation and Governance

Module 36.2: Three Lines of Defense, Risk Appetite, and Risk Culture

Key Concepts

Answer Key for Module Quizzes

READING 37

Risk Identification

Exam Focus

Module 37.1: Identifying Operational Risks

Module 37.2: Operational Risk Taxonomies

Key Concepts

Answer Key for Module Quizzes

READING 38

Risk Measurement and Assessment

Exam Focus

Module 38.1: Operational Loss Data and Qualitative Risk Assessment

Module 38.2: Key Indicators and Quantitative Risk Assessment

Module 38.3: Operational Risk Capital and Resilience

Key Concepts

Answer Key for Module Quizzes

READING 39

Risk Mitigation

Exam Focus

Module 39.1: Risk Mitigation With Internal Controls and Process Design
Module 39.2: Operational Risk Mitigation Measures and Management
Key Concepts
Answer Key for Module Quizzes

READING 40

Risk Reporting

Exam Focus
Module 40.1: Organizational Committees
Module 40.2: Operational Risk Reporting Components
Module 40.3: Operational Risk Reporting Challenges
Module 40.4: External Reporting Best Practices
Key Concepts
Answer Key for Module Quizzes

READING 41

Integrated Risk Management

Exam Focus
Module 41.1: Enterprise Risk Management (ERM)
Module 41.2: Stress Testing
Key Concepts
Answer Key for Module Quizzes

STUDY SESSION 8—OPERATIONAL RISK FOCUS AREAS

READING 42

Cyber-Resilience: Range of Practices

Exam Focus
Module 42.1: Cyber Risks, Governance, and Supervision
Module 42.2: Cybersecurity Information Sharing Between Institutions and
Third-Party Risk
Key Concepts
Answer Key for Module Quizzes

READING 43

Case Study: Cyberthreats and Information Security Risks

Exam Focus
Module 43.1: Information Security Risks and Frameworks
Key Concepts
Answer Key for Module Quiz

READING 44

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

Exam Focus

Module 44.1: Management of Money Laundering and Financial Terrorism Risks

Key Concepts

Answer Key for Module Quiz

READING 45

Case Study: Financial Crime and Fraud

Exam Focus

Module 45.1: Financial Crime and Fraud Risk Management

Key Concepts

Answer Key for Module Quiz

READING 46

Guidance on Managing Outsourcing Risk

Exam Focus

Module 46.1: Managing Outsourcing Risk

Key Concepts

Answer Key for Module Quiz

READING 47

Case Study: Third-Party Risk Management

Exam Focus

Module 47.1: Third-Party Risk Management and Responsibilities

Key Concepts

Answer Key for Module Quiz

READING 48

Case Study: Investor Protection and Compliance Risks in Investment Activities

Exam Focus

Module 48.1: Investor Protection Regulations

Key Concepts

Answer Key for Module Quiz

READING 49

Supervisory Guidance on Model Risk Management

Exam Focus

Module 49.1: Model Risk Management

Module 49.2: Model Validation Process

Key Concepts

Answer Key for Module Quizzes

READING 50

Case Study: Model Risk and Model Validation

Exam Focus

Module 50.1: Model Risk and Model Validation

Key Concepts

Answer Key for Module Quiz

READING 51

Stress Testing Banks

Exam Focus

Module 51.1: Stress Testing

Module 51.2: Challenges in Modeling Losses and Revenues

Key Concepts

Answer Key for Module Quizzes

STUDY SESSION 9—CAPITAL AND REGULATORY FRAMEWORKS

READING 52

Risk Capital Attribution and Risk-Adjusted Performance Measurement

Exam Focus

Module 52.1: Risk-Adjusted Return on Capital

Module 52.2: RAROC, Hurdle Rate, and Adjusted RAROC

Module 52.3: Diversification Benefits and RAROC Best Practices

Key Concepts

Answer Key for Module Quizzes

READING 53

Range of Practices and Issues in Economic Capital Frameworks

Exam Focus

Module 53.1: Risk Measures and Risk Aggregation

Module 53.2: Validation, Dependency, Counterparty Credit Risk, and Interest
Rate Risk

Module 53.3: BIS Recommendations, Constraints and Opportunities, and Best
Practices and Concerns

Key Concepts

Answer Key for Module Quizzes

READING 54

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

Exam Focus

Module 54.1: The Federal Reserve's Capital Plan Rule

Module 54.2: Capital Adequacy Process

Module 54.3: Assessing the Impact of Capital Adequacy

Key Concepts

Answer Key for Module Quizzes

READING 55

Capital Regulation Before the Global Financial Crisis

Exam Focus

Module 55.1: Basel I Regulations and Revisions

Module 55.2: Basel II Regulations

Key Concepts

Answer Key for Module Quizzes

READING 56

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

Exam Focus

Module 56.1: Stressed VaR, Incremental Risk Capital Charge, and
Comprehensive Risk Charge

Module 56.2: Basel III Capital Requirements, Buffers, and Liquidity Risk
Management

Module 56.3: Contingent Convertible Bonds and Dodd-Frank Reform

Key Concepts

Answer Key for Module Quizzes

READING 57

High-Level Summary of Basel III Reforms

Exam Focus

Module 57.1: High-Level Summary of Basel III Reforms

Key Concepts

Answer Key for Module Quiz

READING 58

Basel III: Finalizing Post-Crisis Reforms

Exam Focus

Module 58.1: Basel III: Finalizing Post-Crisis Reforms

Key Concepts

Answer Key for Module Quiz

Formulas

Index

READINGS AND LEARNING OBJECTIVES

STUDY SESSION 7

35. 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:

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

36. 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:

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

37. 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:

- compare different top-down and bottom-up approaches and tools for identifying operational risks.
- describe best practices in the process of scenario analysis for operational risk.
- describe and apply an operational risk taxonomy and give examples of different taxonomies of operational risks.
- describe and apply the Level 1, 2, and 3 categories in the Basel operational risk taxonomy.

38. 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:

- explain best practices for the collection of operational loss data and reporting of operational loss incidents, including regulatory expectations.
- 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 and distinguish between the different quantitative approaches and models used to analyze operational risk.
- 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.

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

40. 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.

41. 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. summarize the role of Basel regulatory capital and the process of determining internal economic capital.
- c. describe elements of a 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

42. 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.

43. 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.

44. 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.

45. 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.

46. 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.

47. 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 case study involving a data breach caused by a third-party vendor employee.

48. 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 and provide lessons learned from the case studies involving violations of investor protection or compliance regulations.

49. 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.

50. 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.

51. Stress Testing Banks

Til Schuermann, (2014), “Stress Testing Banks,” *International Journal of Forecasting*, 30:3, 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

52. 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 risk-adjusted return on capital (RAROC) methodology and its use in capital budgeting.
- c. compute 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. compute 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.

53. 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 making 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.

54. 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

55. 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.

56. 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.

57. 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.

58. 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 35

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 35.1: OPERATIONAL RISK CATEGORIES

Operational Risk Management Framework

LO 35.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 35.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 35.1

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 35.2: OPERATIONAL RISK CHARACTERISTICS

LO 35.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 35.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.

U.K. Regulations

In the United Kingdom, existing ORM regulations were not replaced, but additional regulations were added in 2018 in a collaborative effort by the U.K. 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 35.1, 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 35.1: 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 U.K. 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 35.2

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. Heterogenous.
 - 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 35.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 35.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 35.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 35.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 35.1

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 35.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 35.b)

Module Quiz 35.2

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 35.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 35.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 35.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 36

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 36.1: OPERATIONAL RISK REGULATION AND GOVERNANCE

LO 36.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 Pillars 1 and 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 that is to be used starting January 1, 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):

$$\text{ORC} = \text{business indicator component (BIC)} \times \text{internal loss multiplier (ILM)}$$

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:
 - $15 \times$ 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 36.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 procedures pertaining to ORM within the bank. By carefully documenting the agenda, the actions taken, and the justification behind those actions (in the minutes of the meetings), committees will demonstrate a sufficient level of operational risk governance required by supervisors.

Policies and procedures serve as internal controls and provide detailed steps on the performance of specific processes. The idea here is to serve as initial training for new employees (or refresher training for existing employees) to minimize errors in their performance of job functions. Policies and procedures remain useful only if they are

actively used by employees, change appropriately with the business and industry practices, and are consistent with the bank’s day-to-day operations.

Board of Directors Role (Operational Risk)

Among its many duties, the board must consider risk management—specifically, establishing the bank’s risk tolerance and subsequently operating within the stated constraints.

Specific duties of the board within an ORMF context (per regulators) include the following:

- Approving the ORMF
- Establishing ongoing updates to the ORMF
- Ensuring senior management executes the policies and procedures within the ORMF throughout all levels of the bank

Additionally, the board must create a culture of risk management that is articulated throughout the bank to its staff at all levels. Training is central to fulfilling that requirement, both in terms of the training for board members as well as the relevant staff within the bank whose day-to-day duties involve ORM.

Board of Directors Role (Operational Resilience)

The board must clearly articulate (throughout the organization) its approach to and goals of operational resilience. Such an approach requires integration of the bank’s risk tolerance and its capacity to withstand interruption to its key operations. It must also account for how the bank can continue to operate effectively given “stressed” situations that are harsh and have a low probability of occurrence, and yet remain reasonably foreseen.

Senior management ultimately reports to the board in terms of the operational resiliency methodology, and the board should request periodic reports from them, especially regarding any major issues that would negatively impact the bank’s ability to operate normally. Additionally, it is the board’s responsibility to direct enough funds and other support toward promoting operational resilience within the bank.

Similar to operational risk, training in operational resilience is crucial, and it applies to both the board and all relevant employees. In addition, board members must have relevant skills and experience to properly perform in their roles.



MODULE QUIZ 36.1

1. The Rosedale Community Bank (RCB) has average annual performance over the past three years as follows:

Interest, leases, and dividend income:	EUR740 million
Fee income:	EUR185 million
Fee expenses:	EUR125 million
Other operating income:	EUR45 million
Other operating expense:	EUR25 million
Net (loss) of banking and trading book:	(EUR100 million)

Using only the information provided, what is the yearly average business indicator (BI) for RCB using the standardized approach?

- A. EUR720 million.
 - B. EUR870 million.
 - C. EUR920 million.
 - D. EUR1,070 million.
2. The following data on a bank is available:
- Annual operational losses incurred over the last 10 consecutive years = EUR80 million
 - Business indicator (BI) = EUR900 million

Using the standardized approach for calculating operational risk capital, which of the following statements is most accurate?

- A. The internal loss multiplier (ILM) is less than 1.
 - B. The internal loss multiplier (ILM) is greater than 1.
 - C. The percentage used to calculate the business indicator component (BIC) is 15%.
 - D. The percentage used to calculate the business indicator component (BIC) is 18%.
3. Within a bank, who is ultimately responsible for operational risk management and resilience?
- A. Employees.
 - B. Chief risk officer.
 - C. Board of directors.
 - D. Senior management team.

MODULE 36.2: THREE LINES OF DEFENSE, RISK APPETITE, AND RISK CULTURE

LO 36.c: Describe the “three lines of defense” model for operational risk governance and compare roles and responsibilities for each line of defense.

The Three Lines of Defense Model

Controls and risk management within a bank can be thought of in three interconnected lines:

- *Line 1.* This is the individual business unit management, or the “front line.”
- *Line 2.* This is the objective review of the risk management process in Line 1. It also includes a cross-examination of the risk management work performed by the business units in Line 1. Line 2 is also known as the **corporate operational risk function (CORF)**.
- *Line 3.* This is the objective internal audit of work performed in Lines 1 and 2.

In real life, the three lines may be problematic to put into action as stated, and there will be differences between banks depending on the size and structure. For example, given the decentralized nature of ORM, differentiating between the three lines is not always easy. Also, some areas of risk management (e.g., legal and compliance, IT

security) overlap multiple lines and cannot reasonably be classified into only one single line of defense.

Delineation of the Lines of Defense

It is actually the roles and duties performed in each group that best delineate the three lines. Maintaining independence and objectivity of the CORF within the firm is key. Smaller entities might do so through controls such as segregation of duties and independent review of work performed. For larger entities, the CORF would be required to engineer and manage the ORMF within the entire bank, and the CORF would be wholly separate from the bank's risk-generating (profit-generating) groups. A thorough clarification of the objectives and duties of the CORF is needed that is consistent with the operational scope of a given bank.

For banks that are not sufficiently large, some groups may not be able to clearly delineate between first-line and second-line roles. Due to staffing shortages, sometimes first-line and second-line duties need to be combined into a hybrid function and performed within the same group (e.g., legal, human resources, finance). As a result, the BCBS would mandate clarity in delineating the duties and carefully demonstrating that the two lines are independent. For example, writing up business contracts is typically a first-line duty, and then dealing with the legal issues (e.g., litigation) that arise in the course of business transactions pertaining to those contracts could be a second-line duty—but in a hybrid function, the two duties would be performed in a single legal department. In such a case, the legal department must demonstrate independence between those two duties by ensuring, for example, that employees who write up contracts are not the same employees who are litigating the related matters.

First Line of Defense

The front line is essentially the “business” or the risk owners. The risk owners of the bank generate, but also measure and manage, those risks. For example, the leader of the trading department “owns” the bank's trading risk. Therefore, it is really the risk owners (employees and department head) that manage the risk they generate as opposed to the risk management department.

A proper front line defense would determine which significant operational risks are faced by the bank that need to be managed, create sufficient controls to deal with those risks, evaluate whether those controls are operating as intended, and provide oversight and reporting of operational risk within the business line.

To the extent that the front line is unable to perform its operational risk duties, it needs to inform the CORF in the second line of defense. In addition, any examples of control weaknesses, process weaknesses, and losses that stem from a lack of proper controls need to be escalated to the second line.

Risk Specialists

Within some business groups or larger banks, there could be a so-called risk specialist or champion role who functions as a midway point (“Line 1.5”) between Lines 1 and 2. Such risk specialists would likely serve as the key spokesperson for risk issues in a given business group as well as being responsible for gathering information on the

group's risk incidents and losses. In addition, they would anticipate the key risks and controls within the group and ensure that risk management plans are completed. Having a risk specialist within the first line does not mean that responsibility for all operational risk is taken on by the risk specialist.

Second Line of Defense

Within Line 2, the purpose is to oversee and question what has been done in Line 1. To ensure proper independence, Line 2 must not have any involvement in Line 1, or else there will be a self-review threat. Risk management staff in Line 2 must be thoroughly trained in a broad range of risk matters, as a starting point. On top of that, they must understand the business environment and have thorough knowledge of the relevant regulations to avoid potentially costly regulatory infractions.

The role of a robust second line would include the following duties:

- Developing ORM policies and procedures and providing such training to employees
- Approaching the work in risk management done by Line 1 in a fresh and objective manner
- Cross-examining the work done by Line 1 (e.g., use of ORM tools, risk measurement, reporting) and documenting that there has been useful cross-examination performed
- Overseeing and adding to the bank's monitoring and reporting functions

The second line is also useful when it comes to business decisions. For any major business decision, such as a potential acquisition or divestiture, the second line would be able to provide input on potential incremental risks and methods of managing such risks. Furthermore, the effectiveness of the second line is enhanced when it is given the power to overturn business decisions that do not comply with regulations and/or breach any board-authorized risk limits.

With a clear separation of duties between Lines 1 and 2, it may lead to duplication of work between Lines 2 and 3 (internal audit). In addition, the cross-examination by Line 2 of Line 1 may be ineffective until the risk management work in Line 1 is fully executed and has had time to produce its intended outcomes.

As a result, the second line should focus on guidance and informing all relevant staff about ORM. Such guidance could include a thorough, but clear, definition of operational risk as well as the process for noting and reporting operational incidents. It would also be helpful to explain the positives of having strong ORM in place as well as to explain the negatives of having weak ORM. Furthermore, practical and hands-on training to which employees can relate in their day-to-day work would likely increase employee acceptance of the ORMF. Examples of such training include root-cause and scenario analysis.

Although there may appear to be a fine line between guidance and challenge, Line 2 can avoid the self-review threat by not "coaching" Line 1 on the "correct answers." In other words, Line 2 managers can provide training workshops to Line 1 employees and managers and encourage them to provide feedback and answers to specific questions. Only after the feedback and answers are received should the Line 2 manager provide any challenge. In other words, Line 1 is responsible for its own risk assessment and controls, and Line 2 provides the challenge in an effort to improve them.

Third Line of Defense

Line 3 is internal audit and is completely separate from risk management. It takes an objective approach in reviewing the controls and adherence to the bank's stated policies and procedures for each group. Internal audit maintains its independence from risk management partly by establishing its own list of significant risks faced by the bank (which may not always be the same as those listed by risk management). Lines 2 and 3 will occasionally share information and conclusions in an effort to reduce any redundancies.

The Institute of Internal Auditors (IIA) has provided the following guidance on how the internal audit department could work with the risk management, compliance, and finance department:

- Strictly speaking, internal audit must be separate from the other three departments.
- Internal audit is to provide an evaluation of the sufficiency and competence of the other three departments. There should not be full reliance by internal audit of the work done by the other three departments pertaining to internal controls and risk management. Instead, internal audit should perform its own independent analysis on a reasonable number of samples.
- Reliance by internal audit of any work done by the other three departments pertaining to risk assessment or audit testing is permissible only after internal audit has assessed the reliability of the work done.

Internal audit could provide independent assurance both to internal and external stakeholders. Therefore, maintaining the independence of internal audit could be achieved by having them report directly to one of the bank's nonexecutive directors.

LO 36.d: Explain best practices and regulatory expectations for the development of a risk appetite for operational risk and for a strong risk culture.

Risk Appetite (Regulatory Expectations)

The board of directors is often responsible for determining the bank's risk appetite, or the permitted level of risk. A key challenge here is doing so for nonfinancial risks.

Determining risk appetite requires an evaluation of the bank's significant risks, defining limits to distinguish between acceptable and unacceptable incidents, and establishing controls in conjunction with those limits. A proper definition of risk appetite may expose inconsistencies between reported versus actual ORM. Ideally, the definition of risk appetite will set the key objectives of the bank's control system.

Risk appetite statements should be straightforward to articulate and comprehend, and they should explain why they accept, decline, or minimize specific risks. Overall, risk appetite must be congruent with overall strategy and mission. Risk appetite limits are monitored through metrics such as exposure limits, significant controls, and acceptable loss events. Risk appetite should account for the future and be considered in scenario analysis and stress testing. Regarding stress testing, there should be consideration of incidents that might take the bank beyond the established risk appetite limits.

Regulators link operational risk appetite to risk appetite statements. An underlying assumption is that risk appetite statements are congruent with the bank's operations. For example, stating that there is a "low tolerance for processing errors" must be supported by robust controls and oversight measures to show regulators that the risk of errors is actually low.

The board is responsible for risk limits and must perform ongoing testing on them. The duty is usually passed to the board risk committee, who then require the assistance of the risk management department to put such limits in practice and to perform the associated monitoring and reporting duties. Risk appetite must be congruent with the bank's business objectives and risk management, and business strategies should be aligned.

Risk Appetite (Best Practices)

According to the BCBS, risk appetite should state the reasons for accepting or declining specific risks because accepting risks is necessary to earn sufficient returns, and declining risks entails an opportunity (implied) cost. Therefore, risk appetite statements should always consider the risk-return tradeoff.

Risk appetite establishes risk exposure limits at the business unit level, sets the basic requirements of the significant controls, and sets limits on the frequency and impact of acceptable incidents. The underlying metrics are called boundaries or key risk indicators (KRIs), and they could be quantitative or qualitative.

Risk appetite statements are likely to be conveyed based on the key types of risk. Some financial institutions are more focused on multiple forms of transaction processing—and, therefore, they may choose to convey risk appetite through their main processes. In fact, there might be a separate risk appetite for each process. Newer operational resiliency regulations now mean that financial institutions must consider disruption risk by setting a tolerance threshold on key business services.

Risk appetite statements should include the significant controls or control systems. The control systems should be clearly documented for each key risk faced by the bank. Doing so provides some comfort to banking clients and regulators that the bank takes its risk management goals seriously. Subsequently, oversight measures such as limits and KRIs are useful for management to gain comfort that the bank is functioning as expected. An analysis of near misses and incidents in the context of allowable thresholds provides insight as to whether controls are sufficiently robust to keep the financial impact of incidents within an acceptable range.

Proper risk appetite governance would entail assigning a risk owner to each risk type. In working down the risk appetite governance structure, it is possible, for example, to have controls owners and metrics owners for specific risks. Risk owners function as the front line within the risk management function; they oversee and manage the risks in risk appetite statements. Controls owners must engineer and implement controls, while metrics owners must gather, report, and oversee the performance metrics in context of the bank's risk appetite.

Risk Culture

Regulators place great emphasis on strong risk culture within a bank because it reduces operational risk (e.g., lowers losses from incidents) and increases operational resilience (e.g., quicker recovery from incidents). An effective risk culture and ORMF can be demonstrated through the enforcement of the bank's policies and procedures and awareness of risk throughout the bank, among many factors.

Regulators also link risk culture with ethical behavior. As a result, regulators expect the board to have a code of conduct (or something similar) requiring compliance by all board members and employees. The idea is that ethical behavior should reduce operational risk.

The common phrase "tone at the top" is demonstrated by leadership of risk culture by the board and implementation by top management. Both the board and top management should lead by example through their actions (e.g., ethical behavior) and by communication of acceptable employee behavior.

In the context of taking risk, a significant portion of management compensation might be provided through stock options. In such an instance, managers would more likely be cautious and prudent in taking risk so as to limit their downside and maintain their livelihood. They are far less likely to engage in risky activities to maximize their upside at the cost of significant downside risk. At the same time, setting management bonus payouts based on unreasonably high growth and profit goals could lead to excessively risky behavior and an overall toxic risk culture.

A key part of risk culture lies with proper training and the transmission of essential risk concepts to all employees. This could be achieved through a combination of initial training for new employees, ongoing online training for existing employees, and specialist training for those employees working directly in the risk department. The training should occur periodically, and many jurisdictions require formal training for top management and the board.

The concept of reinforcement in the context of a code of conduct (together with tone at the top) is important to maintain a strong risk culture. Reinforcement can be thought of as the bank emphasizing the need for its employees to comply with the rules, but also for the bank to avoid laying blame. With laying blame, it is encouraged for individuals to use judgment and to escalate issues as they see fit, all without the fear of retribution. A real-life example of such behavior in the workplace would be whistleblowing, which continues to be one of the strongest controls to minimize error and fraud. To conclude the discussion, the concept of blame could be elaborated to deal with situations where repeated infractions and negligence by employees would justify some blame and consequences. In addition, at an entity level, regulators are likely to penalize banks that attempt to hide control weaknesses and incidents.



MODULE QUIZ 36.2

1. Within the context of the three lines of defense model, risk champions (or risk specialists) are most likely to be included in which lines?
 - A. Line 1 only.
 - B. Lines 1 or 2.
 - C. Line 2 only.
 - D. Line 3 only.

2. Which of the following items is least likely to appear in a bank's risk appetite statement?
- A. Key controls.
 - B. Exposure limits.
 - C. Expected losses.
 - D. Tolerated incidents.

KEY CONCEPTS

LO 36.a

Basel II includes the following three pillars for regulation of operational risk.

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 and risk disclosures by banks
- Underlying idea is to have greater capital reserves to balance greater risks taken

LO 36.b

An example and description of a risk committee structure for a 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

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 procedures pertaining to ORM within the bank. By carefully documenting the agenda, the actions taken, and the justification behind those actions, committees will demonstrate a sufficient level of operational risk governance required by supervisors.

Specific duties of the board within an ORMF context (per regulators) include the following:

- Approving the ORMF
- Establishing ongoing updates of the ORMF
- Ensuring senior management executes the policies and procedures within the ORMF throughout all levels of the bank

LO 36.c

Controls and risk management within a bank can be thought of in three interconnected lines.

Line 1 is the front line, or the risk owners. The risk owners of the bank generate, but also measure and manage, those risks. Therefore, it is really the risk owners (employees and department head) that manage the risk they generate as opposed to the risk management department. Within some business groups or larger banks, there could be a so-called risk specialist or champion role who functions as a midway point (“Line 1.5”) between Lines 1 and 2.

Within Line 2, the purpose is to oversee and question what has been done in Line 1. To ensure proper independence, Line 2 must not have any involvement in Line 1, or else there will be a self-review threat. Risk management staff in Line 2 must be thoroughly trained in a broad range of risk matters, as a starting point. On top of that, they must understand the business environment and have thorough knowledge of the relevant regulations to avoid potentially costly regulatory infractions.

The role of a robust second line would include the following duties:

- Developing ORM policies and procedures and providing such training to employees
- Approaching the work in risk management done by Line 1 in a fresh and objective manner
- Cross-examining the work done by Line 1 (e.g., use of ORM tools, risk measurement, reporting) and document that there has been useful cross-examination performed
- Overseeing and adding to the bank’s monitoring and reporting functions

Line 3 is the objective internal audit of work performed in Lines 1 and 2. It is completely separate of risk management. It takes an objective approach in reviewing the controls and adherence to the bank’s stated policies and procedures for each group. Internal audit maintains its independence from risk management partly by establishing

its own list of significant risks faced by the bank (which may not always be the same as those listed by risk management). Lines 2 and 3 will occasionally share information and conclusions in an effort to reduce any redundancies.

In real life, the three lines may be problematic to put into action as stated, and there will be differences between banks depending on the size and structure. For example, given the decentralized nature of ORM, differentiating between the three lines is not always easy. Also, some areas of risk management (e.g., legal and compliance, IT security) overlap multiple lines and cannot reasonably be classified into only one single line of defense.

LO 36.d

The board of directors is often responsible for determining the bank's risk appetite. Determining risk appetite requires an evaluation of the bank's significant risks, defining limits to distinguish between acceptable and unacceptable incidents, and establishing controls in conjunction with those limits. Risk appetite statements should be straightforward to articulate and comprehend, and they should explain why they accept, decline, or minimize specific risks. Regulators link operational risk appetite to risk appetite statements. The board is responsible for risk limits and must perform ongoing testing on them; the duty is usually passed to the board risk committee and the risk management department.

Risk appetite establishes risk exposure limits at the business unit level, sets the basic requirements of the significant controls, and sets limits on the frequency and impact of acceptable incidents. Risk appetite statements are likely to be conveyed based on the key types of risk, and newer operational resiliency regulations now mean that financial institutions must consider disruption risk by setting a tolerance threshold on key business services. Risk appetite statements should include the significant controls or control systems. The control systems should be clearly documented for each key risk faced by the bank. Proper risk appetite governance would entail assigning a risk owner to each risk type. In working down the risk appetite governance structure, it is possible to have controls owners and metrics owners for specific risks.

Regulators place great emphasis on strong risk culture within a bank because it reduces operational risk and increases operational resilience. An effective risk culture and ORMF can be demonstrated through the enforcement of the bank's policies and procedures and awareness of risk throughout the bank, among many factors. Regulators also link risk culture with ethical behavior. As a result, regulators expect the board to have a code of conduct requiring compliance by all board members and employees. The idea is that ethical behavior should reduce operational risk. The common phrase "tone at the top" is demonstrated by leadership of risk culture by the board and implementation by top management. In addition, proper compensation structure and training will promote a robust risk culture.

ANSWER KEY FOR MODULE QUIZZES

Module Quiz 36.1

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

ILDC = EUR740 million

SC consists of the higher of fee income and fee expenses *plus* the higher of other operating income and operating expense = EUR185 million + EUR45 million = EUR230 million

FC consists of the *absolute value* of the net income/loss of the banking book and the trading book = EUR100 million

BI = EUR740 million + EUR230 million + EUR100 million = EUR1,070 million.

(LO 36.a)

2. **B** BI is given as EUR900 million. Because it is less than EUR1 billion, the percentage used to calculate BIC should be 12%.

The loss component (LC) is calculated as $15 \times$ annual operational losses incurred over the last 10 consecutive years = $15 \times$ EUR80 million = EUR1,200 million.

Because $LC > BI$, then ILM is > 1 , and more capital is required. (LO 36.a)

3. **C** The board of directors is ultimately responsible for the operational risk management function, though risk management tasks are delegated to senior management and employees. The chief risk officer would be considered part of senior management, but that role does not assume ultimate responsibility for risk management. (LO 36.b)

Module Quiz 36.2

1. **A** Risk champions or risk specialists are sometimes considered “Line 1.5” and, therefore, included in Line 1 only. (LO 36.c)
2. **C** Expected losses are not likely to be included in a risk appetite statement. Risk appetite consists of items such as exposure limits, key controls, and tolerated incidents. (LO 36.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 3.

READING 37

RISK IDENTIFICATION

Study Session 7

EXAM FOCUS

This reading focuses on the first of four crucial parts of the operational risk management framework (ORMF): (1) identification, (2) measurement and assessment, (3) mitigation, and (4) reporting. Once a risk has been identified, the fundamental question becomes whether to accept the risk and capitalize on it or to reject it and apply mitigation techniques. For the exam, focus less on the mere differences between top-down and bottom-up approaches, and more on understanding the various techniques used in both approaches (e.g., exposures and vulnerabilities, risk wheel, risk and control self-assessment, process mapping). Also, be familiar with the structure for scenario analysis. Finally, understand the Basel risk taxonomy and how it is supplemented with the Operational Riskdata eXchange (ORX) risk taxonomy.

MODULE 37.1: IDENTIFYING OPERATIONAL RISKS

LO 37.a: Compare different top-down and bottom-up approaches and tools for identifying operational risks.

Scope of Risk Identification

There are two approaches to consider for identifying operational risks: the top-down approach and the bottom-up approach. The top-down approach can be subdivided into three general levels. It begins with the board and senior management, then moves down to the separate divisions or business units, and then to the separate business processes. For the bottom-up approach, the business units assess their own risk. By combining both risk identification approaches, we can obtain a more thorough and in-depth understanding of the bank's operational risk.

Top-Down Approach

The top-down approach attempts to determine the significant risks currently facing the bank that would potentially harm its business strategies (e.g., developing and growing an online trading business is an IT risk). In looking at each of the identified risks, they must be rated in terms of impact and then prioritized in terms of importance. Identifying risks could involve key risk owners such as senior management, business

unit leaders, or department heads of important functions such as legal and compliance. It is most effective to do so through brainstorming sessions supplemented with the use of additional methods, including risk wheels, analyses of significant exposures and vulnerabilities, and consideration of potential future risks.

Such brainstorming sessions are likely to occur quarterly or semiannually, but the frequency ultimately depends on the stability and rate of business growth together with the corresponding growth of incremental risks. If the bank is involved in emerging technologies (e.g., automated financial advisors) and/or complex technology, then the risk identification sessions would likely need to occur more frequently and/or be more thorough in scope.

Top-down risk identification sessions can form the basis for scenario analysis; the output from such sessions could also be integrated into the risk and control self-assessment (RCSA) process. In addition to identifying significant risks, such sessions can be used to increase the bank's profitability as well as prevent sudden unexpected losses.

Bottom-Up Approach

The bottom-up approach is not firmwide and focuses on a specific business unit or process. The bottom-up approach is usually done in an RCSA context whereby risks at the business unit level would be identified. The easiest way to distinguish between top down and bottom up is that risk identification for the top-down approach takes place among senior management, and risk identification for the bottom-up approach takes place among the rest of the employees (including lower and middle management).

The breadth within the bank of a risk identification session is positively correlated to the priority as well as the nature of the risk. In practice, from a cost-benefit perspective, it is not optimal to mitigate all risks—so some prioritization of risks is usually required. This means accepting some level of risk that the bank can control effectively. Finally, the classification of risks (e.g., by type or by activity) provides insight into possible patterns of risk or areas of weakness to resolve.

Top-Down Risk Identification Tools

The collection of risks identified forms part of the bank's overall risk inventory—or alternatively, its risk register or risk universe.

Exposures and Vulnerabilities

When identifying **exposures**, consideration is usually given to major clients, key sources of revenue, distribution channels, suppliers, key persons, service providers (e.g., IT systems, transaction processing), and regulations. Reliance on third parties and outsourcing activities, for example, means that banks will face the related operational risks, and the exposures are based on any significant failure(s) arising from them.

Vulnerabilities represent weak spots within the firm such as obsolete processes, control weaknesses, overdue items (e.g., maintenance, testing, updating), or neglected oversight of peripheral business units. The risk occurs where a given vulnerability also links to a significant exposure (e.g., unmonitored rogue trader) with the potential for very large losses or even bankruptcy. By identifying exposures and vulnerabilities

together, it is possible to isolate any potential problems to a specific business line and potentially facilitate the resolution within that business line.

Risk Wheel

A **risk wheel** illustrates selected or common risks in a circle and assists in understanding how the different types of risk are integrated—and, therefore, shows a deeper understanding of the causes and effects.

A risk wheel for a bank could have the following *cogs*: business objectives, labor market, reputation, technology, regulation, economy, natural events, data and information, and business continuity. A simple example could be a weather-related disaster (natural events cog) that results in a multi-day service outage (business continuity cog), and should the disruption remain for an extended period, there could be harm to the bank's reputation (reputation cog). Such causal analysis of risks is useful in risk prioritization and mitigation activities as it is proactive and gets to the root of the problem, rather than being reactive only to the symptoms.

Emerging Risks

With more volatility in the markets, the rise in new technologies and online presence of banks, and the related cybersecurity issues, determining emerging risks has significantly increased in importance. Emerging risks can be divided into two categories: (1) predictable and (2) unpredictable. For **predictable risks**, they can be subdivided into well-known ones such as cyber, regulatory, and climate change. Horizon scanning is used to identify the risks that are less known and are beginning to show up. For **unpredictable risks** (e.g., global pandemic), the best form of defense is overall preparedness and the development of resiliency over time.

Global opinion surveys feature key emerging risks on an annual basis, but it is more important to determine the risks within a specific bank. Using a horizon scanning technique called PESTLE analysis, there is consideration of six factors: political, economic, social, technological, legal, and environmental. Rather than doing a potentially unwieldy analysis of all the changes in the bank's operating environment, there should be a focus on only the changes that potentially have a negative effect on the bank's mission and long-term strategy. In addition, analysis should focus on the specific threats that would be considered in scenario analysis and contingency planning.

The largest banks have been analyzing research and trends in areas directly related to their business, including innovative and competing technology. Machine learning and big data analysis have significant potential to be used for identifying operational risks. Emerging risk committees that meet on a quarterly basis have also been used. They focus on key issues primarily related to compliance risks, consisting of specialists in each of the countries where the bank operates.

Bottom-Up Risk Identification Tools

Event and Loss Data Analysis

Using historical information from internal sources or from competitors or industry sources is more reliable to forecast future potential losses when markets are stable.

Internal losses provide a sense of the level of operational risk concentration within the bank. Losses usually occur in the back offices, starting with financial markets, followed by retail, and then IT. The level of operational risk is highly dependent on transaction volume and size. Recurring internal losses could be an indication of weak internal controls, but if they are instead determined to be a regular “cost of doing business,” then they need to be integrated into pricing decisions. Unexpected internal losses would be addressed in risk identification.

External losses occur at other banks, and Operational Riskdata eXchange (ORX) is a major data consortium. Both serve as useful sources of information on incidents to help a bank identify and evaluate its internal risks. For major incidents reported by other banks, it is useful to think whether a similar incident could happen to the given bank. If so, then the bank should look at how it manages its risks and make appropriate changes to minimize the probability of the same thing happening to them.

Near misses are exactly that; they had the potential to become an operational loss, but did not. The key point is that there was luck involved and, had a loss occurred, it would not have been prevented by the existing controls. There are two general aspects to near misses: they have no monetary cost attached to them and they bring focus to control weaknesses that should be addressed. As such, near misses should be reported as they provide an inexpensive learning experience, and they allow the bank to continually improve their control system.

Keeping a log of prior incidents with actual or no losses is useful information for periodic risk committee meetings. It may reveal an evolution in the risk profile as well as encourage changes to be made to risk management practices as needed.

Risk and Control Self-Assessment

Risk and control self-assessment (RCSA) could involve the entire bank, a particular business unit, or a particular department in a self-evaluation of the key operational risks, the controls to address those risks, and the strength of those controls. In effect, the bank may be able to determine the level of residual risk that is not accounted for by controls currently in place. RCSAs are usually performed by the second line of defense regarding the risks in the first line of defense. Sometimes, the data-gathering process is facilitated by using questionnaires.

In their standard workshop format, RCSAs are one of the main approaches used by banks for both operational risk identification and risk assessment. Choosing appropriate people for RCSAs will enhance its usefulness, and in that regard, the staff who have been there the longest as well as newly hired staff are two of the most relevant groups to choose from. Regarding experienced staff, they serve as a benchmark and provide insight on history as well as potentially providing rationales for past practices. Regarding newly hired staff, it is useful to obtain their views on business practices at their new employer, especially for new hires who have experienced far different work environments in the past. Those insights could be used to assess the bank’s strengths and weaknesses.

RCSAs are usually done every year, and in some cases, after any major change in the bank's risk profile (e.g., major cyber event at a competitor, significant regulatory penalty levied on a competitor for noncompliance) or a change in overall environment (e.g., global pandemic). Care needs to be taken not to perform RCSAs too frequently, or else it becomes more like a checklist task and not an insightful and value-added exercise.

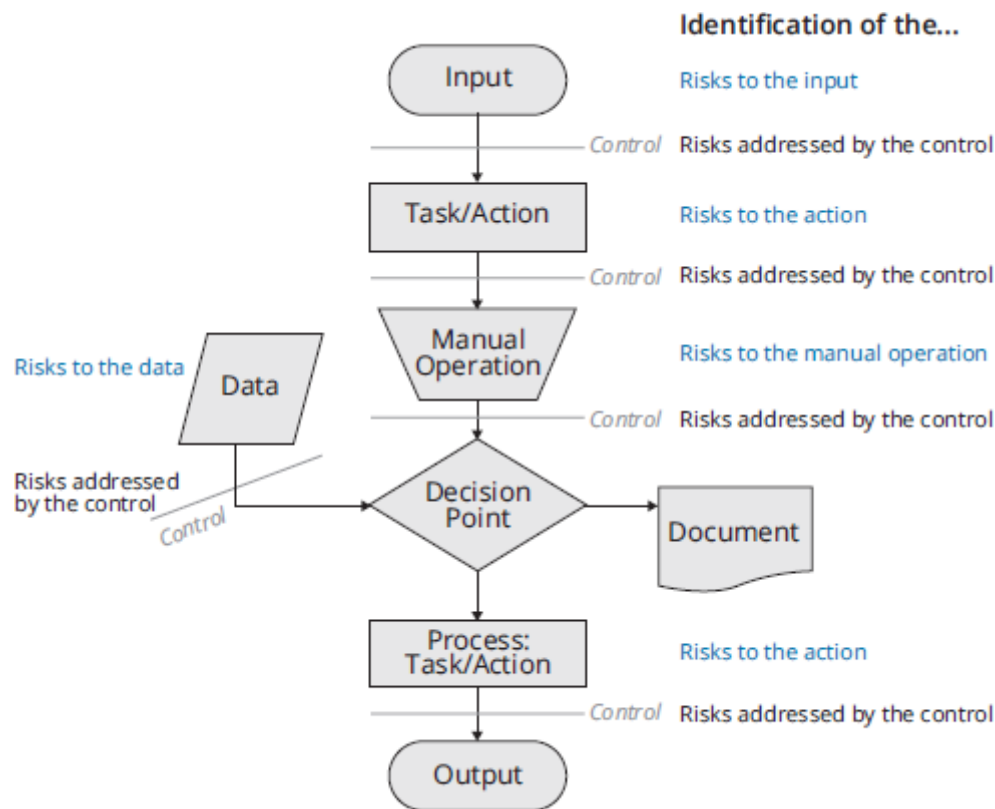
In conducting an RCSA, if there is an excessive level of detail in risk identification, then the outcome may not be so useful. For example, such an RCSA may yield an eclectic mix of minor and mundane risks that may only occur occasionally and have limited financial impact.

Process Mapping

Process mapping involves clearly stating the individual steps of a given process and determining any potential problem(s) in each step. A more realistic approach might be to examine the controls and attempt to tie them to the risks that they are meant to mitigate, with the outcome of determining whether certain risks are undercontrolled or overcontrolled.

Choosing the right amount of detail in process mapping is important in terms of how useful it will be. Excessive detail means that process mapping will take too long and probably focus on less important points. Insufficient detail means that process mapping will not provide sufficient insight. Striking a balance between the two occurs when each step ties into a key action together with its control(s). When process mapping is applied to determining risks, the controls are linked to the risks being mitigated, and there is consideration of the potential problems that could occur at each step. An illustration of process mapping is provided in Figure 37.1.

Figure 37.1: Process Mapping



Scenario Analysis Best Practices

Scenario/stress test identification is the bridging step between risk identification and scenario analysis. The scenarios considered are meant to be extreme and financially severe; they could occur, but are far less likely. Examples include natural disasters, global pandemics, major cyberattacks, and major business disruptions.

Consistent with the introductory description just listed, the Basel Committee on Banking Supervision (BCBS) guidance states that scenario analysis includes “low probability and high severity events, some of which could result in severe operational risk losses.” They go on to state that scenario analysis is used for operational risk and that resilience scenarios are used in business continuity planning so as to reduce the risk and impact of service disruptions.

and qualitative (e.g., legal, reputation) impacts. In terms of business continuity, the focus should be on service resumption; therefore, recovery time objectives (RTOs) and recovery point objectives (RPOs) would be applicable; the RTO and RPO enable the bank to determine how much data it can lose and how long it can be down.

Finally, the BCBS guidance suggests that there should also be provisions for potential unforeseen incidents that could cause major business disruptions.

Brainstorming Methods

Scenario analysis is fraught with pitfalls, including a lack of consistency with methodology as well as the existence of behavioral biases. At the same time, regulators are mandating that scenario analysis results remain consistent after numerous iterations, and that requires neutrality during the scenario identification and assessment process. Achieving such neutrality requires the use of empirical evidence, explanations for how or why a specific scenario was developed, and detailed write-ups to support the assumptions and methodology used in developing the scenarios.

A carefully selected set of documents may be provided to participants before a brainstorming session for scenario identification. Such documents may include the following: external and internal loss data (including specific major incidents and near misses), RCSA feedback, key risk indicator scores, concentrated exposures, and vulnerabilities. Alternatively, the documents are not given to the participants until later to avoid any potential biases and to allow participants to keep an open mind.

Participants are usually members of upper management from the various business units within the bank. Having participants from outside the bank who are risk specialists would be ideal, but this does not happen frequently. External participants could be useful in avoiding myopia whereby there is undue emphasis in the current period on recent events, with such events only to be forgotten even a few years later. In addition, external participants can help to temper the undue emphasis on losses originating externally. In fact, many significant losses by banks occur internally (e.g., rogue trading, internal IT system malfunctions) that also give rise to significant regulatory penalties.

The first step in a scenario workshop is the generation phase, which creates many scenarios that will be screened and narrowed down to selected ones to be further pursued in scenario selection (see next). Workshop facilitators tend to be operational risk management specialists who establish the discussions, monitor them, and come to preliminary conclusions and decisions, considering the feedback of all participants. Facilitators can ask leading and carefully worded questions to assist participants in considering significant losses incurred by the bank in the past as well as ones that could occur in the future. By creating an abundance of scenarios, the facilitator could then address each one of them and solicit feedback from all participants. The scenarios are elaborated and refined, and then the facilitator can classify the scenarios into risk type or impact, which may lead to further discussion and additional scenarios. Within this step, a technique known as silent voting might be used. Here, participants document a few concerns that may have occurred at the bank and could be viewed as continual threats. A key advantage of silent voting is to avoid any potential biases

caused by strong personalities or conversations steered into specific directions by a dominant participant.

The next step in a scenario workshop is scenario selection whereby a few scenarios may be combined, while others are dropped or added so as to come up with a final list that will be assessed. Combined scenarios may occur when the effect(s) on the bank are the same, but they have varying external causes. For example, damage to tangible assets could have been caused by a weather event or civil unrest. Scenarios are usually dropped when it is determined that the impact on the bank is immaterial and/or the potential loss is insufficient to cause a major disruption to operations. Scenarios that are retained or subsequently added to be assessed are ones that have a larger financial impact and are relevant to the bank's operations. Using an example of a midsized bank, there could be about 30 scenarios identified with about half of them remaining after scenario selection; the numbers would likely increase or decrease proportionally for smaller or larger banks.

Banks may find it helpful to cross-check their specific scenarios with ones made available by the Operational Risk Insurance Consortium (ORIC) or the ORX for any omissions. If done properly, it should occur only after the scenario generation process has occurred to avoid introducing any unintended biases.



MODULE QUIZ 37.1

1. In the context of risk identification, which of the following items is most likely to be considered a vulnerability?
 - A. Principal regulator.
 - B. Critical third parties.
 - C. Stand-alone IT systems.
 - D. Main drivers of revenue.
2. The chief risk officer (CRO) at a local bank is more in favor of an assessment of operational risk at a more local and detailed level. Which of the following risk identification tools is the CRO least likely to recommend?
 - A. Risk wheel.
 - B. Process mapping.
 - C. Analysis of near misses.
 - D. Risk and control self-assessment.
3. Which of the following statements regarding scenario analysis workshops and brainstorming sessions at a large bank is most accurate?
 - A. The assumptions used in scenario analysis can only be based on real-life data.
 - B. The facilitators of the workshops and sessions should be taken from the board of directors and senior management.
 - C. The participants in the workshops and sessions should be taken from a full range of seniority levels within the different business units.
 - D. The most common procedure is to withhold a "preparation pack" of documents from participants and distribute them after the generation phase to minimize any bias introduced to the sessions.

MODULE 37.2: OPERATIONAL RISK TAXONOMIES

LO 37.c: Describe and apply an operational risk taxonomy and give examples of different taxonomies of operational risks.

LO 37.d: Describe and apply the Level 1, 2, and 3 categories in the Basel operational risk taxonomy.

A definition of **operational risk** within the financial sector is “the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events.” In describing risks, it is critical to delineate between causes, events, and impacts. For example, a description of risk could be “risk of service interruptions and loss of reputation (impact) due to IT breakdowns (event) caused by lack of timely maintenance and updates (cause).”

With banks, it makes the most sense to break things out as follows: cause, risk/event, impact, and control (organized with taxonomies). With each risk description, there is a separate listing of the causes, impacts, and controls, and then they are integrated with the risks during the risk assessment step. Taxonomies allow the description of risks in an increasing level of detail.

Basel Taxonomy

The BCBS has formulated an operational risk taxonomy for banks, as shown in Figure 37.2. Level 1 provides a broad description of seven events/risks. Level 2 goes into greater specificity than Level 1 and provides 20 specific categories of risk. Level 3 goes even deeper and provides specific examples of the risks. BCBS only considers Levels 1 and 2 as regulatory categories; regulated banks must report operational risk using this Basel taxonomy. At Level 2, for analytical and logistical reasons, it is important to not have too many categories—and, instead, to defer the specific details to Level 3.

Figure 37.2: Level 1 Categories of Operational Risk Events

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

Source: Basel Committee on Banking Supervision, Annex 9, *Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework*, 2006.

As mentioned, each of the seven Level 1 categories identified in Figure 37.2 is further broken down into a Level 2 subcategory. The first two event types in Figure 37.2 have a higher frequency and severity of losses. Thus, it should not be surprising that there are more Level 2 subcategories for these two event types. The Level 2 categories help to further classify the type of loss event. Figure 37.3 identifies the six Level 2 categories for the event type identified as *execution, delivery, and process management (EDPM)*.

For financial firms, the EDPM category typically has the highest frequency of occurrence compared to the other categories. Business units in financial firms often deal with large numbers and executions of transactions. Due to the large volume of transactions on a daily basis, miscommunications and data entry errors are common. For example, in the futures market, FX transactions are typically very large to compensate for the low margins of this product line. Errors in finalizing a transaction even for a few days can result in large losses as counterparties will require compensation for the use of funds. Identifying where the errors occur as well as the number of occurrences is necessary for managing these operational risks.

Figure 37.3: Execution, Delivery, and Process Management (Level 1)

Level 2 Event Category	Examples
Transaction Capture, Execution, & Maintenance	Data entry, miscommunication, delivery failure, and accounting errors
Monitoring & Reporting	Mandatory reporting failure, inaccurate external report of loss incurred
Customer Intake & Documentation	Missing client permissions, incomplete documents
Customer/Client Account Management	Unapproved access, incorrect client records with loss incurred, negligent loss
Trade Counterparties	Non-client counterparty misperformance or disputes
Vendors & Suppliers	Outsourcing or vendor disputes

Source: Basel Committee on Banking Supervision, Annex 9, *Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework*, 2006.

The second category listed in Figure 37.2 is *clients, products, and business practices (CPBP)*. The most common type of loss events in this category arise from disagreements between clients and counterparties, as well as regulatory fines for negligent business practices and advisory fiduciary duties. Litigation cases are high in the United States, and the severity of losses is very high even though the frequency of loss events is typically less than the EDPM category. Figure 37.4 provides the Level 2 subcategories with examples for the CPBP category.

Figure 37.4: Clients, Products, and Business Practices (Level 1)

Level 2 Event Category	Examples
Suitability, Disclosure, & Fiduciary	Fiduciary violations, disclosure issues, privacy violation, account churning
Improper Business or Market Practices	Antitrust, improper trade or market practices, insider trading, market manipulation
Product Flaws	Product defects, model errors
Selection, Sponsorship, & Exposure	Client guidelines failure or excess client limits
Advisory Activities	Advisory performance disputes

Source: Basel Committee on Banking Supervision, Annex 9, *Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework*, 2006.

The *business disruption and system failures (BDSF)* category is far less common than the first two Basel categories. A system crash will result in substantial losses for a firm, but most of these losses would be categorized under the EDPM category. The following example illustrates a type of BDSF loss: Suppose a bank's funding system crashes early in the day and is not back online until after the money markets are already closed, after 4:00 pm ET. Due to this system crash, the bank needs to fund an extra \$30 billion for the day's activities. To do so, the bank must make special arrangements with counterparties at a much higher cost than the daily average funding cost. Basel II defines failed activity examples leading to loss events in the BDSF category as hardware, software, telecommunications, and utility outage.

The Basel Level 1 *internal fraud* category has only two subcategories: (1) unauthorized activity and (2) theft and fraud. Examples of activities that are classified under

unauthorized activity are intentionally not reporting transactions, unauthorized transaction type, and the intentional mismarking of positions. Examples of activities that are classified under the theft and fraud subcategory are fraud, theft, extortion, embezzlement, misappropriation of assets, forgery, tax evasion, and bribes.

The Basel Level 1 *external fraud* category also has only two subcategories: (1) theft and fraud and (2) systems security. Examples of activities that are classified under the theft and fraud subcategory are theft, forgery, and check kiting. Examples of activities that are classified under the systems security subcategory are hacking damage and theft of information with monetary losses.

The Basel Level 1 *employment practices and workplace safety (EPWS)* category has three subcategories: (1) employee relations, (2) safe environment, and (3) diversity and discrimination. Examples of activities that can lead to losses in the employee relations subcategory are compensation, benefit, termination, and organized labor. Examples of activities in the safe environment category are generally liabilities from accidents, employee health and safety rules, and workers' compensation. The last subcategory, diversity and discrimination, captures all activities related to discrimination issues.

The last Basel II Level 1 category for operational risk loss events is *damage to physical assets (DPA)*. The only subcategory is disasters and other events. This category and subcategory captures all loss events related to natural disasters and human losses from external sources, such as vandalism and terrorism.

Custom Taxonomies

The Basel taxonomy is general in nature—and, therefore, many banks will use a taxonomy that is more tailored to their specific operational risk exposures. In that regard, they will account for factors such as size, level of regulation, and geography.

The banking industry and its methods of conducting business have evolved dramatically from a technological point of view since the late 1990s. This has meant that cybersecurity issues have become a dominant issue for banks. In addition, the evolution to a more global operating environment for banks has meant that risks associated with outsourcing, project management, and supply chain management activities have become more prominent. With greater anti-money laundering controls in place, banks need to ensure compliance to avoid regulatory fines. All of these developments have required revisions to the Basel taxonomy.

Operational Riskdata eXchange (ORX) Taxonomy

The ORX reference taxonomy was released in 2019 and includes industry developments and new types of risks based on feedback from banking and insurance practitioners. It is shown in Figure 37.5.

Figure 37.5: ORX Taxonomy

Level 1 Risks	Level 2 Risks
People	Breach of employment legislation or regulatory requirements Ineffective employment relations Inadequate workplace safety
External fraud	Third party/vendor fraud Agent/broker/intermediary fraud First party fraud
Internal fraud	Internal fraud committed against the organization Internal fraud committed against customers/clients, or third/fourth parties
Physical security and safety	Damage to organization's physical asset Injury to employee or affiliates outside the workplace Damage or injury to public asset
Business continuity	Inadequate business continuity planning/event management
Transaction processing and execution	Processing/execution failure relating to clients and products Processing/execution failure relating to securities and collateral Processing/execution failure relating to third party Processing/execution failure relating to internal operations Change execution failure
Technology	Hardware failure Software failure Network failure
Conduct	Insider trading Anti-trust/anti-competition Improper market practices Pre-sales service failure Post-sales service failure Client mistreatment/failure to fulfill duties to customers Client account mismanagement Improper distribution/marketing Improper product/service design Whistleblowing Breach of code of conduct and employee misbehavior
Legal	Mishandling of legal processes Contractual rights/obligation failures Non-contractual rights/obligation failures
Financial crime	Money laundering and terrorism financing Sanctions violation Bribery and corruption Know your customer (KYC) and transaction monitoring control failure
Regulatory compliance	Ineffective relationship with regulators Inadequate response to regulatory change Improper licensing/certification/registration Breach of cross-border activities/extraterritorial

	Breach of cross-border activities/ external regulations Prudential risk
Third party	Third party management control failure Third party criminality/non-compliance with rules and regulations Inadequate intra-group agreements/service level agreements (SLAs)
Information security (including cybersecurity)	Data theft/malicious manipulation of data Data loss Cyber risk events Data privacy breach/confidentiality mismanagement Improper access to data
Statutory reporting and tax	External financial and regulatory reporting failure Tax payment/filing failure Trade/transaction reporting failure
Data management	Unavailability of data Poor data quality Inadequate data architecture/IT infrastructure Inadequate data storage/retention and destruction management
Model	Model/methodology design error Model implementation error Model application error

Source: ORX, Oliver Wyman: The ORX Reference Taxonomy for operational and non-financial risk, SUMMARY REPORT, 2019.

Although generally similar to the Basel taxonomy, there was an increase from 7 to 14 Level 1 risk types. Some Basel Level 2 risks moved to ORX Level 1 (e.g., third-party failure risk, statutory reporting and tax risk, business continuity risk, data management risk, information security risk [including cyber risk], and model risk). The ORX taxonomy is not yet used for reporting purposes.

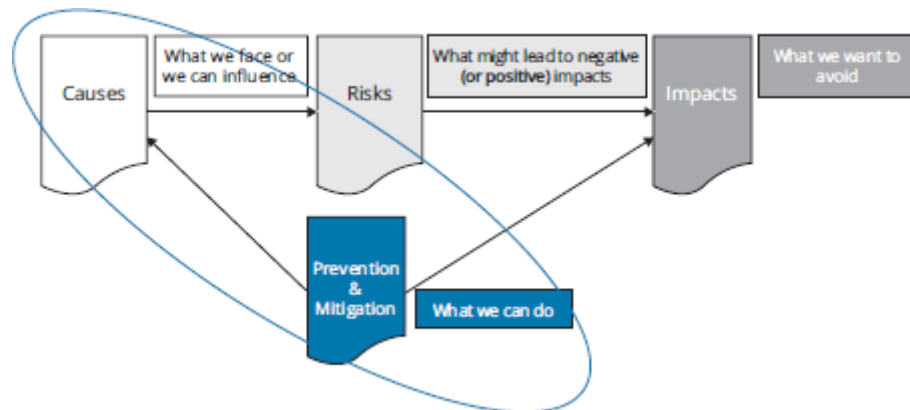
In preparing the ORX taxonomy, it was noted that there was great diversity in how banks defined and classified risks. For example, a given item might be considered a control failure by one bank, but a cause by another, and this difference would stem from the subjectivity inherent in applying judgment. In addition, key risks at banks now include cyber risk, conduct risk, and third-party risk. However, the classification of such risks may vary widely—for example, cyber risk might be classified as external fraud or an IT risk, and third-party risk might be stand-alone or an IT risk. Furthermore, some banks were using taxonomies that focused their risk on internal control failures, which may be representative for a large multinational bank. Firms focused on payment processing would use a taxonomy that focused their risk on information security and technology matters. Given this diversity and lack of consistency, it made sense to develop an “international standard” in the form of the ORX risk taxonomy.

Taxonomies for Causes, Impacts, and Controls

Defining and categorizing the risks, causes, impacts, and controls assist in taking clear steps to mitigate risks. Figure 37.6 illustrates the overall relationship, with the

encircled portion representing the actions steps to be taken based on the causes of the risks and controls that are available.

Figure 37.6: Actionable Operational Risk Management



In analyzing Figure 37.6 and focusing first on impacts, it is specifically the negative impacts that the bank wants to avoid. To avoid negative impacts requires banks to deal directly with the causes and then use controls on the causes with which they do not deal directly. By working with causes and controls, banks can hopefully reduce the probability of losses arising from the risk—and if that is not possible, then at least reducing the potential losses arising from the risk.

Causes

Going back to the Basel definition of operational risk provides the basic taxonomy for causes—employees, process failure, external, and systems. From there, more detail could be added to the next level to consider the specific causes of given incidents. In that regard, ORX has released a taxonomy of causes, with Level 1 consisting of the four items mentioned. Underneath each of the four causes at Level 1 are examples of more specific causes of failures at Level 2:

- **Employees**
 - Human error; unintentional harm
 - Incompetence and/or poor training
 - Poor communication
 - Intentional harm
- **Process failure**
 - Failures in system design, process design, or governance
- **External**
 - Political, regulatory, economic, and physical aspects of the business environment
 - Intentional harm
- **Systems**
 - Malfunctions; lack of capacity
 - Insufficient maintenance and/or testing
 - Service disruption

- Insufficient data storage; data loss

Impacts

ORX has also released a taxonomy of impacts. Impacts are classified at Level 1 as direct financial (losses or remediation), indirect financial, and nonfinancial. Examples of impacts at Level 2 are provided underneath each of the impacts at Level 1:

- Direct financial impact
 - Revenue reductions
 - Lost or damaged assets
 - Legal costs; fines/penalties
 - Regulatory fines/penalties
 - Provisions
 - Compensation to customers and third parties
 - Gains and recoveries
- Indirect financial impact
 - Regulatory compliance
 - Reputational harm
 - Customer detriment
- Nonfinancial impact
 - Customers, employees, third parties (e.g., suppliers, service providers), shareholders, competitors

Controls

Preventive controls are proactive in nature and used to minimize the chance of risks occurring by directly addressing the likely causes. An example in a data entry context would be an edit check (e.g., must be five digits in length) to reduce data entry errors.

Detective controls come into play during or after the event in hopes of minimizing any negative impacts. An example would be a periodic reconciliation of transactions for accuracy (e.g., two independent amounts should “balance”).

Corrective controls try to minimize or fix errors going forward so that they are not repeated in the future. Examples would include training sessions and sharing of “best practices.”

Directive controls consist of guidance, processes, and training that are provided while performing duties to minimize the risk of error. An example would include detailed and step-by-step instructions on how to perform a specific process.



MODULE QUIZ 37.2

1. Regarding the Basel taxonomy of operational risks for banks and the Level 1 category of internal fraud, which of the following items would most appropriately be included at Level 3?
 - A. Insider trading.
 - B. Theft and fraud.
 - C. Unauthorized activity.

- D. Losses due to acts of a type intended to defraud.
- 2. An investor records its investments on its internal systems and reconciles them with the investment listing on the brokerage statement each month. This reconciliation is best described as:
 - A. a corrective control.
 - B. a detective control.
 - C. a directive control.
 - D. a preventative control.

KEY CONCEPTS

LO 37.a

For risk identification, there are two approaches to consider: (1) top down and (2) bottom up. For the top-down approach, it can be subdivided into three general levels—it begins with the board and senior management, then moves down to the separate divisions or business units, and then to the separate business processes. For the bottom-up approach, the business units assess their own risk. By combining both risk identification approaches, we can obtain a more thorough and in-depth understanding of the bank's operational risk.

Common top-down approaches include: (1) analyzing exposures and vulnerabilities, (2) risk wheel, and (3) analyzing emerging risks. Common bottom-up approaches include: (1) event and loss data analysis, (2) risk and control self-assessment, and (3) process mapping.

LO 37.b

Scenario/stress test identification is the bridging step between risk identification and scenario analysis. The scenarios considered are meant to be extreme and financially severe; they could occur, but are far less likely.

Scenario analysis is fraught with pitfalls including a lack of consistency with methodology as well as the existence of behavioral biases. At the same time, regulators are mandating that scenario analysis results remain consistent after numerous iterations, and that requires neutrality during the scenario identification and assessment process. Achieving such neutrality requires the use of empirical evidence, explanations for how or why a specific scenario was developed, and detailed write-ups to support the assumptions and methodology used in developing the scenarios.

Scenario workshops consist of two primary steps: (1) the generation phase (which creates many scenarios that will be screened and narrowed down to selected ones to be further pursued) and (2) scenario selection (a few scenarios may be combined, while others are dropped or added so as to come up with a final list that will be assessed).

LO 37.c

For banks, each risk description has a separate listing of the causes, impacts, and controls; they are integrated with the risks during the risk assessment step. Operational risk taxonomies allow the description of risks in an increasing level of detail. Defining and categorizing the risks, causes, impacts, and controls assist in taking clear steps to mitigate the risks.

LO 37.d

The Basel operational risk taxonomy consists of three levels. Level 1 provides a broad description of seven events/risks. Level 2 goes into greater specificity than Level 1 and provides 20 specific categories of risk. Level 3 goes even deeper and provides specific examples of the risks.

Loss events in the execution, delivery, and process management (EDPM) category have a small dollar amount but a very large frequency of occurrence. Losses are more infrequent but are very large in the clients, products, and business practices (CPBP) category.

The Basel taxonomy is general in nature—and, therefore, many banks will use a taxonomy that is more tailored to their specific operational risk exposures. In that regard, these banks will account for factors such as size, level of regulation, and geography.

The ORX taxonomy was released in 2019. Although generally similar to the Basel taxonomy, there was an increase from 7 to 14 Level 1 risk types. Some Basel Level 2 risks moved to ORX Level 1 (e.g., third-party failure risk, statutory reporting and tax risk, business continuity risk, data management risk, information security risk [including cyber risk], and model risk).

ANSWER KEY FOR MODULE QUIZZES

Module Quiz 37.1

1. **C** Vulnerabilities are the weakest links in business activities. Therefore, a stand-alone IT system is an example of a vulnerability in that it may lack updating or monitoring that could result in an external cyberattack.

The other three items are exposures. For example, failure of critical third parties (e.g., service providers) to perform specific tasks for the bank may result in large losses for the bank. Or, noncompliance with one or more regulations could result in significant fines and penalties assessed by the principal regulator. (LO 37.a)

2. **A** Assessing risk at a more local and detailed level is characteristic of a bottom-up approach to risk identification. In that regard, process mapping, analysis of near misses, and risk and control self-assessments are key tools used in the bottom-up approach.

A risk wheel is a top-down risk identification tool that uses brainstorming to generate ideas during a risk identification workshop. Therefore, it is least likely to be recommended by the CRO in this case. (LO 37.a)

3. **A** To meet regulators' requirements to reduce subjectivity and biases, assumptions used in scenario analysis must be based on empirical (real-life) data and evidence.

The facilitators are usually ORM professionals and far less likely to be internal to the bank. The participants should be senior managers within the different business units. It is more common to distribute such preparation documents before the initial meetings, although less frequently, such documents will be withheld and distributed later to minimize any bias. (LO 37.b)

Module Quiz 37.2

1. **A** The Level 1 category is internal fraud, and it is defined as “losses due to acts of a type intended to defraud . . .” Furthermore, Level 2 subdivides internal fraud into two further categories: unauthorized activity and theft and fraud.
Level 3 provides specific examples of risk and, in that regard, insider trading is a specific example of internal fraud. (LO 37.d)
2. **B** A reconciliation is meant to detect an error as soon as possible so that it can be subsequently corrected, if needed. In that regard, the reconciliation is best described as a detective control. The reconciliation is not a corrective control as the reconciliation itself does not correct the error. (LO 37.c)

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 4.

READING 38

RISK MEASUREMENT AND ASSESSMENT

Study Session 7

EXAM FOCUS

After the identification stage, operational risk must be assessed, measured, and modeled. For the exam, be familiar with the characteristics of operational loss incidents data. In terms of qualitative risk assessment, the focus should be on obtaining a detailed understanding of risk and control self-assessments (RCSAs) and key risk indicators (KRIs). In terms of quantitative risk assessment, emphasis should be placed on fault tree analysis and root-cause analysis. Although a detailed understanding of quantitative methods is not required, a good understanding of the loss distribution approach (LDA) for operational risk is important, specifically frequency and severity modeling. Finally, understand the key steps for operational resilience.

MODULE 38.1: OPERATIONAL LOSS DATA AND QUALITATIVE RISK ASSESSMENT

LO 38.a: Explain best practices for the collection of operational loss data and reporting of operational loss incidents, including regulatory expectations.

Risk management and measurement makes use of historical losses and events. The operational risk management (ORM) framework can be thought of in four concentric circles: (1) incident/loss database, (2) assessment through RCSAs, (3) monitoring through KRIs, and (4) takeaways from major loss events or high-risk exposures.

To maintain being competitive and profitable, banks must be aware of the source of all losses as well as internal control failures and weaknesses. Information on internal incidents is useful for scenario identification and assessment purposes and to quantify regulatory capital reserves. Information on incidents occurring at other banks is useful to a bank for general awareness and to take any necessary precautions or use risk mitigation techniques. The availability of thorough and reliable data on incidents is useful for minimizing the amount of Pillar 2 extra capital requirements.

Regulatory Requirements for Operational Loss Data

The Basel Committee on Banking Supervision (BCBS) has numerous criteria dealing with data quality and collection. The key ones are as follows:

- At least 10 years of data
- Minimum collection threshold of EUR20,000
- Internal losses to be classified to the Basel event-type categories
- Report dates of occurrence and recovery

Other criteria deal with governance issues and the exclusion of losses due to credit and market risk.

Data Collection Process

The overall guidance is that the bank “must have documented procedures and processes for the identification, collection, and treatment of internal loss data.”

In that regard, clarity regarding what is reported is the first step in ensuring sufficient data quality. Items to consider include dates, incident types, thresholds, and loss quantification. Overall, operational incidents are often challenging to clearly describe, and there is subjectivity with quantification. A general example of an IT service disruption problem eventually leading to reputational damage to the bank may involve multiple business units, and attempting to quantify the “intangible” reputational loss would likely produce a wide range of results, depending on which assumptions are used.

When reporting operational incidents, there is a group of data fields used by all banks that are consistent with the taxonomy of risks, causes, impacts, and controls. It is important to maintain a standardized approach to gathering information and reporting. Therefore, the use of free text (i.e., unstructured data) must be carefully controlled so that it only provides supplementary detail instead of being the primary source of loss information.

Examples of data fields used in reporting include the following:

- Place of occurrence
- Date of occurrence
- Event type
- Cause type
- Control failures
- Impact type (loss, gain, near miss)
- Gross loss
- Recovery
- Net loss

Comprehensive Data

Internal loss data must “capture all material activities and exposures from all appropriate subsystems and geographic locations.”

Although the BCBS does not clarify “material activities and exposures,” the loss reporting minimum threshold is EUR20,000. Many banks use a lower threshold (e.g., EUR/USD/GBP 1,000–10,000), although it is no longer common to have a threshold as low as zero due to cost-benefit reasons involved in reporting many small losses. The threshold amount should be supportable and, for example, should not be set deliberately to attempt to reduce capital requirements.

Regulatory requirements focus on recognizing financial losses that directly stem from operational incidents. Examples include compensatory payments, regulatory penalties, and fund losses due to errors. However, regulations do not technically consider losses that are less direct, such as lost customers due to reputation decline, service disruption, reduced productivity due to declining employee morale, and incremental management time. On the other hand, it is good management practice to include the less direct costs because that will reflect the full and true cost of operational risk and allow for better decisions to be made.

Regulations require grouped losses with a common cause to be recognized. Oftentimes, there is a single failure that gives rise to multiple events and losses. For example, an IT failure could result in losses due to incomplete transactions in the trading department and compensatory payments required for online service interruptions to external customers. All of those costs would be combined and reported as a grouped loss.

Incident Dates

Loss events must be reported in terms of gross loss amounts net of any recoveries plus the reference dates. A summary of the sources and causes of the events should be provided as well.

The four relevant dates per event include (1) occurrence (i.e., when it first happened), (2) discovery, (3) reporting, and (4) accounting. In some cases, such as minor employee defalcation and data leaks, the time between occurrence and discovery could be up to several years. The long period of discovery explains why the settlement date of the event is often years after occurrence; in general, the longer the time, the greater the impact.

For internal reporting, regulations are not specific on which date(s) to include. However, it is useful to note the interval between the pairs of dates. For example, the time elapsed between occurrence and discovery demonstrates the level of visibility of the issues. The time between discovery and reporting is a measure of reporting timeliness. In that regard, significant events must be reported within days of occurrence, whereas less significant events can be summarized and reported periodically (e.g., quarterly).

The settlement date essentially occurs with the accounting and entry into the bank’s general ledger. That could take a long time in the case of incidents that have regulatory and legal implications requiring multiple years (e.g., three to five years) between reporting and settlement dates. Given the significant time lag, banks must use caution when analyzing losses “paid out” recently but occurring many years ago in a different business environment. Such losses may not be appropriate to consider when making future projections.

Boundary Events

Boundary events refer to those events that occur in a risk class that is not the same as the cause. They could include market and/or credit losses caused by human error (operational in nature).

Events must be classified appropriately, and the BCBS offers the two following points:

1. Boundary events are considered as a credit risk and not attributed back to their actual cause. In that regard, operational losses in a credit risk context are often included in risk-weighted assets (RWAs)—and, therefore, they do not need to be included in operational losses to the extent they are already included in RWAs.
2. Boundary events are not considered as a market risk. Therefore, operational losses in a market risk context are included in operational losses.

Data Quality Requirements

The BCBS does require banks to “have processes to independently review the comprehensiveness and accuracy of loss data.” To ensure completeness of all significant losses, corroboration of information from multiple sources is required, which includes the general ledger (GL). However, the GL on its own has two notable limitations: (1) by its nature, it can only capture direct items that are easier to quantify but often omits indirect items that are more intangible and/or harder to quantify, and (2) items that might otherwise be unrecorded but would show up indirectly in the form of lower revenues should actually be recorded as expenses or losses on the income statement.

IT logs allow the matching of IT issues to the actual operational incidents recorded. IT issues designated as Priority 1 (P1) or Priority 2 (P2) would be equivalent to operational risk incidents. Other sources of data to mitigate against underreporting operational risk incidents include customer complaints, unfavorable press and media reports, and reserves for upcoming lawsuits.

Underreporting incidents remains a problem, especially for smaller banks. The causes include uncertainty as to what should be reported, unwillingness to pursue control failures, and avoidance of bureaucratic reporting processes. Methods to mitigate underreporting include: gentle reminders, use of risk metrics in assessing managerial performance, and involvement of the internal audit department to ensure that the operational loss data collection methods are reliable.

Operational Risk Data

Operational risk data is vastly different than market and credit risk data. It is idiosyncratic and largely uncorrelated to general markets, which presents problems in measuring and modeling. The presence of wide (fat) tails in their returns and frequency distributions indicates the greater occurrence of extreme events. In addition, the interrelated nature of operational risk creates interpretive difficulties in linking causes and effects.

Risk and Control Self-Assessments

LO 38.b: Explain operational risk-assessment processes and tools, including risk control self-assessments (RCSAs), likelihood assessment scales, and heatmaps.

Risk and control self-assessments (RCSAs) involve assessing the probability and severity of operational risk. The process can be subdivided into examining inherent risk only (no consideration of current controls in place) and examining residual risk (remaining risk after considering the effectiveness of current controls). RCSAs are performed on an annual basis, although a quarterly basis is possible if some operational risks are very significant.

A separate risk assessment unit (RAU) may be used to coordinate RCSA activities. RCSAs usually involve participants discussing inherent risks, controls to manage those risks, and assessing the overall effectiveness of those controls. At larger banks, some of the assessment data comes from questionnaires. The two main types of controls are *preventive* (e.g., reduce the chance of risk materializing) and *corrective* (e.g., if a risk materializes, minimize any negative effects).

The objective of an RCSA is for the bank to be aware of and comprehend its inherent risks, its internal controls in place, and its residual risks. RCSAs, by nature, are primarily nonquantitative and require significant judgment. Therefore, they are not meant to quantify risk exposures. Instead, RCSAs are meant to provide greater awareness of risks and controls within a bank—and, ultimately, to determine whether additional steps need to be taken to mitigate risks. Similar to a financial statement audit performed by external auditors, an RCSA may involve tests of controls to determine whether controls are operating effectively—and, therefore, inherent risks are considered to be reduced to a level within the bank's risk appetite.

Some banks perform backtesting of the RCSA versus historical incidents. Backtesting results often reveal underestimates of the probability of occurrence of an incident, but overestimates of the severity. In that regard, RCSAs should account for cost-benefit considerations. However, RCSAs are often a regulatory requirement.

Alternatives to RCSAs include **risk and control assessment (RCA)** and **residual risk self-assessment (RRSA)**. With RCAs, tests of controls are documented, occurrences are analyzed to demonstrate where controls were effective in avoiding incidents or minimizing the severity, and actual losses are compared to those of similar activities either internally or at other banks. With RRSAs, there is emphasis on determining the level of risk remaining once the controls in place are accounted for; there is no direct analysis of inherent risk.

RCSAs have some disadvantages, including subjectivity, the introduction of behavioral biases, and limited data—which, as a collective whole, may impair the usefulness of the results. In addition, comparing results between differing assessment units and departments can be problematic because the performance of RCSAs may lack significant consistency between business units. As a result, a basic level of consistency would require standardized risk descriptions and exact definitions of probability and severity. This way, it is possible to rank the risks and create a priority list of which risk management activities are employed first.

RCSA output is documented and sent to unit managers for approval and signoff. Unit managers must perform all mitigation actions agreed upon arising from the RCSA. The output will provide a summary of the significant residual risks after all the stated controls are applied. Based on the assessment of inherent risk, the RCSA may also provide some clues as to what may happen in the event of failure of the main controls. RCSAs help to identify whether the risk level of a particular business unit is within the overall risk appetite. If not, then additional risk mitigation is necessary. It could be in the form of introducing new controls or enhancing existing controls. Alternatively, exposure reduction could be implemented by reducing transaction volumes or purchasing insurance from a third party.

Impact Scales

Impact, here, refers to financial, regulatory, customer, and reputation—although in the context of resiliency, it could include continuity of service. Impact scales typically consist of four or five ratings (e.g., low, medium, high, very high, extreme).

Financial impacts are usually based on a relative measure, such as percentage of revenue or operating income. This is useful to allow flexibility to accommodate different sizes. Similarly, customer impacts are usually based on a percentage of customer base. Regulatory and reputation impacts are typically nonquantitative in nature, although some metrics may be used.

Likelihood Assessment Scales

Amounts are stated either as a probability or frequency of occurrence. Because RCSAs have a maximum time horizon of 1 year, a 1-in-25-year event means that there is a 4% chance of the event occurring within the year. That is not the same as saying it will occur once over a 25-year period, especially when dealing with emerging and quickly changing risks involving technological advancements, cyberattacks, and regulatory penalties. History is the starting point for determining probability of occurrence, although it is well known that the past can be a poor indicator of the future. The problem with using past information to predict the future is exacerbated when the business environment is volatile.

Rating categories for a likelihood scale might be described on this five-point scale: remote, unlikely, possible, likely, highly likely.

Heatmaps

The combination of likelihood and impact is the RCSA matrix, or **heatmap**. The combinations are assigned colors (e.g., green, yellow, amber, red) that correspond to risk intensity.

Green indicates a level of risk exposure that is permissible, with no further steps required. Green could occur, for example, when the likelihood is possible, but the impact is low—or when the likelihood is remote, but the impact is high.

Yellow indicates a level of risk exposure that is permissible, but is getting near the limit. Therefore, some monitoring and risk mitigation steps could be needed. Yellow could occur, for example, if the event is likely to happen, but the impact is low—or if the event is unlikely to happen, but if it does, the impact is high.

Amber indicates a level of risk exposure that exceeds the permissible limit, and the risk must be lowered in terms of likelihood or impact; otherwise, it must be escalated for approval. Amber could occur, for example, if the event is likely to happen and the impact is medium—or if the event likelihood is remote, but the impact is extreme.

Red indicates a level of risk exposure that far exceeds the permissible limit, and risk must immediately be lowered in terms of likelihood and/or impact. Red could occur, for example, if the event is likely to happen and the impact is high—or if the event is unlikely to happen, but the impact is extreme.

Note that the ratings are qualitative in nature. Therefore, it is erroneous to compare them mathematically. For example, a risk that has a remote chance of occurring but with a major impact (ratings of 1 and 3; $1 \times 3 = 3$) is not equivalent to a risk that has a possible chance of occurring but with a low impact (ratings of 3 and 1; $3 \times 1 = 3$).



MODULE QUIZ 38.1

1. A bank employee has been manipulating suspense (transitory) accounts for a prolonged time, and this event was determined to be a significant operational incident. Which of the following time intervals in terms of the operational incident date is most likely to be the longest?
 - A. Date of reporting to date of accounting.
 - B. Date of discovery to date of reporting.
 - C. Date of occurrence to date of discovery.
 - D. Date of occurrence to date of reporting.
2. Which of the following statements regarding risk assessment is most accurate?
 - A. Risk and control self-assessments (RCSAs) are a good mixture of qualitative and quantitative aspects.
 - B. The main purpose of risk assessment is to prioritize risk management and risk mitigation responses.
 - C. When backtesting the results of risk assessment against past incident experience, there is a tendency to overestimate the likelihood of an operational risk event.
 - D. When backtesting the results of risk assessment against past incident experience, there is a tendency to underestimate the impact of an operational risk event.

MODULE 38.2: KEY INDICATORS AND QUANTITATIVE RISK ASSESSMENT

LO 38.c: Describe the differences among key risk indicators (KRIs), key performance indicators (KPIs), and key control indicators (KCIs).

Key Risk Indicators (KRIs)

KRIs will indicate the bank's exposure level at a specific point in time. Preventive KRIs indicate a rise or fall in the intensity of a cause of a risk. Therefore, KRIs will indicate a rise or fall of the impact or likelihood of the risk.

Examples of KRIs used in measuring likelihood would be an increase in the number of transactions processed per employee (risk of error) or an increase in sales level needed to earn a bonus (risk of fraud).

Examples of KRIs used in measuring impact would be an increase in the sensitivity of data maintained on a server (greater impact if data leakage were to occur) or an increase in transaction limits for traders (greater impact if unauthorized trading were to occur).

Key Performance Indicators (KPIs)

KPIs provide measurements on how effectively the bank operates. In that regard, a bank may have KPIs such as the number of customer complaints, error rates on customer transactions, and average downtime of IT systems.

Key Control Indicators (KCIIs)

KCIIs provide measurements on how effectively the bank's controls are operating. In that regard, a bank may have KCIIs such as the number of business continuity plans not reviewed or updated before the set due dates, errors remaining after two sets of independent and qualified reviews, and the number of general ledger data entry errors after application of edit checks.

Overall, KRIs, KPIs, and KCIIs overlap significantly—and a given metric can have one or more of the risk, performance, and control elements, and that is especially the case when analyzing a deficiency from a required benchmark level. For example, key control failures would be an automatic source of risk and could have elements of KRIs, KPIs, and KCIIs. Using the scenario of a control failure with incorrect transaction processing despite multiple checks, including edit checks, the KCI would relate to the inaccurate transaction processing, the KRI would relate to increased risk of litigation by customers resulting from the errors, and the KPI would relate to weak back-office abilities.

KRIs account for the bank's risk appetite. The metrics chosen for risk oversight purposes are an indication of the bank's priorities in terms of its goals and the risks that are most important to manage. The thresholds reflect the level of control desired by management in terms of risk mitigation.

LO 38.d: Describe and distinguish between the different quantitative approaches and models used to analyze operational risk.

LO 38.e: Estimate operational risk exposures based on the fault tree model given probability assumptions.

Quantitative analysis involves a detailed analysis of the causes that impact the probability of operational risk events happening. The risk assessment methods used here are factor models, which are concerned with control layers and their failure rates. By analyzing scenarios and risk estimates in terms of probability and severity, the output of the analysis becomes more reliable together with greater transparency in the methodologies employed.

Causal analysis is purely future oriented in terms of computing likelihood and impacts and does not rely on historical losses. Quantifying scenarios, especially impacts, is

difficult given that a very large sample size of empirical data is required to ensure reliable outputs.

Fault Tree Analysis (FTA)

FTA is a form of deductive failure analysis whereby fault trees break out failure scenarios into external and internal conditions required for a major event to occur. FTA is seeing more use at banks now, where a chain of failures leads to a major loss; a set of conditions could happen at the same time (“AND conditions”) or happen alternately (“OR conditions”).

Assuming that all events happen independently of each other, the joint probability of occurrence is simply the multiplicative of each of the separate probabilities. For example, assume four independent controls each have a 5% chance of failing. The probability of them failing all at the same time is $0.05^4 = 0.00000625 = 0.000625\%$. This generic example could be applied to something more specific, such as an inadvertent leakage of sensitive information at a bank involving failures in multiple steps. The percentage 0.000625% is the minimum probability of the scenario occurring. In real life, it is unlikely that the failures are completely independent of each other because the controls were probably designed together, for example. As a result, conditional (or Bayesian) probabilities would need to be applied to get a more realistic sense of the probability of occurrence. In this case, probabilities are updated with new information or new events; a simple example would be that the probability of an error in transaction processing is increased, given that there was IT service interruption.

If we apply the calculation to an information leakage scenario and there are 50,000 employees at the bank, then the likelihood of the scenario occurring becomes at least 31% ($0.000625\% \times 50,000 = 31.25\%$) on the assumption of a consistent failure rate for all employees. Therefore, it is crucial not only to simply look at the low failure rate, but also to consider the exposure—which, in the case just listed, would be the number of employees.

Causal analysis requires the estimation of risk factor probabilities from third-party and empirical information. Probabilities for weather-related and other known events might be obtained from insurance and reinsurance companies. Other scenarios rely on past experiences of peers, so if 1 out of 50 banks suffers losses arising in a specific scenario over the past three years, then the baseline probability for the risk over a one-year horizon would become 1 out of 50; that baseline probability could be subsequently adjusted to take into account the specific circumstances of the given bank. Finally, some absolute worst-case scenarios of the risks examined during the RCSA sessions might deserve some consideration to provide more complete coverage.

Factor Analysis of Information Risk (FAIR)

For factor models, risks are broken out into individual factors. In that respect, the FAIR model considers the following three steps:

1. Determine risk factors and how they interrelate.
2. Measure each factor.
3. Computationally combine all factors.

The output is a loss distribution for a given scenario. Scenarios have the following attributes: (1) asset at risk, (2) threat, (3) threat type, (4) losses occurring, if risk occurs. With the created scenarios, estimates must be made for the frequency of losses and the likely loss amounts. Everything is stated as a distribution instead of single points, and those distributions become inputs for Monte Carlo simulations. The output from Monte Carlo simulations is the distribution of the simulated losses.

Swiss Cheese Model

This model states that “[i]n an ideal world each defensive layer would be intact. In reality, however, they are more like slices of Swiss cheese, having many holes—though unlike in the cheese, these holes are continually opening, shutting, and shifting their location. The presence of holes in any one “slice” does not normally cause a bad outcome. Usually, this can happen only when the holes in many layers momentarily line up to permit a trajectory of accident opportunity—bring hazards into damaging contact with victims.”¹

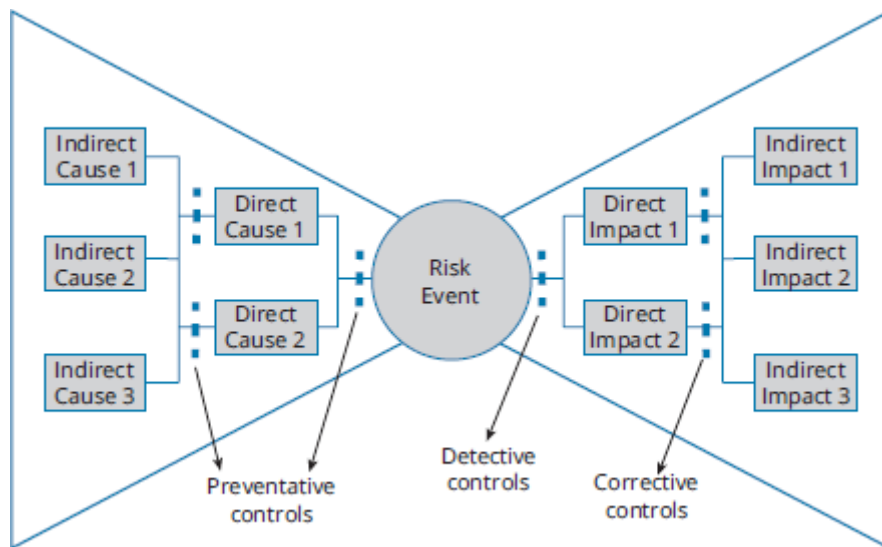
To deal with such a risk, proper control layering is required so that the holes can never be aligned to create the “perfect storm.” To do so, the control failure rates cannot be correlated, and there should be compensating controls that effectively nullify any weaknesses. Periodic reviews would be required to ensure that controls remain independent of each other and to ensure that each independent control is reliable.

Root-Cause Analysis

In an operational risk context, root-cause analysis is done by the first line of defense for significant incidents and near misses. The second line would then add to and/or query the analysis. If applicable, it would be useful to compare the current analysis to any past analyses in search of any common themes in terms of causes and failures. This may assist in risk mitigation efforts going forward.

The **5-whys analysis** is an in-depth investigation that requires asking, a minimum of five times, “Why did this happen?” It attempts to determine the numerous causes of the failures. An application of this approach can be seen in a **bow tie diagram**, like the one in Figure 38.1.

Figure 38.1: Bow Tie Diagram



The risk event to be analyzed is placed directly in the center of the diagram, with causes and preventive controls dealt with on the left side, while impacts and detective and corrective controls are dealt with on the right side.

Bow tie analysis can also be used to assess the expected frequency and severity (within a range) of incidents in view of all the current controls and other mitigation techniques. It also goes deeper than just the direct causes, and it looks at indirect and root causes of incidents as well as determining any additional relevant KRIs to monitor.

Root cause analysis allows for a much stronger comprehension of causes of incidents, together with the control failures that led to them. That, in turn, may allow for a more accurate estimation of the frequency of occurrence of specific events. Overall, root-cause analysis is thorough in nature and methodical in assessing the severity of the risk, taking into account any mitigation. The bow tie approach can be used to determine the timeliness in terms of event detection, together with the bank's effectiveness in minimizing the impacts.



MODULE QUIZ 38.2

1. One of the bank's compliance managers notices that there are two business continuity plans that have not been reviewed, and it is now past their review due date. The incomplete reviews of the business continuity plans are best described as:
 - A. a key assessment indicator.
 - B. a key control indicator.
 - C. a key performance indicator.
 - D. a key risk indicator.
2. In the context of a potential nonmalicious data leakage incident by a bank employee, the following information is provided:
 - There is a 99% chance that bank employees will receive a phishing email through their work email.
 - There is a 95% chance that the bank's firewalls will operate as intended.
 - There is a 90% chance that the employee will know to immediately delete the phishing email.
 - There is a 3% chance that the detective controls of suspicious network activity will fail.
 - There is a 1% chance that there will be an exit of the leaked information.

Using fault tree analysis (FTA) and assuming that the conditions just listed are fully independent, the likelihood of the risk of data leakage materializing for a given time period is closest to:

- A. 0.0001485%.
- B. 0.0004365%.
- C. 0.0048015%.
- D. 0.0253935%.

MODULE 38.3: OPERATIONAL RISK CAPITAL AND RESILIENCE

LO 38.f: Describe approaches used to determine the level of operational risk capital for economic capital purposes, including their application and limitations.

Stochastic models are used with the idea of fitting a statistical distribution to the distribution of historical losses (in terms of loss frequency and severity). Those distributions would then be used to simulate the bank's loss distribution.

Loss Distribution Approach (LDA)

The LDA is the most common approach and is supplemented by extreme value theory or scenario analysis when analyzing tail risk. LDA breaks out loss events into frequency and severity, which increases the number of data items used for modeling by twofold. The frequency and severity distributions are independently modeled and then convoluted into an aggregated loss distribution. The Monte Carlo convolution approach creates the aggregated distribution using millions of random draws of frequency and severity. Alternative methods use equations instead, which are less computer intensive.

Frequency distributions are based on whole numbers (i.e., discrete) and express the number of times an operational incident occurs over a year. Modeling is usually done with a *Poisson distribution*; an alternative is a *negative binomial distribution*. Poisson distributions provide the probability of an event, k , occurring in a specified time period. They also have one parameter, l , which is called the intensity or hazard rate. The l is equal to both the mean and variance of the distribution. The observations are assumed to be independent and identically distributed.

Severity distributions are continuous, asymmetric, and have fat tails; there are many minor incidents, but there are only a handful of major incidents resulting in significant losses. Modeling is usually done with a *lognormal distribution*, although a few other distributions with fat tails are becoming more common. A key attribute of lognormal distributions is that the random variable can only assume positive real values.

The LDA usually assumes that both distributions are independent, which is questionable given that empirical evidence suggests a high frequency of low-severity events and a low frequency of high-severity events. In addition, the LDA assumes that there is no implied correlation between losses within a risk class (i.e., losses are independent and identically distributed), which is consistent with the heterogeneous

nature of operational risk incidents. Testing for independence and identical distribution requires the same or similar losses to be clustered and tested to ensure no autocorrelation.

The LDA is used on each loss cluster with a unit of measure (UoM) that is transformed into a total loss distribution. The 99.9th percentile of the distribution is the required stand-alone capital for operational risk, assuming only the use of the LDA. Given that operational risk events are so diverse, trying to cluster data in homogeneous UoMs is difficult. UoMs could include external fraud events, internal fraud events per business unit, and processing error events. Effective UoMs are operational risk events that have similar or the same drivers, so they result in a similar distribution. Although homogeneity within the UoM is desirable, the resulting segmentation comes with the cost of having less available data. Having less data means less reliable results and more difficulty in combining the data into a distribution.

Model dependencies will significantly impact the capital requirement computations. In that regard, UoMs should be consistent with the way the bank is organized and how the model is ultimately used. Aggregating UoMs is done through copulas, which are generalizations of correlations; copulas are used to analyze situations such as tail dependence and dependence between extreme values.

LDA models are not able to handle the very-high skewness of operational risk losses. To do so properly, one or more of the following steps need to be taken: (1) adding large losses to the existing data, (2) applying extreme value theory, or (3) using scenario analysis.

Extreme Value Theory (EVT)

The two EVT methods are as follows:

1. The block maxima (Fisher-Tippett) approach looks at the maximum operational loss per equally spaced time period and per UoM when considering the distribution of such losses.
2. The peaks-over-threshold (POT) approach looks at items past a specific high threshold that would be considered “sufficiently large.” The distribution of the amounts past the threshold could be estimated with the generalized Pareto distribution (GPD).

EVT is effective only when there is one main underlying cause that generates all losses and will generate future losses that are greater than current ones. However, given the diverse nature of operational losses, the idea of a main underlying cause is not realistic—and, therefore, severely compromises the usefulness of EVT in quantifying operational risk. Therefore, alternative methods such as scenario analysis, causal modeling, fixed multipliers, and macro determinants of operational risk could be considered.

Internal and External Loss Data

Internal loss data plays multiple roles—it is a source of detailed information on risks and control failures as well as the starting point for the LDA. Internal loss data can often give many data points to generate distributions, especially the area of “critical mass” consisting of high-frequency and moderate-severity events. Compared to

external data, internal data likely has more relevance to the bank, together with greater detail.

In context of causal models, databases containing information on internal incidents can give insights on risk exposure and causes of losses, which is useful for scenario analysis and assessment purposes. Usually, there are differences between the internal incident database and the data used for modeling computations. The differences arise because some exceptional incidents are not fully reported. For example, near misses and inadvertent gains might not be considered true losses; therefore, the amounts are omitted when computing frequency and/or severity.

Overall, internal loss data alone must be complemented with external loss data from other banks, for example. This will allow for a much greater understanding of the entire scope of loss outcomes that could affect a given bank. External loss data from public sources (full loss details available for all incidents), members-only databases (loss details available per incident on an anonymous basis only), and industry associations (e.g., Operational Riskdata eXchange Association) may be obtained although there is less data available from public sources, which may result in a less reliable model. To obtain relevant and comparable loss information, consideration must be given to factors such as geographic location(s), concentration of activities, and materiality thresholds for reporting incidents.

Internal and external loss data are combined to arrive at the computational data used for model calibration. The methods of combining the data include the following:

1. *Scaling*. These are size adjustments for losses to be consistent with the bank's size. Another example would be for inflation adjustments, when a large number of years are involved.
2. *Cut-off mix*. At a specific loss threshold when there are few(er) internal losses, then external losses would be included in the model to have sufficient data points to generate a reliable distribution.
3. *Filtering*: This is setting specific rules for the inclusion or exclusion of losses in the dataset to be used for modeling to avoid the potential manipulation of results.

Capital Modeling

The new standardized approach for calculating operational risk capital technically eliminates any requirements for banks to model their operational risk. As a result, their modeling activities are now focused on Pillar 2, the internal capital adequacy assessment process (ICAAP), stress testing, and operational resilience.

Before the implementation of the standardized approach, banks had to determine the amount of capital needed to account for all potential operational losses for a 99.9% confidence level for a one-year time horizon. In general, the idea was to set an amount of regulatory capital that was congruent with the bank's risk profile, which remains the same with the new standardized approach.

The ICAAP covers operational risk and other risks and is included in Pillar 2, which requires coverage of both financial and nonfinancial risks. The ICAAP consists of self-assessment of capital sufficiency in the context of the nature of the business, potential changes in risk exposure due to business changes in the medium term, and current

controls. An operational risk ICAAP report involves choosing and quantifying appropriate scenarios based on current business risks, past experiences (internal and external), and controls within the bank. To be more specific, scenario identification, mitigation, and assessment is covered in Pillar 2a—and capital assessment, planning, and stress testing is covered in Pillar 2b.

Scenario aggregation is used to compute the required capital. Smaller banks use a simpler process of provisioning capital that is greater than the loss estimate of the largest scenario and greater than the loss estimate of two to four scenarios that might occur as a cluster. If a bank has already set aside capital greater than those amounts, then that will suffice. Larger banks use more complex methods, such as variance-covariance matrices or copulas.

Ultimately, a report is forwarded to the regulator with full justification behind choosing and quantifying each of the scenarios or the capital components. In addition, there should be explanations to support why certain scenarios were eliminated. Scenario quantification could consider different amounts for the various potential states (e.g., low, medium, high, extreme) for items such as revenue, costs, and regulatory penalties together with probability estimates of each of the states. Estimated losses could be expressed in amounts in terms of quantiles.

The ICAAP essentially allows a bank to compute its economic capital, which is equal to the internal capital needed to ensure it can meet its potential losses and remain a going concern (and to maintain its external credit rating).

Operational Resilience

LO 38.g: Describe and explain the steps to ensure a strong level of operational resilience, and to test the operational resilience of important business services.

When performing scenario analysis, the results may suggest that a bank may suffer immensely in terms of future profits and reputation due to an operational event. Operational resilience mandates that banks consider such possible events (which may have yet to occur) and determine whether they have sufficient resilience to recover from such events. In fact, operational resilience should be the result of a strong ORM framework. By identifying and assessing risk, mitigating risks where needed, and monitoring risks, the goal is to reduce the impacts of any operational disruptions—and, as a result, to enhance the bank's resilience.

It is important to distinguish between resilience frameworks and business continuity management (BCM). BCM emphasizes each business process and its continuity and recovery on a timely basis, while resilience is more specific to “important business services” (IBSs) subject to “impact tolerances.” There may be “intolerable impacts” that breach the impact tolerances, and those would not be covered by operational resilience; operational resilience only considers important business services in non-extreme situations.

The seven main steps for operational resilience are as follows:

1. Determine important business services.
2. Establish impact tolerances for important business services.
3. Map important business services and determine resources needed to provide them.
4. Design harsh, but realistic, scenarios to test vulnerabilities when providing important business services.
5. If impact tolerances are breached, review the lessons learned from stress tests and implement changes as needed.
6. Ensure all communication plans are ready to be executed when an incident happens.
7. Perform an annual self-assessment that is approved by the board of directors.

Resilience is focused on IBSs, and the IBSs between banks will naturally differ based on their respective business focus(es). For larger banks, it may be necessary to prioritize and narrow down the list of IBSs in resilience planning activities. Upon selecting the IBS, resilience assessment and reinforcement must be performed. This is a complicated process involving the mapping of the dependencies between the IBSs (Step 3), assessing key steps involved in potential disruption events and how to either avoid such events or recover from them on a timely basis. Obviously, the larger the bank, the greater complexity and much more data, IT resources, and people (over a wide range of different groups within the bank, such as human resources and IT) are required to establish a proper plan of resiliency.

Step 2 regarding establishing impact tolerances requires some elaboration, and the starting point would be business impact analysis (BIA). BIA reports examine the operational and financial implications arising from disruption as well as what is needed to recover from them. Implications could include one or more of the following: lost or delayed sales and profits; additional costs, penalties, and fines; and/or loss of customers. BIA reports will recommend that the restoration of business processes be done with priority given to those with the most operational and financial implications.

In the context of resilience, single points of failure (SPOFs) are appropriate KRIs. SPOFs should be eliminated through a system of backups and redundancies; otherwise, they are included in establishing tolerance thresholds and stress tests. Examples of a resilience KRI would be dependence on key employees (e.g., coding and cybersecurity experts) who have very specialized skills and who have not documented their processes and/or are difficult to replace, or dependency on a key supplier that has few or no substitutes (e.g., IT, data, and internet providers).



MODULE QUIZ 38.3

1. A quantitative analyst is in the process of combining internal and external loss data for model calibration purposes. The analyst has established specific criteria for the inclusion or exclusion of losses in the dataset. The method used by the analyst is best described as:
 - A. cut-off mix.
 - B. filtering.
 - C. scaling.
 - D. rule based.

KEY CONCEPTS

Risk management and measurement makes use of historical losses and events. The ORM framework can be thought of in four concentric circles: (1) incident/loss database, (2) assessment through RCSAs, (3) monitoring through KRIs, and (4) takeaways from major loss events or high-risk exposures.

The bank “must have documented procedures and processes for the identification, collection, and treatment of internal loss data.” Also, internal loss data must “capture all material activities and exposures from all appropriate subsystems and geographic locations.”

Loss events must be reported in terms of gross loss amounts net of any recoveries plus the reference dates. A summary of the sources and causes of the events should be provided as well. The four relevant dates per event include the following: (1) occurrence, (2) discovery, (3) reporting, and (4) accounting.

Boundary events refer to those that occur in a risk class that is not the same as the cause. They could include market and/or credit losses caused by human error (operational in nature).

The BCBS does require banks to “have processes to independently review the comprehensiveness and accuracy of loss data.”

LO 38.b

RCSAs involve assessing the probability and severity of operational risk. The process can be subdivided into examining inherent risk only (no consideration of the current controls in place) and examining residual risk (remaining risk after considering the effectiveness of current controls). RCSAs are performed on an annual basis, although a quarterly basis is possible if some operational risks are very significant.

RCSAs, by nature, are primarily nonquantitative and require significant judgment; therefore, they are not meant to quantify risk exposures. Instead, RCSAs are meant to provide greater awareness of risks and controls within a bank—and, ultimately, to determine whether additional steps need to be taken to mitigate risks.

Impact scales focus on the following categories: financial, regulatory, customer, and reputation, and they typically consist of four or five ratings. With likelihood assessment scales, amounts are stated either as a probability or frequency of occurrence. The combination of likelihood and impact is the RCSA matrix or heatmap. The combinations are assigned colors that correspond to risk intensity.

LO 38.c

KRIs will indicate the bank’s exposure level at a specific point in time. KPIs provide measurements on how effectively the bank operates. KCIs provide measurements on how effectively the bank’s controls are operating. KRIs, KPIs, and KCIs overlap significantly, and a given metric can have one or more of the risk, performance, and control elements, which is especially the case when analyzing a deficiency from a required benchmark level.

LO 38.d

There are three basic steps to the factor analysis of information risk (FAIR) model:

1. Determine risk factors and how they interrelate.
2. Measure each factor.

3. Computationally combine all factors.

LO 38.e

Fault tree analysis (FTA) is a form of deductive failure analysis whereby fault trees break out failure scenarios into external and internal conditions required for a major event to occur. FTA is seeing more use at banks now, where a chain of failures leads to a major loss; a set of conditions could happen at the same time (“AND conditions”) or happen alternately (“OR conditions”).

The Swiss cheese model involves “holes” (or vulnerabilities) in numerous layers that momentarily line up to permit the “perfect storm” in terms of an incident or loss. To deal with such a risk, proper control layering is required so that the holes can never be aligned.

Root-cause analysis allows for a much stronger comprehension of causes of incidents, together with the control failures that led to them. That, in turn, may allow for a more accurate estimation of the frequency of occurrence of specific events. Overall, root-cause analysis is thorough in nature and methodical in assessing the severity of the risk, taking into account any mitigation.

LO 38.f

The loss distribution approach (LDA) breaks out loss events into frequency and severity. The frequency and severity distributions are independently modeled and then convoluted into an aggregated loss distribution.

Frequency distributions are based on whole numbers (i.e., discrete) and express the number of times an operational incident occurs over a year. Modeling is usually done with a Poisson distribution. Severity distributions are continuous, asymmetric, and have fat tails; there are many minor incidents, but there are only a handful of major incidents resulting in significant losses. Modeling is usually done with a lognormal distribution.

Extreme value theory (EVT) is effective only when there is one main underlying cause that generates all losses and will generate future losses that are greater than current ones.

Internal loss data plays multiple roles—it is a source of detailed information on risks and control failures as well as the starting point for the LDA. Internal loss data can often give many data points to generate distributions, especially the area of “critical mass” consisting of high-frequency and moderate-severity events. However, internal loss data alone must be complemented with external loss data from other banks, for example. That will allow for a much greater understanding of the entire scope of loss outcomes that could affect a given bank. Internal and external loss data are combined to arrive at the computational data used for model calibration. The methods of combining the data include scaling, cut-off mix, and filtering.

The new standardized approach for calculating operational risk capital technically eliminates any requirements for banks to model their operational risk. As a result, their modeling activities are now focused on Pillar 2, the internal capital adequacy assessment process (ICAAP), stress testing, and operational resilience. The ICAAP covers operational risk and other risks and is included in Pillar 2, which requires coverage of both financial and nonfinancial risks. The ICAAP consists of self-

assessment of capital sufficiency in context of the nature of the business, potential changes in risk exposure due to business changes in the medium term, and current controls.

LO 38.g

The seven main steps for operational resilience are as follows:

1. Determine important business services.
2. Establish impact tolerances for important business services.
3. Map important business services and determine resources needed to provide them.
4. Design harsh, but realistic, scenarios to test vulnerabilities when providing important business services.
5. If impact tolerances are breached, review the lessons learned from stress tests and implement changes as needed.
6. Ensure all communication plans are ready to be executed when an incident happens.
7. Perform an annual self-assessment that is approved by the board of directors.

ANSWER KEY FOR MODULE QUIZZES

Module Quiz 38.1

1. **D** The dates of an operational incident (in order) are as follows: occurrence, discovery, reporting, and accounting. In the case of a prolonged and undiscovered manipulation of suspense accounts, the period between the date of occurrence and the date of discovery is long. However, because the date of reporting happens after the date of discovery, then the time interval between the date of occurrence and the date of reporting would be the longest. (LO 38.a)
2. **B** RCSAs are qualitative and largely judgment based. When backtesting the results of risk assessment against past incident experience, there is a tendency to *underestimate* the likelihood and *overestimate* the impact of an operational risk event. (LO 38.b)

Module Quiz 38.2

1. **B** KCIs provide measurements on how effectively the bank's controls are operating—and, in that regard, the fact that the business continuity plans are now past due their review date means that the control of the due date is not operating effectively. KRIs will indicate the bank's exposure level at a specific point in time. KPIs provide measurements on how effectively the bank operates. (LO 38.c)
2. **A** The equation is $0.99 \text{ (phishing email received)} \times 0.05 \text{ (firewall failure)} \times 0.10 \text{ (employee failure)} \times 0.03 \text{ (activity detection failure)} \times 0.01 \text{ (exit of information)} = 0.000001485 = 0.0001485\%$. (LO 38.e)

Module Quiz 38.3

1. **B** Filtering involves setting specific rules for the inclusion or exclusion of losses in the dataset to be used for modeling to avoid potential manipulation of results. With cut-off mix, at a specific loss threshold when there are few(er) internal losses, then external losses would be included in the model to have sufficient data points to generate a reliable distribution. With scaling, there are size adjustments

for losses to be consistent with the bank's size or inflation adjustments when a large number of years are involved. In this context, there is no such thing as a rule-based method. (LO 38.f)

¹ Reason, J. *Human error: models and management*, BMJ. March 18, 2000; 320(7237): 768–770.

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 5.

READING 39

RISK MITIGATION

Study Session 7

EXAM FOCUS

After identifying, assessing, and quantifying operational risks, the next logical step is risk mitigation. There is key terminology and specific knowledge that needs to be absorbed in this reading. For the exam, focus on the four types of internal controls and identifying examples of each. Also, be familiar with the four types of control testing and the factors that impact the effectiveness of control testing. In addition, pay careful attention to the four measures of impact reduction. Finally, understand the two key risk transfer methods as well as how to maintain and possibly enhance reputation through operational risk controls and mitigation strategies.

MODULE 39.1: RISK MITIGATION WITH INTERNAL CONTROLS AND PROCESS DESIGN

LO 39.a: Explain different ways firms address their operational risk exposures.

Risk Mitigation Characteristics

Risk mitigation identifies the measures a firm can undertake to minimize operational risk to acceptable levels. Operational risk is distinct from other risks like credit, market, and liquidity risks. In the context of risk mitigation, it is important to understand that minimizing operational risk involves a risk-return trade-off.

There are two types of operational risk: external and internal. **External operational risk** refers to risks from external events, including competitive forces, regulation, or geopolitical changes. While firms cannot prevent external operational risks, they can minimize them by reducing the exposure or mitigating the impact.

Internal operational risk refers to risks from people, systems, and processes. Firms can rely on strong internal controls to prevent this risk, and they can optimize the level of acceptable risk exposure through optimizing the risk-return trade-off.

Operational risks often arise from a financial institution's normal activities that create credit, market, or liquidity risks. The type of activity will determine the level of risk, and the compensation for the activity is typically in line with the level of risk taken.

For example, bank fees for wire transfers reflect compensation for the operational risk of a delay in or the failure of transfers, fraud, incorrect order execution instructions, etc. Investments in automation and stronger controls can improve the risk-return trade-off and reduce operational risk.

Operational risk cannot be eliminated, but it can be reduced. Reducing operational risk can generally be done in one of three ways: (1) establishing strong controls, (2) buying insurance, or (3) reducing or completely eliminating certain activities. Holding a minimum level of capital is also one way in which firms are mandated by regulation to reduce operational risk. How each institution responds to operational risk depends on its risk appetite. For example, some financial institutions may be comfortable with maintaining some level of risk while others prefer to minimize their risk exposure.

Risk Response

There are four ways to respond to risk: (1) tolerate, (2) treat, (3) transfer, or (4) terminate.

- *Tolerating risk* implies accepting the risk and its potential consequences without a need to mitigate it.
- *Treating risk* involves accepting the risk but mitigating its impact through some action or remedy. These mitigants include a robust set of internal controls, automating processes, and planning for risk scenarios.
- *Transferring risk* implies initially accepting the risk, but subsequently transferring it to a third party that is willing to take on the risk. The common way of risk transference is through insurance, in which one party pays a fee (e.g., an insurance premium) to a third party that in return is willing to accept the risk now or if/when it arises. Outsourcing is another example of risk transference. Note that while the risk itself can be transferred, accountability for the risk cannot be transferred as it remains with the original entity.
- *Terminating risk* is a more extreme outcome when none of the other risk responses will work, and it involves removing all risk exposure. This could involve discontinuing particular products or services altogether or discontinuing them in certain countries.



PROFESSOR'S NOTE

Think of tolerating risk as an unhedged position, treating or transferring risk as a hedged position, and terminating risk as avoiding the position altogether.

Types of Internal Controls

LO 39.b: Describe and provide examples of different types of internal controls, and explain the process of internal control design and control testing.

For risk mitigation with internal controls, the four main types to consider are: (1) preventive, (2) detective, (3) corrective, and (4) directive.

- **Preventive controls** aim to lower the chances of an event occurring in the first place; such controls are focused on the underlying causes and eliminating them. For example, segregation of duties is the primary control against fraud. In short, generation of, approval of, payment of, and recording of a given transaction occurs with the participation of four different parties. Other preventive controls within banking include limiting access, matching up signatures prior to processing at trade, and cross-checking client trades to client information on file to ensure that the trade is consistent with the client's risk and return preferences, for example.
- **Detective controls** serve as "alarms" of an event and aim to eliminate the event as quickly as possible while reducing any losses or other negative effects to the bank. An example of a well-known detective control would be a notice given to the cardholder of possible fraud based on unusual transactions. Other detective controls include exception reports and security/intrusion alarms. In some cases, there is crossover between detective and preventive controls; a second review of a transaction is detective in nature if the transaction has been processed but it could be preventive in nature if the transaction has yet to be processed and the error can be fixed prior to processing.
- **Corrective controls** aim to reduce the negative impacts of an incident and include business continuity plans (BCPs) and data backups. Such controls are not preventive in nature, but they often allow business to continue with less disruption and lost productivity.
- **Directive controls** provide guidance on performing a particular transaction or process and include policies, procedures, training, and supervision. The idea here is to educate and guide at all steps of the process to prevent errors (or at least reduce the impact of them).

Key Controls

Key controls function solely on a standalone basis to prevent the risk from occurring. They encompass all four of the control types just discussed. For example, key controls are preventive (e.g., automation) if they eliminate the risk of errors occurring, or they are corrective (e.g., backups) if they nullify the data loss because the backup will contain most or all of the data that was lost. Key controls are also known as primary controls and can be differentiated from non-key (secondary) controls, the latter of which merely supplement key controls but are not able to reduce risk on a standalone basis.

Automated Controls

In general, automated controls are superior to manual controls because automated controls provide much more reliability as they are not prone to human error. Examples of automated controls include reconciliations, data validation checks, and credit card fraud detection. However, automation may have merely changed the nature of the risk; human error risk now becomes an IT risk because the IT system could not execute the control properly or it becomes a model risk because the model is based on specific data and if that data is biased or inaccurate, the corresponding control becomes useless.

Notably with the change in manual to automated controls, there is a movement from high-likelihood/low-impact risks from random manual errors to low-likelihood/high-impact risks from a larger system-wide control failure.

Specific problems arising with automated controls include Type 1 (false positive) and Type 2 (false negative) errors when analyzing unusual and potentially fraudulent transactions, loss of automated controls due to system downtime, or system overcapacity. Automated controls are especially useful for settings involving large dollar amounts and/or high transaction speeds when the controls can detect potential problems as soon as possible and escalate them to allow the problems to be mitigated in time.

Control Testing

Control testing is part of the control assessment process whereby the bank's risk mitigation techniques are tested for their effectiveness. Control testing attempts to determine if controls are designed properly and if they are consistently and properly applied.

Ineffective controls may become or increase a vulnerability. Examples of poorly designed controls include the following:

- **Optimistic controls.** These controls are highly dependent on the individual operating the control. They are generally superficial controls such as document sign-offs in large quantities immediately prior to deadlines or any type of approval where the validating party has insufficient time and information to fully comprehend what she is signing off.
- **Collective controls.** These controls divide the work over numerous parties, which reduces individual accountability. Using the "double check" collective control is very common but the risk is that an individual may not be as thorough in verifying a given transaction because the individual is aware that someone else will look at it again and possibly catch their mistake. Therefore, it is best that double checks be performed by individuals at different hierarchy levels (e.g., supervisor and subordinate) or by individuals working in different departments.
- **More of the same.** Following an operational event arising from a control failure, a common response is to simply add more of the same type of control. This does not make sense as adding more of a bad/faulty thing will perpetuate the problem and result in more of the same control failures. Therefore, adding more controls here will not reduce risk.

Control testing is more rigorous with more inherent risk. The four main categories of control testing are as follows:

- **Self-assessment.** The lack of objectivity limits this form of testing to secondary controls or controls that relate to low inherent risk situations.
- **Examination.** There is documentation of the control process together with a written summary of the testing results. The level of detail and quality of the documentation will drive the usefulness of this control test. The limited scope of testing makes examination most appropriate for automated controls.

- **Observation.** The control in operation is witnessed on a “live” basis to determine if it works properly. Given the large number of controls in place, observation must be done on a sampling basis and given the thoroughness of testing, it is most appropriate for key controls.
- **Reperformance.** Control testing is done on a sample of transactions. A clear example would be the introduction of erroneous data into the system to determine whether the system is able to detect the error. This form of testing is used in model validation to compare the output with different datasets.

Control testing should also consider the following points:

- For reasons pertaining to independence and potential bias, control testing should generally be performed by an individual who is independent of the individual who designed the control. Self-certification is the notable exception.
- More (less) frequent control testing should be performed on risks with higher (lower) severity. Unstable risk situations also require more frequent testing.
- Testing samples need to be selected in a manner that closely mirrors the true population of items. A large enough sample size is required to ensure that the results are robust and repeatable. Care must be taken to avoid biased samples as they may overstate the effectiveness of controls.

Finally, control testing is usually done by the internal audit department (third line of defense), but it is common for the first line of defense to test certain key controls. The operational risk management (ORM) group (second line of defense) is not typically involved in control testing but must receive confirmation that the controls are properly designed and operating properly.

Process Design and Categories of Human Errors

LO 39.c: Describe methods to improve the quality of an operational process and reduce the potential for human error.

When organizations are exposed to operational risk, an important consideration is to design techniques to minimize process errors and to increase efficiency. The notion of **prevention through design (PtD)**, or safety by design, refers to optimizing processes by creating checklists, protocols, optimized systems, and standardization in order to minimize operational risk. PtD has parallels with the *Swiss Cheese model*, (introduced in Reading 38), which presents an analogy for why and how process errors and losses can occur due to human errors. In several fields, such as engineering, human error is often seen as a symptom but not the cause of errors, while poorly designed systems and processes are what give rise to human error.

It is therefore important to categorize human errors and look at process remedies for each type of error. Human error can be categorized as *slips* and *mistakes*, with mistakes further segmented into *rule-based* and *knowledge-based* categories.

- **Slips** are involuntary errors (i.e., skill-based), meaning they are not intentional. Slips can be due to inattention, distraction, or fatigue. They also include inadvertent typos like “fat finger” mistakes, for example, when a trader types an extra zero at the end of

a trade order or enters a transaction as a buy instead of a sell. Slips can be remedied by finding the root cause and treating it (e.g., by creating a better workspace, reducing noise levels, redesigning the processes, or establishing clearer accountabilities and consequences for actions).

- **Mistakes** are voluntary errors due to intentional actions.
 - **Rule-based mistakes** are due to flawed rules that often create conflicts of interest. Examples include selling inappropriate products to customers due to aggressive reward incentives to employees. Remedies include improving/changing the rules or establishing stronger controls.
 - **Knowledge-based mistakes** occur when an incorrect choice of action is made in a new situation or environment by relying on knowledge that may have worked in different circumstances. Remedies include better documentation of procedures, training, or support resources, as well as clear escalation rules.

Violations are another example of human operational risk, although not strictly characterized as an error. Violations are voluntary misdeeds (e.g., when an employee decides to take a different course of action despite knowing the rules). These can be remedied by establishing stronger supervisory controls, installing cameras, or recording calls to be able to document violations.

Lean Six Sigma and Quality Improvement

Lean Six Sigma is a managerial approach that aims to improve operational performance by eliminating waste and minimizing variations. It is essentially an optimized workflow process. **Lean techniques** look at eliminating the eight kinds of waste—or process ineffectiveness—including resource underutilization, time loss, and unnecessary tasks. **Six Sigma** focuses on minimizing variability, including variability of extreme outcomes and improving output quality. The Lean Six Sigma method is based on the *DMAIC cycle*, which looks to define, measure, analyze, improve, and control the processes. The Lean Six Sigma method is a popular analytical tool with many organizations that have complex products and processes.

Quality improvement is a managerial approach that also looks to improve operational processes by using the *PDSA cycle* for model improvement: plan, do, study, and act.

- *Plan* starts with defining an objective or goal and defining the outcome, including what, when, where, and who will implement the plan.
- *Do* refers to plan execution, collecting data, and documenting problems along the way.
- *Study* is the actual analysis of the collected data, comparing data to forecasts, and assessing opportunities for improvement.
- *Act* refers to making necessary adjustments to the processes based on analyzed data and creating the process for the next cycle, at which point the PDSA cycle starts again.



MODULE QUIZ 39.1

1. XYZ Bank just completed an internal reorganization in which it significantly improved its internal controls and management oversight of its businesses to address its operational risks. Which of the following risk responses best captures this scenario?

- A. Treating risk.
 - B. Tolerating risk.
 - C. Transferring risk.
 - D. Terminating risk.
2. Business continuity planning (BCP) would most likely be described as:
- A. a corrective control.
 - B. a detective control.
 - C. a directive control.
 - D. a preventive control.
3. A trader whose daily trading limit in a particular stock is 10,000 shares mistakenly enters a client order to sell 3,000 shares as an order to sell 30,000 shares. The trader's action is most likely an example of which of the following operational risk types?
- A. Slip.
 - B. Violation.
 - C. Rule-based mistake.
 - D. Knowledge-based mistake.

MODULE 39.2: OPERATIONAL RISK MITIGATION MEASURES AND MANAGEMENT

LO 39.d: Explain how operational risk can arise with new products, new business initiatives, or mergers and acquisitions, and describe ways to mitigate these risks.

Assessing New Products and Initiatives

Firms often assess and mitigate the risks of new products and initiatives through the New Product Approval Process (NPAP) and the New Initiative Risk Assessment Process (NIRAP). In the context of operational risk, new initiatives are especially important. They include new financial products or services to customers, new or updated outsourcing arrangements, and new projects and restructurings.

From a best-practice perspective, the owner of a new initiative should present a business case. A well-structured NIRAP business case has five components:

1. *Objective*. What the firm wants to achieve and why a product is introduced.
2. *Alternatives*. What other options exist outside of the proposed product.
3. *Expected benefits*. What are the benefits and potential disadvantages of the product.
4. *Commercial aspects*. What are the costs and funding needs.
5. *Risks*. What are the main risks that arise from the product and key mitigants to these risks.

Project risk levels vary greatly related to time, budget, and scope and, therefore, the levels of mitigation also vary. Project risks are managed by the *project team*, which produces regular reports on risks that are available to all stakeholders. Firms with a more mature risk culture will typically include a post-product delivery review, debriefs, and quality assessments in order to ensure that past successes can be replicated and mistakes can be avoided.

Introducing new products, software, or initiatives can also modify a firm's existing risks or introduce new risks. The ORM teams should help identify, assess, and mitigate the direct and indirect risks. The involvement of the ORM function will vary based on a project's life:

- *Initial stage (prior to the kickoff)*. Identify and assess the risks and establish plans to mitigate and monitor the risks.
- *Project life*. Provide regular reporting of operational and project risks, together with regular meetings with the risk and project teams to provide assessments and risk updates.
- *Project closure*. Provide debriefs, evaluation of deliverables, and analysis of the risks that materialized and those that were mitigated, along with lessons learned.

Mergers and Acquisitions

Mergers and acquisitions (M&A) represent large and complex projects and initiatives in a firm's life. The acquiring firm takes on (i.e., inherits) the risks of the acquired firm, including credit, market, and operational risks. The key problem the acquiring firm faces is that these risks are often not known in advance and can only be assessed after the merger/acquisition. Once the M&A project takes place, the acquiring firm's risk management team must undertake a complex risk assessment exercise. While the assessment of credit risk (and even market risk) is generally straightforward, the assessment of operational risk is more challenging. The level and details of operational risks are often only known months or even years following the merger/acquisition. In this regard, ORM can assist with assessing operational risk by creating a risk profile of operational risk exposures.

The integration of the acquired firm also creates operational risks. Risks can relate to potential errors or failures of integrating customer and account functions, payroll and other systems, and inter-company communications. Once again, the ORM function is useful in identifying, assessing, and mitigating these risks.

LO 39.e: Identify and describe approaches firms should use to mitigate the impact of operational risk events.

Financial institutions understand that even with very strong controls, losses and defaults will occur. As a result, reducing the impact of operational risk events and minimizing credit risk is critical. There are four measures of impact reduction: (1) contingency planning, (2) resilience measurement, (3) crisis management, and (4) communication.

Contingency Planning

Contingency planning is an alternative action plan should the expected outcome fail to materialize. It aims to provide an alternative solution and buffer to systems, processes, and people. Most firms have some form of contingency planning, which can be thought of as part of their *business continuity* or *disaster recovery* playbook. Responsibilities and timelines should be clearly established as part of contingency planning. A simple

form of contingency planning is having an extra charger or laptop for backup, while a much more sophisticated example is a bank having a remote disaster recovery site in case of a cyber or physical attack.

Two forms of contingency planning are business continuity management (BCM) and a disaster recovery plan (DRP), which improve operational resilience by helping recover critical functions in case an adverse scenario occurs. Systemically important financial institutions (SIFIs) often use BCM and DRP because a disruption in their operations could have systemic adverse impacts on the financial industry.

Business Continuity Management

BCM is essentially a firm's action plan detailing a series of tasks on what to do in case of a crisis scenario. BCM helps determine which business areas are critical to maintain in a crisis, and is typically part of a firm's business continuity plan (BCP).

The first step in the BCM process is to ensure senior management's support because proper governance starts at the top. BCM should have an owner assigned to it, which can be an individual or a team. The owner is responsible for the BCM design, including establishing the team members, key deliverables, a budget, and consulting specialists if necessary. The risks identified under the BCM process should be related to operational risk management. These can include technological, reputational, and environmental risks. The BCM process also identifies and manages the risks, develops a strategy and a plan, and implements the plan.

The BCM process is often supplemented by *business impact analysis*, which is a risk analysis for each possible event. This will also help define the recovery time. Additional risk mitigants can include obtaining external insurance and engaging external crisis-management specialists.

Event and Crisis Management

Strong event and crisis management and how well a firm can respond to major disruptions depends on the following three factors that determine the success of its BCP:

- *Speed*. The response to a crisis must be fast, especially considering that crises can spread quickly.
- *Competence*. Each task should be assigned to a specialist. Firms should engage external specialists if needed, especially for technology and communications.
- *Transparency*. Firms should promptly and transparently disclose operational loss events to staff, external stakeholders, and the public. A lack of transparency can seriously hurt a firm's credibility and lead to reputational and financial losses. Negative news headlines can amplify reputational risk and cause a loss of public confidence (but a prompt and transparent response may improve a firm's image).

Firms with strong risk management should have both a technical team and a communication team to ensure effective and quick response to risk events. The *technical team* includes experts like IT or security specialists who focus on IT-related disruptions (e.g., system failures, hacking) while business continuity specialists focus on business disruptions. The *communications team* is in charge of media

communications to employees, external stakeholders, and the public. Both of these teams should report to a member of the firm's senior leadership team. A BCP should be regularly tested. It is not uncommon for a firm to set up a "war room" for scenario analysis under various realistic and extreme stress scenarios.

When a significant operational risk event occurs, it typically has four key phases:

1. *Crisis*. The crisis is the firm's realization that an incident occurred, which can be within minutes, hours, or significantly longer. Incidents include cyberattacks or ransomware, damage to physical infrastructure (an earthquake damaging a building), or violent actions.
2. *Emergency response*. In this phase, specialists determine the best course of action and quickly implement it.
3. *Recovery*. This is the period during which the firm's operations fully or partially resume. Two recovery measures include (1) *Recovery Point Objective (RPO)*, which is the amount of data lost or to be recovered following a risk event; and (2) *Recovery Time Objective (RTO)*, which is the maximum amount of time that a business can endure a disruption.
4. *Restoration*. In this phase, all lost functions are recovered or restored, and the business is back to normal operations. This can happen quickly (e.g., a recovery following a power outage) or it can be very lengthy (e.g., a multi-year business recovery following the COVID-19 pandemic).

LO 39.f: Describe methods for the transfer of operational risks and the management of reputational risk, and assess their effectiveness in different situations.

Risk Transfer

Although risk transfer is often effective, it is not free, and it may bring on incremental risk(s). External insurance and outsourcing are two common forms of risk transfer.

External Insurance

By purchasing insurance, the insured will incur an ongoing premium cost and will receive financial compensation if a specific loss occurs, therefore, loss volatility is reduced. For example, insurance coverage is usually provided for errors and omissions made by employees.

In deciding whether to purchase insurance, the firm needs to determine whether the insurance will fully or only partially mitigate the risk. Insurance is a logical form of risk mitigation if the risk is reasonably predictable and quantifiable so as to determine a reasonable premium payment. Also, the risk exposure and impact should be largely transferable to the insurance company so that the risk is largely mitigated for the insured.

There is always a cost-benefit decision to be made about paying the insurance premium versus assuming the loss volatility. From the perspective of the insurance company over the long-term, accurate pricing of insurance means that the insurance premium will equal or be greater than the expected losses should the risk event occur. Because

insurance costs may be relatively high in some cases, many larger banks will choose to self-insure and assume the low loss volatility when it comes to small losses. Those banks will purchase insurance where they may face very significant losses (e.g., tail events including cyberattacks or business interruption) that could cause greater volatility in profit and loss.

Insurance does not fully transfer risk as the insured relies on the insurance company being able and willing to provide compensation for the loss. For example, compensation may not occur until several months after the event, which could subject the insured to a liquidity crunch during that time.

Outsourcing

In many instances, it makes good business sense for a firm to contract out some duties that might be better performed by a third party that specializes in those duties (e.g., accounting, IT, marketing). In recent years, specialized financial technology (FinTech) banks have emerged that are more likely to handle their own IT needs and outsource more traditional tasks like credit decisioning.

Outsourcing transfers risks to a third party but the exact amount of risk mitigation is case-specific. For example, if a bank outsources its IT activities to a foreign country with lower wage rates to reduce costs, then in exchange for higher profits, the bank will face new risks due to the IT services being performed offsite. The potential service delays, lack of supervision, and language barriers could represent the incremental risks taken on.

Alternatively, the bank may outsource specialist services (such as data storage) to a much more capable firm with far superior security capabilities. In this case, there may be a net higher financial cost to outsourcing in exchange for reduced internal retention of operational risk.

In either instance, there is incremental third-party risk as the bank must rely on the controls of the third party operating properly. Properly operating controls may not always be the case and, therefore, outsourcing is sometimes more accurately described as risk sharing rather than risk transfer.

Managing Reputational Risk

Reputational damage goes far beyond the scope of operational risk although it is significantly impacted by operational events. As a result, numerous controls and other preventive strategies to address timeliness and communication with stakeholders could be implemented to minimize reputational damage after a major operational risk event occurs.

A preventive strategy could be focused on customer confidence. A detective control (e.g., monitoring system downtime) is meant not only to detect an operational failure but also to minimize the negative reputational effects. In general, corrective risk controls and mitigation activities are meant to maintain the bank's reputation. Doing so requires a long-term approach and, in that regard, reputation management has to be integrated into employees' ongoing duties. Rewarding employees who maintain and enhance the bank's reputation is encouraged (e.g., department with the highest

customer satisfaction scores). Although far from common, rewarding employees for self-reporting operational risks and near misses (which helps avoid future costs and reputational damage) is encouraged.

General business decisions have an impact on the bank's reputation. For example, being the banker for an individual or firm convicted of significant fraud poses a significant reputational risk. Sufficient due diligence and a cost-benefit analysis must be performed prior to making a decision to enter into a business relationship with specific clients, suppliers, and other third parties.

Reputation management has prevention and mitigation aspects. In terms of prevention, image building, relationship building, and contingency planning are some key considerations. In terms of mitigation, communication, timely response, and transparency are important. Specific to crisis communication, the *three Rs* must be followed:

- *Regret*. Ownership and taking responsibility for the event.
- *Reason*. Honesty in terms of identifying the exact cause(s) of the event.
- *Remedy*. Finding a fair resolution to reimburse affected parties.

Stakeholder analysis/differentiation is key to ensure that reputation management is targeted so that the remedies are effective. For large banks, the regulators are always a key stakeholder. Therefore, large banks should always be building their reputation for transparency and cooperation with regulators as a preventive measure. That will be useful when having to deal with regulators should an operational failure occur.

A strong relationship and open communication with stakeholders can generate goodwill or reputational capital that can be relied on during a crisis and enhance a bank's resilience after an operational incident. Additionally, crisis management that is handled with care and transparency can maintain or even enhance a bank's reputation. In other words, a bank's superior ability to deal with a crisis may allow it to shine and limit any associated reputational damage.



MODULE QUIZ 39.2

1. In which of the New Initiative Risk Assessment Process (NIRAP) business case topics would you most likely find an analysis of project costs and funding arrangements?
 - A. Initial stage.
 - B. Alternatives.
 - C. Expected benefits.
 - D. Commercial aspects.
2. A disaster recovery plan (DRP) is generally considered to be a form of:
 - A. event management.
 - B. contingency planning.
 - C. business continuity planning (BCP).
 - D. business continuity management (BCM).

KEY CONCEPTS

Risk mitigation refers to minimizing operational risk to acceptable levels. It involves a risk-return trade-off. External operational risks are risks from external events, like competition, regulation, or geopolitical changes. Internal operational risks are risks from people, systems, and processes.

Operational risk can arise from a financial institution's normal activities, and the type of activity will determine the level of risk. The compensation for the activity is typically in line with the level of risk taken. Operational risk cannot be eliminated, but it can be reduced.

Reducing operational risk can be done by (1) establishing strong controls, (2) buying insurance, or (3) reducing or completely eliminating certain activities. How institutions respond to operational risk depends on their risk appetite.

There are four ways to respond to risk:

- Tolerating risk implies fully accepting the risk.
- Treating risk involves mitigating its impact through some action or remedy.
- Transferring risk implies finding a third party that is willing to take on the risk (e.g., via insurance).
- Terminating risk involves removing all risk exposure (e.g., by discontinuing certain products or services).

LO 39.b

For internal controls, the four main types to consider are preventive, detective, corrective, and directive. Preventive controls aim to lower the chances of an event occurring in the first place; such controls are focused on the underlying causes and eliminating them. Detective controls serve as alarms of an event and aim to eliminate the event as quickly as possible while reducing any losses or other negative effects to the bank. Corrective controls aim to reduce the negative impacts of an incident and include business continuity plans and data backups. Directive controls provide guidance on performing a particular transaction or process and include policies, procedures, training, and supervision.

In general, automated controls are superior to manual controls because automated controls provide much more reliability as they are not prone to human error. However, automation may have merely changed the nature of the risk. Specific problems arising from automated controls include Type 1 (false positive) and Type 2 (false negative) errors and loss of automated controls due to system downtime or system overcapacity.

Ineffective controls may become or increase a vulnerability. They include optimistic controls that are highly dependent on the individual operating the control and such controls are often quite superficial. In addition, they include collective controls that divide the work across numerous individuals, which reduces individual accountability. Finally, following an operational event arising from a control failure, a common response is to simply add more of the same type of control.

The four main categories of control testing are self-assessment, examination, observation, and reperformance.

LO 39.c

Prevention through design (PtD, or safety by design) aims to minimize operational risk by creating checklists, protocols, optimized systems, and standardization. It aims to improve processes to reduce or eliminate human error.

Human error can be categorized as slips or mistakes, with mistakes further segmented into rule-based and knowledge-based mistakes.

Slips refer to involuntary errors, including inattention or distraction, and can be remedied by creating a better workspace or work environment, redesigning processes, or establishing clearer accountabilities.

Mistakes are voluntary errors. Rule-based mistakes arise due to flawed rules, and can be remedied by improving rules, establishing stronger controls, etc. Knowledge-based mistakes happen when an incorrect choice of action is made in a new environment, and can be remedied by improved process documentation, appropriate training, or clearer escalation rules.

Violations are not caused by human error but are voluntary misdeeds (e.g., by taking a different course of action despite knowing the rules). Violations can be remedied by improved supervisory controls or better detection methods (e.g., cameras or recording calls).

Lean Six Sigma is a managerial approach that looks to improve operational performance by eliminating waste, minimizing variability, and improving output quality. It is based on the DMAIC cycle to define, measure, analyze, improve, and control the processes.

Quality improvement is another operational risk optimization approach. It is based on the PDSA cycle for model improvement: plan, do, study, and act.

LO 39.d

The New Initiative Risk Assessment Process (NIRAP) can help assess the risks of new products and initiatives. The NIRAP business case has five components: (1) objective, (2) alternatives, (3) expected benefits, (4) commercial aspects, and (5) risks.

Project risks vary greatly by time, budget, and scope. The project team should create regular reports on risks. Firms can also include a post-product delivery review, debriefs, and quality assessments. The operational risk management (ORM) team helps identify, assess, and mitigate risks. The ORM function depends on the stage of a project's life: (1) initial stage: identify, assess, mitigate, and monitor risks; (2) project life: present reports on project risks, and provide risk updates; and (3) project closure: post-project debriefs of lessons learned, evaluation of deliverables, and analysis of the risks.

Mergers and acquisitions (M&A) present unique risks to the acquiring firm because many of the risks relating to the project are not known in advance. As a result, the acquiring firm's risk management team must undertake a complex risk assessment exercise by creating a risk profile of operational risk exposures. The integration of the acquired firm creates additional risks (e.g., related to the integration of customer and account functions, payroll, and other systems). The ORM function should identify, assess, and mitigate these risks.

LO 39.e

There are four measures of reducing the impact of operational risk events: (1) contingency planning, (2) resilience measurement, (3) crisis management, and (4) communication.

Contingency planning is an alternative action plan in case the expected outcome does not materialize. It is seen as a part of firms' business continuity framework. Two forms of contingency planning include business continuity management (BCM) and a disaster recovery plan (DRP).

BCM is a firm's action plan detailing what tasks to do in case of a crisis scenario, and it is typically part of a firm's business continuity plan (BCP). Steps in the BCM process include senior management support, assigning an owner responsible for the BCM design, identifying and managing the risks, developing a strategy/plan, and implementing the plan. The BCM process can be supplemented by business impact analysis (which is a risk analysis for each possible event), obtaining external insurance, and engaging external crisis-management specialists.

The following three factors determine the success of a firm's BCP:

- Speed: The response to a crisis must be fast.
- Competence: Each task should be assigned to an internal or external specialist.
- Transparency: Firms should promptly and transparently disclose details of risk events to all stakeholders.

Firms should have both a technical team and a communication team to respond to risk events effectively and quickly. The technical team focuses on IT-related disruptions as well as business disruptions. The communications team focuses on media communications to all stakeholders.

The four key phases of a significant operational risk event include (1) crisis (realization that an incident occurred), (2) emergency response (promptly determining the best course of action), (3) recovery (period during which the firm's operations resume), and (4) restoration (firm is back to normal operations).

LO 39.f

By purchasing insurance, the insured will incur an ongoing premium cost and will receive financial compensation if a specific loss occurs. Therefore, loss volatility is reduced. There is always a cost-benefit decision to be made about paying the insurance premium versus assuming the loss volatility. Because insurance costs may be relatively high in some cases, many larger banks will choose to self-insure and assume the low loss volatility when it comes to small losses.

In many instances, it makes good business sense for a bank to contract out some duties that might be better performed by a third party that specializes in those duties. Outsourcing transfers risks to a third party but the exact amount of risk mitigation is case-specific. In some cases, there is incremental risk taken on and, in other cases, outsourcing is more accurately described as risk sharing rather than risk transfer.

General business decisions have an impact on the bank's reputation. Therefore, sufficient due diligence and a cost-benefit analysis must be performed prior to making a decision to enter into a business relationship with specific clients, suppliers, and other third parties. Reputation management has prevention and mitigation aspects. In

terms of prevention, image building, relationship building, and contingency planning are some key considerations. In terms of mitigation, communication, timely response, and transparency are important. Stakeholder analysis/differentiation is key to ensure that reputation management is targeted so that the remedies are effective. For large banks, the regulators are always a key stakeholder.

A strong relationship and open communication with stakeholders can generate goodwill that can be relied on during a crisis and enhance a bank's resilience after an operational incident.

ANSWER KEY FOR MODULE QUIZZES

Module Quiz 39.1

1. **A** Treating risk involves accepting the risk but mitigating its impact through some action or remedy. These mitigants include a robust set of internal controls, automating processes, and planning for risk scenarios. (LO 39.a)
2. **A** BCP is a corrective control that involves reducing the impact from an operational incident. In that regard, although BCPs do not reduce the likelihood of risks occurring, BCPs help reduce the negative impacts if they do. Specifically, a good BCP that is properly implemented with the onset of an operational incident helps ensure that the business continues to operate as normal or as close to normal. (LO 39.b)
3. **A** Slips refer to involuntary errors, and include inadvertent typos such as mistakenly entering incorrect trade instructions. The trader's daily limit is irrelevant in determining the type of human error.
Violations are not a type of human error but are voluntary misdeeds. Rule-based mistakes arise due to badly designed or flawed rules. Knowledge-based mistakes arise due to incorrect choices of action in a new environment. (LO 39.c)

Module Quiz 39.2

1. **D** An analysis of costs and funding arrangements would be included under the *commercial aspects* component of the NIRAP model. The other four components include (1) objective (analysis of product rationale), (2) alternatives (analysis of other options), (3) expected benefits (analysis of benefits and disadvantages of the product), and (4) risks (analysis of risks). (LO 39.d)
2. **B** DRP and BCM are considered specific forms of contingency planning. (LO 39.e)

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 6.

READING 40

RISK REPORTING

Study Session 7

EXAM FOCUS

The focus of this reading is on all aspects of operational risk reporting. For the exam, be familiar with the different board subcommittees that have operational risk management responsibilities, as well as the members of the organization's central risk functions and business lines. Also, understand the many components that must be included in operational risk reports and best practices for how those components are reported. Whether the audience is internal or external, there are data and reporting challenges that entities must navigate to comply with regulations and meet stakeholder expectations.

MODULE 40.1: ORGANIZATIONAL COMMITTEES

LO 40.a: Identify roles and responsibilities of different organizational committees, and explain how risk reports should be developed for each committee or business function.

As the final step of risk management, risk monitoring provides organizational leaders with a view of the organization risk profile, assurance of operating within risk appetite limits, and the tools to evaluate the effectiveness of the risk management framework. The operational risk profile includes operational exposures, risk appetite and indicators, past risk events, mitigation strategies, and resilience measures. In assessing risk at a general and granular level, a key measure is the variance between actual and expected losses (both frequency and severity).

The audiences for operational risk reporting are external and internal. External audiences include risk regulators, clients, suppliers, and the public. Internal audiences include the risk committee, the audit committee, the executive committee (ExCo), central operational risk function, and business lines. Individuals may serve on multiple boards concurrently. Internal audiences and their reporting needs are described next.

Risk Committee (Within the Board of Directors)

The **risk committee** is charged by the board with monitoring the firm's risk management framework. The committee, which monitors operational and all other

risks, must receive reports that are sufficient for them to determine that monitoring and control systems are operating and complying with the board-set risk appetite. The information received by the risk committee includes summary information on operational risk exposures, trends, and emerging risks. Detailed level information includes key risk indicators (KRIs), large event investigations, and the frequency and severity of risk events. Based on this information, the risk committee will provide directives to be executed by the ExCo.

Audit Committee (Within the Board of Directors)

The **audit committee** is responsible for third-level oversight of an organization, which is directly managed by the internal audit function. This function provides assurances regarding the effectiveness and efficiency of an entity's internal control system. Internal audit reviews operational risk and internal control functionalities on a regular basis and reports findings to the audit committee and the ExCo.

Executive Committee (Within the Board of Directors)

The **executive committee (ExCo)**, serves as the steering committee for the overall board and consists of senior executives and elected board members. Responsibilities include prioritizing issues, ensuring strong governance, overseeing board policies, and facilitating decision-making between board meetings and during crisis situations. The ExCo also oversees the effective and proper execution of the operational risk management framework. Included in the reporting received by the ExCo are risk exposures, trends, events, action plans, culture, and remediation efforts.

Central Operational Risk Function (And Operational Risk Committee)

As the second line of oversight, the **central operational risk function** collects and aggregates information for reporting to both the risk committee and individual business line managers. The information collected includes risk exposures, action plan statuses, controls, risk profile modifications, and information on risk events. The presentation of this information should support decision-making at all levels while presenting the risks and their interactions in a comprehensive and holistic manner.

Business Line Managers (And Risk Champions)

The closest level of monitoring operational risk data is performed at the **business line managers** level, with a focus on KRIs, action plan progress, and the types and impacts of operational risks. These managers and risk champions are tasked with monitoring their own risks and benchmarking them to firmwide averages or other lines/departments.

A major challenge is determining the appropriate size of reports. Reports that are too large can cause readers to miss critical information, while reports that are too small and condensed may be too aggregated to provide real value. For defective key controls, near misses, and high risks, these elements are typically escalated to higher levels with minimal adjustments. All other data is typically summarized in aggregate.



MODULE QUIZ 40.1

1. Which of the following statements about the board of directors is most accurate regarding operational risk monitoring?
 - A. The audit committee serves as the second line of risk oversight.
 - B. The risk committee is only tasked with monitoring operational-type risks.
 - C. A committee member cannot serve on both the risk committee and the audit committee.
 - D. The executive committee oversees the execution of the operational risk management framework.
2. The internal group most likely to focus on key risk indicators (KRIs) and benchmarking is:
 - A. the audit committee.
 - B. the executive committee.
 - C. the business line committee.
 - D. the central operational risk function.

MODULE 40.2: OPERATIONAL RISK REPORTING COMPONENTS

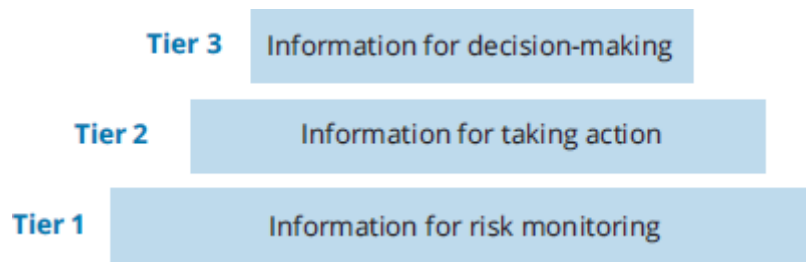
LO 40.b: Describe components of operational risk reports and explain best practices in operational risk reporting.

The overall goal of risk reporting is to help ensure actions are in alignment with risk appetite, risk acceptance, and strategies for risk mitigation. Although it is a relatively new area, operational risk management can be accomplished through the use of quantitative and qualitative measures.

The **reporting cake** is a term coined by Chapelle (2015)¹ and used by banks to reflect the volume of information reported to various stakeholders. The tiers are described next and shown in Figure 40.1.

- *Tier 1 (bottom layer).* The recipients of the information are *business line managers and risk champions*. In this tier, there is no distinction between risk reporting and risk monitoring. The metrics presented represent a full set, and monitoring is performed daily.
- *Tier 2 (middle layer).* The recipients of the information are the *operational risk committee*, and the only information provided is that which requires actions (e.g., fixing a process, budget discussions, or early interventions to mitigate risk event impacts). Non-action items can be presented in summary form on a monthly or quarterly basis.
- *Tier 3 (top layer).* The recipients of the information are the *executive and board risk committee*. The data presented is high level and often includes leading indicators, performance trends, progress on strategic plans, and the results of risk impacts relative to objectives.

Figure 40.1: The Reporting Cake



A comprehensive internal **operational risk management (ORM) report** contains the following components, described in detail next: (1) prioritized risks and outlook, (2) heatmap and risk register, (3) risk appetite metrics, (4) key risk indicators (KRIs) and issue monitoring, (5) risk events and near misses, (6) action plans and remediation, and (7) emerging risks and horizon scanning.

Prioritized Risks and Outlook

Often narrowed down to the top 10, this list presents the most important risks out of the entire risk inventory. The prioritization may derive from the magnitude of inherent risk (if no action is taken) and/or the level of residual risk (the net impact after mitigation activities are employed). Top 10 lists typically include risks related to technology breakdowns, cyberattacks, loss of data, regulatory and compliance breaches, and transformation projects (like the implementation of a new financial system). For each risk identified, the presentation should include the ranking, description, inherent components (likelihood, severity, rating), residual components (likelihood, severity, rating), and outlook (improving, getting worse, or status quo).

Heatmap and Risk Register

Risk and control self-assessment (RCSA) exercises are used to create a risk register that lists the different operational risks within an entity. The risk register is similar in form to the top 10 list, although the risk register will often list the controls applied to go from inherent risk to residual risk.

A **heatmap** is a visual representation of the risk register that is often a more effective way of presenting the data than lengthy narratives and small-font data tables. Figure 40.2 illustrates a potential heatmap where likelihood is mapped against severity. Boxes in dark blue represent the highest risks, while boxes in dark gray represent the lowest risks. The numbers in the boxes represent a hypothetical number of risks identified. Note that heatmap colors often consist of red (urgent), amber (above acceptable levels), yellow (approaching limits), and green (within risk appetite).

Figure 40.2: Operational Risk Heatmap

Likelihood	Near certain	5	2	7	1	1
	Likely	4	4	2	1	1
	Possible	3	6	1	2	1
	Unlikely	4	5	3	2	0
	Rare	1	3	2	2	3
		Insignificant	Minor	Moderate	Major	Severe
		Severity				

Risk Appetite Metrics

The information presented to the board of directors helps them determine whether the firm's operations are aligned with its risk appetite, such that any deviations require action plans to mitigate the risk. Risk appetite KRIs (also known as **risk appetite metrics**) measure a firm's compliance with risk limits in line with its risk appetite. A standard KRI presentation template will include the type of KRI, the name, thresholds, actual values relative to thresholds, and an overall score for each KRI.

KRIs and Issue Monitoring

Key risk indicators (KRIs) are used by management in conducting forward-looking analyses across different activities and/or detailed analyses for specific risks. To be efficient, firms tend to leverage information already collected. A KRI dashboard is a summary presentation of key metrics, along with values, trends, and overall scores. Examples of metric sources and indicators include the following:

- *Human resources.* This includes attendance for compliance training, the percentage of individuals trained, and disciplinary case counts.
- *Risk control.* This includes the percentage of completed risk management action plans, and the percentage of timely reporting for operational incidents.
- *Audit.* This includes timeliness of responses to audit findings, and the number of findings.
- *Compliance.* This includes the percentage of complaint responses received within an established timeline, and the number of conflicts of interest reported.

In this case, *issues* are defined as indicators of operational problems or control system concerns that can cause incidents if not addressed. Operational problems, process delays, and documented IT problems are examples of issues. Issues tend to be specific to a business line or activity and are often process based. As issues appear before actual incidents, they may be useful as preventive KRIs and should be grouped by business line or by major project or initiative, if applicable.

Risk Events and Near Misses

Fundamental to ORM reporting is the need to report on risk events, near misses, and losses. **Risk event reports** include details on the events (number and size), frequency

and severity on a per-period basis, trends over time (monthly, quarterly, or annually), and specific narratives concerning larger incidents that extend above predefined materiality thresholds.

Reporting thresholds will vary by entity. While some firms may focus just on collecting events tied to large losses (i.e., five- and six-digit losses), others may want to collect data on all risk events, regardless of the size of financial loss. Events tied to regulatory impacts or reputational damage tend to be collected and reported for all entities. Fortunately, entities seem to incur small losses with far greater frequency than large losses.

Near misses are critical to report and are evaluated based on the materiality of potential impact avoided. The lessons learned are tremendously valuable to an entity, without the incurrence of actual losses. In theory, reporting thresholds for both actual risk events and near misses should be based on potential impact. Challenges in estimating potential impact lead organizations to use observed impacts to establish reporting thresholds.

Action Plans and Remediation

An **action plan** is designed to improve the control environment through the use of risk mitigation programs. Corrective plans are reactionary in nature and often stem from large incidents. A corrective risk mitigation strategy comes from surprise loss events or unexpected gaps and weaknesses in ORM systems. Detective controls are designed to identify potential incidents before they become loss events. Preventive action plans are put in place to proactively manage risks before they become major problems.

Business line owners are responsible for tracking and reporting action plans, implementing controls, and providing progress updates. The goal is to hit a *zero objective*, which means there are no overdue action plans and no overdue audit recommendations. *Discipline indicators* is another phrase for overdue metrics, which are reported along with current metrics to entity leadership on a periodic basis.

Emerging Risks and Horizon Scanning

Horizon scanning is used to identify emerging risks and new trends that are reported on a monthly or quarterly basis to the board risk committee. Horizon scanning tends to be focused on the regulatory and compliance environment, with an eye on emerging risks and volatility changes. Risk timeline categories include risks expected to arise within one year, within one to three years, and beyond three years.

Risk Software

Governance, risk, and compliance (GRC) systems are risk software applications that help organizations collect and report on operational risk data. Although they vary in cost and complexity, GRC systems are all designed to collect and collate risk data, link risks with internal controls, and generate automated reports that can be used throughout the organization.



1. Using a reporting cake model, high-level data such as leading indicators and strategic plan progress will most likely be reported in which tier?
 - A. Tier 1.
 - B. Tier 2.
 - C. Tier 3.
 - D. Tier 4.
2. A presentation provided to executive leadership on the top 10 risks an entity is facing should include all of the following except:
 - A. descriptions of the risks.
 - B. timelines for risk eliminations.
 - C. inherent and residual elements of each risk.
 - D. a ranked order based on likelihood and severity.

MODULE 40.3: OPERATIONAL RISK REPORTING CHALLENGES

LO 40.c: Describe challenges to reporting operational risks, including characteristics of operational loss data, and explain ways to overcome these challenges.

As with any monitoring and reporting activities, the cost-benefit relationship must be evaluated when determining what operational risk data to collect, the frequency of monitoring, and the level of reporting. The three analytical considerations that apply are (1) the cost of collecting the information must be less than the value of that information; (2) the information should be useful, and the content should align with entity objectives and priorities; and (3) reporting should influence decision-making (even if the decision is to make no changes). In addition to the cost-benefit challenge, there are several other challenges related to operational risk reporting, as described next.

Operational Risk Event Data Asymmetry

Operational losses tend to be heavily skewed away from the mean such that there are a small number of high-severity, but low-frequency events. High-frequency, low-severity events tend to have a minimal impact on the loss budget. Resources devoted to risk management should be geared toward the mitigation and prevention (if possible) of large incidents, as opposed to trying to remedy visible but insignificant events.

Large Risk Event Escalation

Upper management needs to review and act on large risk events and on near misses that are significant enough to be above the organization's risk tolerance. These events require root-cause analyses, detailed reporting, and action plans.

Small, Frequent Losses

Fortunately, most of the operational risk incidents reported by entities are small (but frequent) losses. While they may not have a huge impact on the budget, they should be regularly analyzed and reviewed to determine if there are any structural flaws or control breaches that merit action. Random and relatively insignificant losses are less of a concern.

Operational Loss Benchmarking

Using benchmarks when reporting operational risk losses can help management decide on capital allocations and operational risk budgets. Benchmarks may be measures such as regulatory capital (basis points of capital consumed) or gross income. Similar entities across business units can be compared by reporting losses in basis points of capital or as a percentage of total project budget, total cost center budget, or gross income. Percentage reporting makes it easier to compare entities of different sizes.

Operational Risk Distributions

Averages (mean values) have more meaning in symmetric, bell curve-type distributions with no skewness or outliers, minimal variance, and a single mode. Operational risk distributions do not follow this pattern, which makes averages misleading. In fact, the real value of ORM comes from identifying and understanding outliers (departures from the norm). Because averages hide the diversity in the data, reviewing an entire distribution and analyzing it by subcategories can be more helpful.

Describing these distributions using the median (i.e., midpoint) and first and third quartiles is a superior approach. Alternatives to using the average apply not only to operational losses, but also to risk assessments, ratings, key performance indicators (KPIs), and KRIs.

Concentrations, Outliers, and Scenarios

As noted earlier, outliers hold tremendous informational value in risk management. Past patterns, distribution concentrations, and distances between observations all merit significant analysis. A *normality* baseline can be established through the lens of a trend analysis across multiple cycles.

For data analytics to be valuable, they have to be adaptable to the features and nature of data considered. Data that has different underlying functions and distributions should not be presented in the same exact way across the board. Although most risk management reporting is devoted to problems and large losses, there are lessons to be learned from positive outliers and good performance.

Loss profiles need to be analyzed through the assessment of high-, medium-, and low-risk scenarios. Climate change and associated weather-related impacts are an example of risks that, in more recent years, have taken on added importance and have required significant scenario modeling.

Qualitative Risk Data Aggregation

Qualitative risk data must be aggregated for operational risk reporting purposes, but the ways in which it is presented (e.g., color ratings, risk scores) make it difficult to

quantify. For example, an extreme risk (Level 1) and a low risk (Level 3) do not average out to equal a moderate risk (Level 2). Options for aggregating qualitative data include the following:

- *Conversion and addition.* This method involves taking qualitative metrics and converting them into a monetary unit that is continuous, additive, and linear. Nonfinancial elements like continuity and reputation are converted into financial amounts and summed. Presenting risks in monetary terms helps increase executive-level awareness.
- *Categorization.* Color and score can also be used for reporting. For example, red, yellow, and green can indicate high, moderate, and low risks. When presented in a graphical format like a bar chart, the longer (or taller) the red area, the greater the concern regarding the high risks.
- *Worst-case reporting.* This is the most conservative approach, where a group of KRIs may have a negative score and the entire group is reported as red in aggregate even if only one of the KRIs is red. While this approach is helpful when risk tolerance is low, it may create more concern than is merited.

Combined Assurance

The goal of **combined assurance** is to align assurance processes among all providers (including internal audit) to inform senior management and the audit committee about governance, controls, and risk management. Combined assurance requires significant coordination and collaboration among the three lines of defense within an entity. Ownership, accountability, and the avoidance of duplication are critical. The combined assurance map is owned by the ORM function and is used to report risk oversight results to the appropriate committees. The map identifies risk types and assessment scopes, and for each line of defense, a color coding (in line with the heatmap presented earlier) is assigned to indicate whether an assessment has been made—and if so, whether the assessment is satisfactory (green), needing of attention (yellow), or unsatisfactory (red).

In terms of the *three lines of defense*, the reviews conducted are as follows:

- *First line:* assessment of risks and controls, controls testing, and attestation that risk management and control activities are functioning as intended.
- *Second line:* oversight of the activities performed in the first line, sample control testing, and deeper dives into specific risk types.
- *Third line:* periodic internal audit reviews in line with the audit cycle.



MODULE QUIZ 40.3

1. Operational risk distributions do not lend themselves to using averages (i.e., mean values) for all of the following reasons except:
 - A. the distribution is asymmetric.
 - B. the data may have significant variances.
 - C. there may be a large quantity of outliers.
 - D. there is minimal skewness in either the right or left tail.
2. For the second line of defense in a combined assurance approach, the central operational risk function will perform which of the following activities?

- A. Internal audit reviews.
- B. Deep dives into specific types of risks.
- C. Overall assessments of risks and controls.
- D. Oversight of the activities performed by the third line.

MODULE 40.4: EXTERNAL REPORTING BEST PRACTICES

LO 40.d: Explain best practices for reporting risk exposures to regulators and external stakeholders.

The Basel regulatory framework (**Pillar 3**) addresses public disclosure of financial and operational risk information. This framework requires banks to calculate their operational risk capital using information that complies with the standardized approach. Relevant information includes 10 years of internal loss events (for the internal loss multiplier [ILM]) and data from the last three years for the business indicator component (BIC).

The three types of operational risk disclosure requirements include the following:

- *Qualitative information.* The risk management and governance arrangements established by the entity to manage, mitigate, and/or transfer its operational risks are presented. Also included is information on the structure of their ORM and control functions, as well as policies, procedures, and guidelines. Data and systems used to measure operational risk are also included here.
- *Historical losses.* There must be 10 years of aggregate operational losses reported, along with operational risk capital calculations. Regulated entities and banks should provide qualitative narratives and material information along with the quantitative data presented, while at the same time protecting proprietary and confidential information.
- *Business indicator and subcomponents.* These form the primary part of calculations for operational risk capital. As with historical loss disclosures, narratives covering significant changes during the reporting period and associated key drivers are expected.

The saying “absence of evidence is evidence of absence” means that auditors and regulators will require proof over verbal assertions regarding controls and risk. Reports and documentation provide the proof needed. Minutes from committee meetings and discussions, issues, and decisions included in these minutes serve as an appropriate level of documentation.

Independent of Pillar 3 requirements, financial institutions in most areas are required to inform regulators about breaches of conduct and significant operational risk events triggered by the following criteria:

- *Reputation criteria.* These are events that could have a significant impact on firm reputation.

- *Resilience criteria.* These are events that could negatively impact goods or services provided to customers or cause them harm.
- *Materiality criteria.* These are events that exceed loss or materiality thresholds.
- *Stability criteria.* These are events that could negatively impact the financial system or ability to continue operations.

Transparency with regulators is the best policy, although there is an inherent conflict between the need to comply with regulations and the negative effects of disclosing operational risk failures.

Firm annual reports should include not only financial risk reporting, but also operational risk reporting. There is, again, a balance between transparency/honesty and creating excess stakeholder concern. Perception is positive when firms are transparent about risk and are competent in addressing risk.

Operational resilience and operational risk reporting will soon be aligned to meet regulator and market expectations. Regulated financial firms in the United Kingdom have until March 2025 to establish mapping and testing processes so that they can be within impact tolerances for significant business services, make adjustments and investments as needed, and be able to report on them.



MODULE QUIZ 40.4

1. Significant operational risk event triggers can be categorized under all of the following criteria except:
 - A. stability.
 - B. materiality.
 - C. functional.
 - D. reputation.
2. To meet operational risk disclosure requirements, the number of years of historical aggregate operational losses that must be disclosed is closest to:
 - A. 3 years.
 - B. 5 years.
 - C. 10 years.
 - D. 15 years.

KEY CONCEPTS

LO 40.a

Risk monitoring provides organizational leaders with a view of the organization risk profile, assurance of operating within risk appetite limits, and the tools to evaluate the effectiveness of the risk management framework.

Internal audiences for operational risk reporting include the following:

- The board of directors risk committee, charged with monitoring the firm's risk management framework
- The board of directors audit committee, responsible for third-level oversight of an organization, directly managed by the internal audit function

- The board of directors executive committee (ExCo), which serves as the steering committee for the overall board
- The central operational risk function and operational risk committee, which serves as the second line of oversight by collecting and aggregating information for reporting to both the risk committee and individual business line managers
- Business line managers and risk champions, who are most directly responsible for day-to-day monitoring of operational risk data

Risk report size is a challenge, as well as ensuring that the right audience receives the appropriate reports.

LO 40.b

The three tiers of the “reporting cake” are as follows:

- Tier 1 (bottom layer): The metrics presented represent a full set, and monitoring is performed daily by business line managers and risk champions.
- Tier 2 (middle layer): The recipients of the information are the operational risk committee, and the only information provided is that which requires action. Non-action items can be presented in summary form on a monthly or quarterly basis.
- Tier 3 (top layer): The recipients of the information are the executive and board risk committee. The data presented is high level.

A comprehensive internal operational risk management (ORM) report contains the following components: (1) prioritized risks (usually a top 10 list) and outlook, (2) heatmap and risk register, (3) risk appetite metrics, (4) key risk indicators (KRIs) and issue monitoring, (5) risk events and near misses, (6) action plans and remediation, and (7) emerging risks and horizon scanning.

Governance, risk, and compliance (GRC) systems are risk software applications that help organizations collect and report on operational risk data.

LO 40.c

Regarding monitoring and reporting activities, three analytical considerations that apply are (1) the cost of collecting the information must be less than the value of that information; (2) the information should be useful, and the content should align with entity objectives and priorities; and (3) reporting should influence decision-making (even if the decision is to make no changes).

Other challenges related to operational risk reporting include the following:

- Operational risk event data asymmetry: Operational losses tend to be heavily skewed away from the mean such that there are a small number of high-severity, but low-frequency events.
- Large risk event escalation: Upper management needs to review and act on large risk events and on near misses that are significant enough to be above the organization's risk tolerance.
- Small, frequent losses: Although they have low impact to the budget, these losses should be regularly analyzed to determine if there are any structural flaws or control breaches that merit action.

- Operational loss benchmarking: Using benchmarks when reporting operational risk losses can help management decide on capital allocations and operational risk budgets.
- Operational risk distributions: These distributions do not follow symmetric, bell curve patterns, which makes averages misleading. Median and quartiles are preferable.
- Concentrations, outliers, and scenarios: Past patterns, distribution concentrations, and distances between observations all merit significant analysis. Loss profiles need to be analyzed through the assessment of high-, medium-, and low-risk scenarios.
- Qualitative risk data aggregation: Qualitative risk data must be aggregated for operational risk reporting purposes. Options for aggregating qualitative data include (1) conversion and addition, (2) categorization, and (3) worst-case reporting.

The goal of combined assurance is to align assurance processes among all providers (including internal audit) to inform senior management and the audit committee about governance, controls, and risk management. Combined assurance requires significant coordination and collaboration among the three lines of defense in an entity.

LO 40.d

The Basel regulatory framework (Pillar 3) addresses public disclosure of financial and operational risk information. The three types of operational risk disclosure requirements include the following:

- Qualitative information
- Historical losses, which includes 10 years of aggregate operational losses
- Business indicator and subcomponents, which form the primary part of calculations for operational risk capital

Auditors and regulators require proof regarding controls and risk, which comes from reports and documentation like committee meeting minutes.

Financial institutions in most areas are required to inform regulators about breaches of conduct and significant operational risk events triggered by the following criteria:

- Reputation criteria: events that could have a significant impact on firm reputation
- Resilience criteria: events that could negatively impact goods/services provided to customers or cause them harm
- Materiality criteria: events that exceed loss or materiality thresholds
- Stability criteria: events that could negatively impact the financial system or ability to continue operations

In meeting reporting requirements for Pillar 3, for annual reports, and for specific reports on operational resilience and risk management, transparency with regulators is the best policy even though there is an inherent conflict between the need to comply with regulations and the negative effects of disclosing operational risk failures.

ANSWER KEY FOR MODULE QUIZZES

Module Quiz 40.1

1. **D** The executive committee is tasked with overseeing the execution of the operational risk management framework, prioritizing issues, ensuring strong entity-wide governance, overseeing board policies, and facilitating decision-making. The audit committee is the third line of risk oversight. The risk committee monitors all risk types, not just operational. Because there is often overlap in these functions, a committee member may serve on multiple committees (including audit and risk committees). (LO 40.a)
2. **C** Business line managers are the closest level of operational risk management, and they will focus heavily on KRIs. (LO 40.a)

Module Quiz 40.2

1. **C** The top layer of the reporting cake is Tier 3, which is the information that is presented to the executive and board risk committee. The data is high level and includes information such as performance trends, leading indicators, and strategic plan progress. Tier 1 is the bottom layer, which represents a full set of data going to business line managers and risk champions. Tier 2 is the middle layer, and information presented there goes to the operational risk committee. The data in Tier 2 is not high level, as it often requires action. There is no Tier 4 described in the reporting cake. (LO 40.b)
2. **B** A prioritized risk presentation will include (for each identified risk) a ranking, description, inherent components, residual components, and the outlook. Although it is unlikely that a risk can be totally eliminated, even if it could be eliminated, a timeline for it is unlikely to be presented in this structure. (LO 40.b)

Module Quiz 40.3

1. **D** Operational risk distributions often have significant skewness in the tails, which does not lend itself to using averages. An average has more meaning in symmetric, bell curve-type distributions with minimal outliers, no skewness, minimal variance, and a single mode. (LO 40.c)
2. **B** Deep dives into specific types of risk is a function of the second line of defense (the central operational risk function). The second line also oversees the activities performed by the first line, not the third line. The overall assessments of risks and controls are performed by the first line, and internal audit reviews are performed by the third line. (LO 40.c)

Module Quiz 40.4

1. **C** The four criteria are reputation, resilience, materiality, and stability. There is no category in this context called *functional*. (LO 40.d)
2. **C** The requirement to report aggregate operational loss data is 10 years. (LO 40.d)

¹ Chapelle, Ariane. "Have Your Cake and Eat It," *Operational Risk & Regulation* (October 2015).

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 7.

READING 41

INTEGRATED RISK MANAGEMENT

Study Session 7

EXAM FOCUS

The enterprise risk management (ERM) framework serves as the foundation for integrated risk management. For the exam, understand how governance, culture, and appetite fit within the ERM framework. Regulatory and economic capital, along with measures such as risk-adjusted return on capital (RAROC) and aggregate versus individual capital requirements, are critical for managing risk. Stress testing allows institutions to incorporate worst-case scenario modeling into their forecasts to ensure they are able to remain financially and operationally resilient in times of economic distress. Finally, be familiar with the different models used for operational risk stress testing, understanding that there are nuances to each type of model that present challenges for risk analysis.

MODULE 41.1: ENTERPRISE RISK MANAGEMENT (ERM)

Introduction to ERM

LO 41.a: Describe the role of risk governance, risk appetite, and risk culture in the context of an enterprise risk management (ERM) framework.

The **enterprise risk management (ERM) framework** includes the tools and methods that an organization uses to manage the different types of risks that can impact the achievement of business goals and objectives. In the financial industry, the risk management cycle includes four stages: (1) identification, (2) assessment, (3) mitigation, and (4) reporting/monitoring. Because risks and exposures change, risks must be managed continuously.

Risk governance, risk culture, and risk appetite apply to all aspects of organizational and financial risk across all organizations. In the financial industry, risk capital and stress testing represent a fourth element. Regulatory capital represents the minimum level of long-term stable funding and equity required for banks and insurance companies. Capital requirements are needed to protect against operational, credit, and market risk. Beyond minimum requirements, individual banks have their own

thresholds for the capital they need to protect against unexpected losses, to maintain credit ratings, and to ensure stability and solvency. Banks must ensure that they are both financially and operationally resilient.

Structure of ERM

ERM and related priorities are guided by risk governance, risk culture, and risk appetite. *Governance* sets the roles and responsibilities associated with an entity's three lines of defense and establishes the committees responsible for reporting and decision-making. *Culture* relates to the behaviors and values associated with managing risk. *Appetite* helps firms define priorities and the levels of risk exposure they are willing to tolerate.

Risk Governance

Roles and responsibilities are established for each of the three lines of defense within an organization:

- **First line of defense.** This is represented by business line staff and management. These individuals have primary decision-making authority, accountability, and responsibility for managing risk. Designated risk owners are tasked with identifying, measuring, mitigating, and reporting on their respective risks and must manage the balance between risks and rewards.
- **Second line of defense.** This provides oversight for the risk management activities of the business line staff, management, and risk owners. Responsibilities include measuring risk types; establishing risk tools, methods, and models; and overseeing the risk management process throughout the organization. Continuous monitoring is needed at this level to ensure the effectiveness of the ERM framework. For banks, this second line includes the operational, market, and credit risk management departments. Compliance, legal, and IT oversight may also be in this line.
- **Third line of defense.** Independent third parties and internal auditors will conduct reviews as part of this line of defense. These entities report independently to the board of directors and must evaluate the effectiveness and design of risk management activities.

An external audit is often seen as adding a *fourth line of defense*, while the Risk Committee is tasked with overseeing all risks across an entity.

Risk Culture

Risk culture and corporate culture are often used interchangeably and include the values, behaviors, and beliefs of executives, senior leadership, and employees. Inevitably, corporate culture impacts the preferences and attitudes of risk management.

A 2013 Journal of Finance paper on U.S. bank holding companies (BHCs) during the 2007–2009 financial crisis showcased the linkages between risk culture, resilience, and risk management. Using a risk management index (RMI) to measure the independence and strength of risk management functions, banks with higher precrisis RMIs outperformed banks with lower precrisis RMIs in the areas of operational performance, stock performance, loan performance, and tail risk.

These findings speak to the importance of risk culture as a driver of ERM effectiveness and the linkages of governance and culture to financial and nonfinancial risk tolerance and appetite.

Risk Appetite

An organization's risk appetite will dictate how much risk they are willing to take to achieve their desired objectives. Credit risk, market risk, liquidity risk, and operational risk (and their associated premiums) are all risks that banks and other financial industry participants take in pursuit of their objectives.

Banks have credit risk policies that cover maximum loan amounts, minimum ratings for borrowers, acceptable financial ratios, collateral requirements, monitoring metrics, and what constitutes a “watch list” loan. Market risk policies cover exposure limits, trading limits, and metrics monitoring.

Overarching criteria and statements are used by entities to express their risk appetites. Examples include the following:

- *Customer service.* All negative feedback from customers merits a direct response to each impacted customer.
- *Ethics.* Any fraud or misconduct must be addressed immediately with a defined timeline and resolutions acceptable to impacted parties.
- *Available capital (overcapitalization).* This should be at least 50% above regulatory capital requirements at all times.

Capital Elements of the ERM Framework

LO 41.b: Summarize the role of Basel regulatory capital and the process of determining internal economic capital.

Protection against unexpected losses across all risk types by remaining solvent and sustainable is another key goal of ERM. Key elements of an ERM framework include regulatory capital, economic capital, risk-adjusted return on capital, and capital aggregation/diversification.

Regulatory Capital

The guidance for the supervision and regulation of banks comes from the Basel Committee on Banking Supervision (BCBS). The objectives of regulating the financial industry include ensuring intermediary solvency and soundness, providing protection to customers, and promoting the competitiveness and efficient performance of financial institutions. The first objective is the most important and is addressed through regulatory capital requirements.

Basel I (1988) recommended a minimum capital level for covering unexpected credit losses of 8% of risk-weighted assets (RWA)—known as the **Cooke ratio**. Even with regulatory capital extended to market risk in 1996, Basel II kept the RWA level at 8%. This level, again, remained the same even as Basel II added regulatory capital for

operational risk and refinements to credit risk capital calculations in 2002. It is important to note that Basel frameworks are recommendations, not laws.

Basel III brought the addition of minimum regulatory ratios for liquidity risk and an incremental 2.5% of RWA capital requirements for banks. The latter is in place so that banks can add more capital during strong periods to protect against the negative impacts from market crises or recessions.

The Basel regulatory framework has three associated pillars:

- **Pillar 1: regulatory capital.** This includes minimum capital levels required to cover market, credit, and operational risks, as well as a minimum liquidity ratio.
- **Pillar 2: supervisory review process.** This includes adjustments to Pillar 1 requirements based on factors unique to each institution.
- **Pillar 3: market discipline.** This relates to mandatory information disclosures by financial institutions concerning risk information and financial situations.

Economic Capital

Although minimum regulatory capital requirements set a baseline, each individual financial institution must determine the appropriate level of capital needed to meet their risk profile and to cover unexpected losses. The combination of Pillar 1 and Pillar 2 requirements most accurately reflects economic capital, which represents the level of funds a bank/insurance company needs to cover any unexpected losses.

Credit rating plays a big role in economic capital, as a larger amount of capital provides more protection against unexpected losses and will support a higher credit rating. Higher ratings translate to lower borrowing costs. For example, if firms with AAA ratings (the highest rating) have a default probability of 0.01%, a target rating of AAA implies that a bank will ensure its economic capital will cover unexpected losses at a confidence level of 99.99% ($= 100\% - 0.01\%$).

Risk-Adjusted Return on Capital

Risk-adjusted return on capital (RAROC) is a risk-adjusted version of return on equity (ROE). It is calculated by taking expected after-tax risk-adjusted net income and dividing it by economic capital. The numerator adjusts net income for expected losses (EL) generated by activity-related risks. The application of RAROC is easier with credit risks than market risks because credit risks have underlying historical data to reference. EL are often set to zero for market risks, and RAROC is often not used for operational risks.

RAROC is useful in quantifying funding costs, managing capital, and aligning activities with objectives. RAROC calculations offer considerable flexibility, as revenues and EL may be estimated at a business line, portfolio, client, or even transaction level. Economic capital represents the amount of capital earmarked for specific activities. Managers are able to price transactions based on the minimum requirements for RAROC at these various levels.

Capital Assessment Risk Aggregation

Capital needs for each risk class must be aggregated, accounting for the fact that not all risks are prevalent at the exact same time. **Inter-risk diversification** aggregates risks across the different risk classes (market, credit, and operational), while **intra-risk diversification** covers risks within each class. Because each risk class is unique, total aggregated capital will be less than the sum of each individual risk's stand-alone capital. Operational risk, which often exists independent of market and credit risk, provides a significant diversification benefit due to its low correlation with other financial risks.



MODULE QUIZ 41.1

1. Sovereign Bank has an internal audit department, but the bank CEO hires an external auditor to review their financial statements and assess their internal control system. The audit firm is most likely considered to be which line of defense?
 - A. First.
 - B. Second.
 - C. Third.
 - D. Fourth.
2. Which of the following statements about the risk-adjusted return on capital (RAROC) measure is most accurate?
 - A. The numerator utilizes pretax, risk-adjusted income.
 - B. Regulatory capital is the denominator of the calculation.
 - C. Expected losses (EL) are typically set at zero for credit risks.
 - D. RAROC is applied more often to credit risks than to operational risks.
3. Assume that a credit rating of A has a default probability of 0.07%, and a credit rating of AA has a default probability of 0.04%. If a bank is seeking a target rating of A, it will want to ensure that its economic capital will cover unexpected losses at a confidence level of:
 - A. 93.00%.
 - B. 96.00%.
 - C. 99.93%.
 - D. 99.96%.

MODULE 41.2: STRESS TESTING

Fundamentals of Stress Testing

LO 41.c: Describe elements of a stress-testing framework for financial institutions and explain best practices for stress testing.

Stress testing is used to assess the stability of an entity or system. Testing involves stretching a system to its breaking point, or at the very least, beyond its normal operational capacity. After the financial crisis of 2007–2009, stress tests were deployed to test how entities would perform under extreme market and macroeconomic conditions. The key to successful stress tests was ensuring that an entity could absorb losses in these extreme situations and still be able to function moving forward.

Stress testing is viewed by the Basel Committee as a very important risk management tool as it helps institutions understand the appropriate level of capital needed to absorb losses in extreme market conditions. The stress testing principles shown in Figure 41.1 were published by the BCBS in 2018.¹

Figure 41.1: Stress Testing Framework Principles

1. Frameworks need clearly articulated and formally adopted objectives.
2. Frameworks should have an effective governance structure.
3. Testing should be used as a tool for risk management and to inform business decisions.
4. Frameworks should capture relevant and material risks and apply appropriately severe stresses.
5. Organizational structures and resources should be appropriate for meeting framework objectives.
6. Robust IT systems and granular data are needed to support stress tests.
7. Methodologies and models must be appropriate to assess sensitivity and scenario impacts.
8. Frameworks, models, and results should be regularly reviewed and challenged.
9. Findings and practices should be communicated across and within jurisdictions.

Before the financial crisis of 2007–2009, stress testing emphasized quantitative measures. The crisis called to attention weaknesses such as methodologies, scenario selection, testing integration with risk governance, and testing specific risks and products. Now, stress testing incorporates both qualitative and quantitative elements.

Taxonomy

The taxonomy for stress testing relies on two dimensions, which are (1) the analytical approach and (2) the types of risk captured:

- *Dimension 1: quantitative-qualitative approach.* This dimension covers a range of highly qualitative to highly quantitative methodologies. More qualitative methodologies use scenario analysis, like macro stress testing and reverse stress testing. Modeling the impact of a crisis on a bank's reputation is an example. More quantitative approaches include stress testing the sensitivity of models to parameter shocks.
- *Dimension 2: measurable-immeasurable risks.* The analysis spectrum here covers fact-based probabilistic analysis for measurable risks to possibilistic analysis for immeasurable risks:
 - With **measurable risks**, included here are analytical methods that tie probabilities to outcomes. For market and credit risk, stress testing often involves modifying model parameter values. For operational risk, tail risk modeling may also incorporate parameter stress testing.
 - With **immeasurable risks**, included here are analytical methods used to assess risks considered *unknown unknowns*. These risks cannot be calculated or estimated, which is referred to as *Knightian uncertainty*.

Stress Testing Approaches

The three different classifications of stress testing approaches include (1) parameter testing, (2) macroeconomic testing, and (3) reverse testing:

- **Parameter (model) stress testing.** This form of stress testing changes parameter values to test model robustness. Quantitative approaches and the analysis of

measurable risks are used under this testing approach. Banks often use this form of testing to determine the impact of additional stress on the bank overall, on specific portfolios, or on specific models. Outside of formal stress testing, banks also use this approach to estimate the impact of shocks for strategic or business planning purposes.

- **Macroeconomic (macro) stress testing.** Major bank jurisdiction regulators provide an annual list of macroeconomic shock scenarios (e.g., large swings in GDP, the unemployment rate, inflation) that banks can use to evaluate solvency and financial resilience. This form of testing is holistic in that it incorporates quantitative and qualitative approaches, as well as stressing both measurable and immeasurable risks. The focus of the testing is on how model outputs are impacted by changes in macroeconomic factors.
- **Reverse stress testing.** This form of scenario-driven stress testing looks to analyze immeasurable risks using mostly qualitative approaches. The starting point is a specific outcome resulting from an institution failure, and from there, the bank will identify what circumstances may lead to this outcome. Examples of shocks include major client losses, major portfolio losses, credit rating downgrades, and the loss of major revenue sources. Operational resilience assessments are a key focal point for reverse stress testing, as banks must use testing results to determine which mitigating controls they need to put in place.

Resolution planning involves planning for the closure of an institution with minimal impacts to the financial system and institutional stakeholders. Events that could lead to this closure must be identified through a review of the business model, exposures, and vulnerabilities. Resource needs must also be assessed.

Stress Testing Operational Risk

LO 41.d: Explain challenges and considerations when developing and implementing models used in stress testing operational risk.

Both the 2007–2009 financial crisis and the COVID-19 pandemic had significant impacts on how institutions conduct stress testing. While the loss distribution approach (LDA) was in place for operational risks as part of Basel II, current operational risk stress testing incorporates both parameter testing and macroeconomic testing to understand how risk changes due to changing macroeconomic conditions.

Robust operational risk stress testing is needed for forecasting impacts from several macroeconomic scenarios, with scenario analysis, LDA forecasting, and regression all incorporated into quantitative approaches.

The **Comprehensive Capital Analysis and Review (CCAR)**, the U.S. Federal Reserve stress testing program, serves as the benchmark program for operational risk stress testing expectations. An institution's risk identification process should align with its operational risk capital planning process. Over time, forecasts have been driven less by quantitative modeling and more by expert judgment and scenario analysis.

The three components (modules) of a comprehensive operational risk stress testing framework include the following:

- *Expected nonlegal loss forecast module.* This is a quantitative model estimating a loss forecast for every risk type and expert judgment refinements. The two subcomponents of this module are the quantitative model output and expert refinement. The outputs of the quantitative model should be loss forecasts for each risk type under baseline and adverse macroeconomic scenarios. Expert refinement involves incorporating industry, controls, and entity-specific risk knowledge from subject-matter experts.
- *Legal loss module.* This is a model that forecasts losses for immaterial litigation cases, losses above a threshold for current cases, and future litigation cases. Litigation losses represent a significant share of operational risk losses for most banks but should be broken out separately from other operational losses. A challenge with this module is the delay between macroeconomic events and the incurrence of legal losses by an institution. Forecasts should consider this inevitable lag time.
- *Idiosyncratic scenario add-on module.* This captures risk exposures unique to each individual bank based on storylines like extreme event scenarios. The storylines used to develop this module, which are based on the most material risks, should be unique and tied to the vulnerabilities of each individual bank.

There is still considerable debate as to whether operational risk is independent of macroeconomic factors and events. However, institutions are being driven by regulatory pressures to link operational risk and macroeconomic conditions.

Operational Risk Stress Testing Models

Banks can model either total operational risk losses or the individual loss components (i.e., frequency and severity). The preferred approach is to model frequency and severity separately. For these individual components, regression models are used to capture the dependency between macroeconomic conditions and operational losses. A secondary approach is to use the **loss distribution approach (LDA)**, where Monte Carlo simulations are used to project losses. A modified or conditional LDA can be used to model loss frequency based on macroeconomic variables. LDA is a secondary approach because it assumes institutional risk exposures are unchanged over time.

A conditional LDA provides a trade-off between a full regression-based stress test and a simple LDA. Frequency is modeled using regression, while severity is kept constant, and expert judgment is used to reflect firm expectations of average losses. These losses are combined with Monte Carlo simulations using forecasted frequencies. The percentile used for the severity is a significant challenge for a conditional LDA. Setting it at the 99.9th percentile (like what is used for regulatory capital purposes) would be too high and will result in perpetual undercapitalization projections. Fortunately, regulators do not impose percentile requirements with stress testing.

As mentioned, modeling severity presents a greater challenge than monitoring frequency. Models can assume that both severity and frequency have relationships with macroeconomic factors. Because loss severity is usually heavily impacted by tail events, a bank is limited in its ability to use severity mean data as an estimator. Using median loss data may be a better approach.

Financial institutions may use regression analyses that incorporate macroeconomic variables to analyze average loss severity. Macroeconomic and other variables may be used in both simple linear regression models and log-linear models. Model outputs will include estimates of stressed losses that will require expert refinement using scenario analysis to ensure that material risks have been appropriately captured by the model.

The model refinement element involves the specialist and risk owner reviewing and challenging the following:

1. The process used for the model-based, nonlegal loss forecast
2. Model inputs and outputs
3. Historical data used in the model
4. Approaches selected
5. Support for the macrodrivers chosen
6. Plausibility estimates for losses (frequency, severity, and total) for each risk type

Experts must also address any new or potential changes to conditions that could impact future operational risk loss expectations and how they may differ from historical loss results.



MODULE QUIZ 41.2

1. The loss of a major client, downgrades in credit ratings, and significant portfolio losses are examples of shocks used as the starting point for which type of stress testing?
 - A. Model stress testing.
 - B. Reverse stress testing.
 - C. Parameter stress testing.
 - D. Macroeconomic stress testing.
2. A significant challenge in estimating the legal loss module of an operational risk stress test is that:
 - A. future litigation cases cannot be estimated.
 - B. banks are minimally impacted by legal losses.
 - C. operational risks and legal losses cannot be separated.
 - D. there is a lag between the macroeconomic event itself and the incurrence of legal losses.
3. Risks that are only applicable to each unique bank are best captured using which module in a comprehensive operational risk stress testing framework?
 - A. Legal loss.
 - B. Individual risk loss.
 - C. Idiosyncratic scenario add-on.
 - D. Expected nonlegal loss forecast.

KEY CONCEPTS

LO 41.a

The enterprise risk management (ERM) framework includes the tools and methods that an organization uses to manage all types of risks that can impact the achievement of goals and objectives.

Risk governance, risk culture, and risk appetite apply to all aspects of organizational and financial risk across all organizations. In the financial industry, risk capital and

stress testing represent a fourth element. Regulatory capital represents the minimum level of long-term stable funding and equity required for banks and insurance companies.

ERM and related priorities are guided by governance, culture, and appetite. Governance sets the roles and responsibilities associated with an entity's three lines of defense and establishes the committees responsible for reporting and decision-making. Culture relates to the behaviors and values associated with managing risk. Appetite helps firms define priorities and the levels of risk exposure they are willing to tolerate.

The first line of defense is the business line staff and management. The second line of defense provides oversight for the risk management activities of the business line staff, management, and risk owners. The third line of defense includes independent third parties and internal auditors. An external audit is often seen as adding a fourth line of defense, while the Risk Committee is tasked with overseeing all risks across an entity.

LO 41.b

Key elements of an ERM framework include regulatory capital, economic capital, risk-adjusted return on capital, and capital aggregation/diversification. The objectives of regulating the financial industry include ensuring intermediary solvency and soundness (addressed through regulatory capital requirements), providing protection to customers, and promoting the competitiveness and efficient performance of financial institutions.

The Basel regulatory framework has three associated pillars:

- Pillar 1: regulatory capital. This includes minimum capital levels required to cover market, credit, and operational risks, as well as a minimum liquidity ratio.
- Pillar 2: supervisory review process. This includes adjustments to Pillar 1 requirements based on factors unique to each institution.
- Pillar 3: market discipline. This relates to mandatory information disclosures by financial institutions concerning risk information and financial situations.

The combination of Pillar 1 and Pillar 2 requirements most accurately reflects economic capital, which represents the level of funds a bank/insurance company needs to cover any unexpected losses.

RAROC is a risk-adjusted version of return on equity (ROE) and is calculated by taking expected after-tax risk-adjusted net income divided by economic capital. RAROC is useful in quantifying funding costs, managing capital, and aligning activities with objectives.

Capital needs for each risk class must be aggregated, accounting for the fact that not all risks are prevalent at the exact same time. Because each risk class is unique, total aggregated capital will be less than the sum of each individual risk's stand-alone capital. Operational risk provides a significant diversification benefit due to its low correlation with other financial risks.

LO 41.c

Stress testing is used to assess the stability of an entity or system. Testing involves stretching a system beyond its normal operational capacity and potentially to its breaking point. Stress testing incorporates both qualitative and quantitative elements.

The taxonomy for stress testing relies on two dimensions: (1) the analytical approach and (2) the types of risk captured. Dimension 1 is the quantitative-qualitative approach, and Dimension 2 covers measurable-immeasurable risks.

The three different classifications of stress testing approaches include (1) parameter testing, (2) macroeconomic testing, and (3) reverse testing. Parameter (model) stress testing changes parameter values to test model robustness. Macroeconomic stress testing incorporates macroeconomic shock scenarios that banks can use to evaluate solvency and financial resilience. Reverse stress testing starts with a specific outcome resulting from an institution failure and evaluates the circumstances that may lead to this outcome.

LO 41.d

Current operational risk stress testing incorporates both parameter (model) testing and macroeconomic (macro) testing to understand how risk changes due to changing macroeconomic conditions.

The three components (modules) of a comprehensive operational risk stress testing framework include: (1) the expected nonlegal loss forecast module, (2) the legal loss module, and (3) the idiosyncratic scenario add-on module.

To model frequency and severity, regression models are used to capture the dependency between macroeconomic conditions and operational losses. A secondary approach is to use the loss distribution approach (LDA), where Monte Carlo simulations are used to project losses. A modified or conditional LDA can be used to model loss frequency based on macroeconomic variables. A conditional LDA provides a trade-off between a full regression-based stress test and a simple LDA. Modeling severity presents a greater challenge than monitoring frequency.

ANSWER KEY FOR MODULE QUIZZES

Module Quiz 41.1

1. **D** The external audit firm is considered the fourth line of defense, as the first line of defense is the business line staff and management, the second line of defense provides oversight for the first line, and the internal audit department will be the third line of defense. (LO 41.a)
2. **D** The RAROC measure is most often applied to credit risks, while it is typically not used for operational risks. The numerator uses after-tax risk-adjusted income, while the denominator is economic capital. Expected losses are typically set at zero for market risks, not credit risks. (LO 41.b)
3. **C** With a default probability of 0.07% for an A credit rating, the bank will want to ensure that its economic capital will cover unexpected losses at a confidence interval of 99.93% ($= 100\% - 0.07\%$). (LO 41.b)

Module Quiz 41.2

1. **B** Reverse stress testing is a form of scenario-driven stress testing that is used to analyze immeasurable risks using mostly qualitative approaches. The starting point is a specific outcome (shocks like major client losses and credit rating

downgrades) resulting from an institution failure, which is followed by an assessment of what circumstances may lead to this outcome. (LO 41.c)

2. **D** Inevitably, there is significant lag time between when a macroeconomic event occurs and when the bank or financial institution actually incurs legal losses. This lag time should be accounted for in the model. Future litigation cases can be estimated, banks are certainly impacted by legal losses, and legal losses can be separated out from other operational risks. (LO 41.d)
3. **C** The idiosyncratic scenario add-on module captures risk exposures unique to each individual bank (based on extreme event scenarios). While the legal loss and expected nonlegal loss forecasts are both actual modules, the individual risk loss module is not the name of a module that exists in this framework. (LO 41.d)

¹ "Basel Committee on Banking Supervision Stress Testing Principles," 2018.
<https://www.bis.org/bcbs/publ/d450.pdf>

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 assigned reading—Basel Committee on Banking Supervision.

READING 42

CYBER-RESILIENCE: RANGE OF PRACTICES

Study Session 8

EXAM FOCUS

This reading gives an overview of the different cyber-resilience practices in global jurisdictions and institutions' threat preparedness. It also looks at jurisdictional approaches to cyber-resilience guidance standards, and assessments of the varying governance and cyber-resilience practices, as well as testing and incident response and recovery approaches. For the exam, pay attention to the various types of practices for the sharing of cybersecurity information between different types of institutions, and the range of practices for risk governance of third-party service providers.

MODULE 42.1: CYBER RISKS, GOVERNANCE, AND SUPERVISION

Increasing automation and connectedness with third-party service providers exposes institutions to a growing risk of cyberattacks and cyber threats. In response to the frequency and severity of threats, national and international regulators enacted a number of supervisory and legislative changes. In December 2018, the Basel Committee on Banking Supervision published a report with the aim to identify, describe, and compare various cyber practices across banks and regulatory and supervisory bodies.

Cyber-Resilience Standards and Guidelines

LO 42.a: Define cyber resilience and compare recent regulatory initiatives in the area of cyber resilience.

Cybersecurity and cyber-resilience in most jurisdictions is addressed through information technology (IT) and operational risk standards. The goal of the standards is to encourage good governance and risk management, and to address IT recovery and outsourcing. Even when the standards focus primarily on business continuity planning and outsourcing, they could have relevance to cyber risks.

Several jurisdictions have specific guidance on cyber risk management, including in Hong Kong, Singapore, Brazil, and the European Union (EU) (through the European Banking Authority). For example, guidance in Hong Kong focuses on effective cybersecurity risk management; guidance in Singapore focuses on detecting cyberattacks; guidance in Brazil focuses on establishing cybersecurity policies; while guidance in the EU concentrates on establishing common procedures and methodologies. In Australia, the objectives of the standards by the Australian Prudential Regulation Authority (APRA) is to minimize the likelihood of incidents by requiring entities to clearly define roles and responsibilities, maintain adequate information security capability, and implement and test controls. In Germany, the Banking Supervisory Requirements for IT (BAIT) covers IT strategy and governance, information risk and security management, user access agreements, and IT project management, among others.

Other jurisdictions may not have specific cyber-related standards. Entities in these jurisdictions are encouraged to adopt and implement international standards.

Cyber-Governance

LO 42.b: Describe current practices by banks and supervisors in the governance of a cyber-risk-management framework, including roles and responsibilities.

Regulators issue either prescriptive regulations or principles-based guidance. While guidance may not directly address cyber risk standards and supervisory practices, they address broader enterprise IT risk management. The five areas of cyber-related governance include:

1. Cybersecurity strategy.
2. Management roles and responsibilities.
3. Awareness.
4. Architecture and standards.
5. Workforce.

Cybersecurity Strategy

Regulators require covered entities to establish broader information security strategy and policies, even if they don't directly require the development of a cybersecurity strategy. Jurisdictions like Australia, Brazil, and parts of Europe require entities to have a broader risk management and information security framework that covers cyber risk, and this framework should be reviewed and monitored by senior management.

As a result, supervisors generally review a regulated entity's information security strategies but do not require stand-alone cybersecurity initiatives. For example, neither United States nor Mexican regulations specifically focus on the development of cybersecurity strategies. On the other hand, Canadian guidance focuses on whether financial institutions have established cybersecurity strategies and their alignment with the institutions' overall business strategy.

In general, there are three approaches to cybersecurity strategy:

1. Regulators establish sector-specific or cross-sectoral cybersecurity requirements. This is common in emerging markets with homogenous banking systems.
2. A regulated entity (e.g., a financial institution) establishes its own cybersecurity strategy, which is then reviewed by regulators as part of the entity's broader risk management practices.
3. Regulators review whether financial institutions have appropriate IT strategies that cover cyber risk. This is common in Europe.

Management Roles and Responsibilities

The majority of jurisdictions recognize the importance of the board of directors and senior management in addressing either specific cyber risk strategies, or cyber risk as part of broader enterprise risk management strategies. The United States, EU, and Japan encourage banks to implement clear and well-defined risk management frameworks through initiatives of the board. European regulations under the European Banking Authority (EBA) also cover more granular requirements on cyber risk.

Regulatory standards often include the *three lines of defense* risk management model for cyber risk, but have not required institutions to adopt this model. Rather, regulators expect that institutions are able to clearly define the different lines' responsibilities themselves. However, since regulatory supervision tends to focus on the first and second line of defense, this could reduce the effectiveness of the model. Only few jurisdictions have guidance around the independent reporting of the chief audit executive and the audit committee.



PROFESSOR'S NOTE

In general, the three lines of defense are: (1) front office that owns and manages risk, (2) compliance and chief risk officer that oversee risk management, and (3) independent risk assurance, namely internal and external audits.

Awareness

It is critical that staff at all levels of an organization are aware of cyber risk. Management and the board are responsible for ensuring proper training for employees and cybersecurity awareness. Regulators often encourage regulated entities to develop a common risk culture that improves the effectiveness of cyber risk management. Regulators may also require entities to set up proper screening and background checks for new employees and to have new employees sign nondisclosure agreements to safeguard against cyber risk. Risk management for existing employees could include a periodic reverification process.

Architecture and Standards

There are no consistent regulatory standards requiring that cyber architecture and guidelines are in place, and only a few countries have specific controls around cybersecurity architecture. U.S. regulations require supervisors to ensure content is current and properly stored, while Saudi Arabia requires entities to have periodic self-assessments around cybersecurity.

Workforce

Cyber workforces differ greatly in the level of their skills and competencies. Standards often focus on training of the IT workforce to manage risks, with less focus specifically on cybersecurity. Supervisory practices include assessing team responsibilities, employee expertise, security checks, and training.

Regulators tend to assess the effectiveness of the cybersecurity workforce through on-site inspections, which may include a review of the training process, or of the qualifications of employees or the head of IT or risk. Regulations that explicitly address the roles and responsibilities of IT staff can be found in Argentina, Australia, the EU, Japan, and Saudi Arabia. Switzerland has regulations that are embedded in the global governance framework. Regulations in the United States and Mexico typically focus on the requirements of the board and senior management.

Jurisdictions which explicitly have guidelines around cybersecurity include South Africa (as part of its national cybersecurity strategy), Japan and South Korea (on cybersecurity workforce management), and Hong Kong, Singapore, and the United Kingdom (on certification of cyber workforce skills and competencies).

Approaches to Cyber Risk Management and Incident Response and Recovery

LO 42.c: Explain methods for supervising cyber resilience, testing and incident response approaches, and cybersecurity and resilience metrics.

The four areas of cyber risk management and incident response and recovery are:

1. Supervision of cyber-resilience.
2. Information security controls.
3. Incident response and recovery.
4. Cybersecurity and resilience metrics.

Supervision of Cyber-Resilience

Jurisdictions differ in their approach to supervision, but primarily focus on the complexity and business model of key risks, including cyber risk. Cybersecurity reviews by regulatory authorities can be triggered by institutions' own risk assessments, by findings from inspections, or by analyses of cyber incidents. In addition to incident reports, risk specialists and supervisors can also draw on survey responses, inspections, and meetings with risk personnel, although the nature and breadth of supervisory approaches varies significantly across jurisdictions. Supervisory reviews can be conducted both as part of general technology assessments, or as part of risk management assessments, with a focus on various risk controls and governance.

Jurisdictional differences also include varying types and number of regulated institutions and different sizes of specialist teams. Regulations in Australia, Brazil, and Singapore have enabled supervisors with knowledge to assess and diagnose IT risks through specific guidelines and assessments. Australia and the United Kingdom also have the ability to appoint an auditor or other third party to review cyber risk and provide a report to the regulator.

Jurisdictions also started to increasingly engage with industry to address cyber risk, influence behavior, and aid regulatory work. Approaches include conference participations, speaking engagements, and risk publications. For example, regulators in both France (Autorité de Contrôle Prudentiel et de Résolution [ACPR]) and the United Kingdom (Prudential Regulation Authority [PRA]) issued discussion papers in 2018 on IT risk and operational resiliency, respectively, while the European Commission, EU FinTech Lab, and the EBA FinTech Knowledge Hub have organized industry events.

Information Security Controls

Mapping and classification of business services and assets is done in many jurisdictions, including in the United States, EU, Australia, Hong Kong, and Singapore. This process can be done as part of business impact analysis, recovery planning, or scoping for assessments. Several jurisdictions assess the ability of institutions to detect threats in real-time including monitoring and surveillance of threats. Reviews may be thematic or using international standards. These reviews can be complemented by independent assurance (i.e., audits) on whether appropriate controls exist.

Institutions typically test security controls for both hardware and software data to detect and prevent cybersecurity incidents. Regulators then analyze survey responses and threat and vulnerability or other risk assessments by institutions, as well as audit and control testing reports. Several regulators in the EU also developed penetration tests on regulated entities, and three jurisdictions (the European Central Bank [ECB], the Netherlands, and the United Kingdom) provide guidance on how to conduct tests. For the most part, tests remain voluntarily funded by the regulated institutions themselves. Tests tend to focus on protection and detection of cyber-resilience capabilities. As a further step, the ECB published a Europe-wide framework in May 2018 that facilitates controlled testing of cross-border entities. The regulators and regulated entities together determine whether and when testing is necessary, with the goal of these tests to enable institutions to learn and to improve their cyber risk preparedness.¹

Jurisdictions may use risk taxonomies to identify gaps in controls and supervision. Currently, taxonomies are not harmonized and are instead specific to each jurisdiction.

Incident Response and Recovery

For the most part, regulators require institutions to establish a risk framework or policies for risk detection and response and recovery. Such requirements tend to focus on overall risk management and not specifically on cybersecurity, although some jurisdictions, including China and Japan, require cyber-specific frameworks within overall cyber-governance. The United States issued guidance on incident management and incident analysis, classification, escalation, and reporting. At the same time, regulations in Japan focus on analysis of potential threats and information sharing to reduce reporting delays. Other jurisdictions, for example Canada, focus on reducing contagion by assessing banks' both internal and external communications protocol and whether all necessary stakeholders are included. Supervisory reviews of learning following incidents are done in Australia, the United States, Hong Kong, Japan, and Belgium.

Banks and supervisors also use training exercises on how to respond to incidents. Many of these are joint public-private exercises, which recently included the Group of Seven (G7) and the joint U.S.-U.K. exercises. Other examples include an annual exercise regime in the United Kingdom which incorporates cyber risk scenarios, and exercises in Japan with a goal to improve response coordination and communication.

Cybersecurity and Resilience Metrics

As we previously noted, assessing cyber-resilience and security is typically done through surveys, incident reports, tests, and inspections. Methodologies to test cybersecurity do not have standardized quantitative metrics similar to assessments of financial risks; rather, regulators rely on institutions' own management information and indicators.

While indicators use backward-looking data, they are useful in predicting future performance when institutions function in a stable operating and risk environment. However, "adversaries" (individuals or groups trying to gain illegal access) continuously adopt to institutions' changing defenses. When a single system is attacked from multiple malicious sources, it gives rise to **distributed denial of service (DDOS)** incidents. As a result, institutions are increasingly recognizing the importance of forward-looking indicators to improve resilience to attacks, while more broadly improving metrics for resilience. Trend analysis is important because it allows a review of whether risks are increasing or declining.

A regulatory review of regulated entities' cyber metrics is useful in assessing the adequacy of their cyber-preparedness strategy and the level of their cyber resiliency. Analysis of survey results has been especially common, and findings can be used to create indicators and highlight trends. Regulatory findings from these surveys can be published with the goal to influence behavior (Australia) or shared directly with regulated entities (United Kingdom).



MODULE QUIZ 42.1

1. Country X's banking regulator established sector-specific cybersecurity requirements. This most likely indicates that Country X is:
 - A. an emerging economy with a homogenous banking system.
 - B. a developed economy with a homogenous banking system.
 - C. an emerging economy with a fragmented banking system.
 - D. a developed economy with a fragmented banking system.
2. Which of the following concepts is not one of the four areas of cyber risk management and incident response and recovery?
 - A. Architecture and standard.
 - B. Incident response and recovery.
 - C. Supervision of cyber-resilience.
 - D. Cybersecurity and resilience metrics.

MODULE 42.2: CYBERSECURITY INFORMATION SHARING BETWEEN INSTITUTIONS AND THIRD-PARTY RISK

Sharing Cybersecurity Information Between Institutions

LO 42.d: Explain and assess current practices for the sharing of cybersecurity information between different types of institutions.

The five types of information-sharing practices include sharing (1) among banks, (2) from banks to regulators, (3) among regulators, (4) from regulators to banks, and (5) from banks and regulators to security agencies. Sharing of cybersecurity information among market entities can be either voluntary or mandated.

The three most common sharing types are sharing among banks, sharing with security agencies, and sharing from banks to regulators. Sharing among regulators and from regulators to banks tends to be less frequent given the less systematic nature of their sharing arrangements. Information shared between banks and regulators include information related to cyber threats, specific incidents, regulatory or supervisory responses, and best practices. Banks tend to share cybersecurity incident information with regulators and cyber threat information among themselves.

In jurisdictions where information sharing among banks is well established, information sharing from regulators to banks tends to be less prevalent given that banks already have a well-functioning mechanism among each other. Likewise, in jurisdictions with established sharing of information from banks to regulators, occurrences of sharing with security agencies tend to be less common, likely given the division of responsibilities between regulators and security agents.

Some jurisdictions have a mix of both voluntary and mandatory information-sharing measures depending on the type of information shared. For example, Singapore mandates financial institutions to report cybersecurity incidents to the Monetary Authority of Singapore (MAS), however, exchange of cyber risk information between the MAS and the Cyber Security Agency (CSA) is voluntary. Information sharing can also include sharing between public and private institutions and public announcements on cyber incidents. Participants can include third-party service providers, customers, and nonbank critical infrastructure operators.

Sharing Among Banks

Banks share cyber threat information among each other to improve other banks' preparedness and responses to similar threats. While regulators are typically not involved in information exchanges, they often facilitate information sharing through establishing mechanisms to share cyber threats, incidents, or other information. Only three jurisdictions—Brazil, Japan, and Saudi Arabia—have regulations that mandate information sharing among banks. Other jurisdictions may have public/private forums or even government-led centers for information sharing. Jurisdictions may also have data protection regulations that may create obstacles and make information sharing among banks more difficult. Ultimately, sharing of cyber threat information among banks depends to a large degree on the level of trust between banks. It has been shown

that banks can build trust through a two-tier approach by sharing information with a smaller group first before widening the dialogue to a larger group of banks.

Sharing From Banks to Regulators

For the most part, banks share cybersecurity information with regulators and supervisors that has been mandated/required by regulation and is usually limited to operational incidents, including cyber incidents. Requirements are intended to (1) enable systemic risk monitoring, (2) enhance regulatory requirements or recommendations, (3) improve regulatory oversight and incident resolution, and (4) facilitate information sharing between the regulator and the industry to develop a broader cyber risk response framework.

For example, the majority of financial institutions in the EU are required to report cyber incidents to their regulatory authorities and may also be required to include an incident root-cause analysis or a postincident analysis. The supervisory framework for these regulations includes the Single Supervisory Mechanism (SSM) cyber incident reporting framework and several EU directives. Regulatory requirements and reporting frameworks vary due to differences in the type of regulatory authority, their mandates, the specific sectors, and the financial institutions' geographic scope. Most regulations focus on reporting of incidents that have already occurred, although some include requirements to proactively monitor and track potential cyber threats.

Specific differences in incident reporting include (1) the reporting taxonomy, (2) reporting time frame (how soon following an incident is reporting required; for example, after 2 hours, 4 hours, or 72 hours), (3) templates, and (4) incident reporting thresholds. Because these differences exist, the reporting system can be fragmented, and financial institutions operating in multiple jurisdictions may see increased regulatory burden which increases costs and time and could also increase the complexity of information received by regulators.

Incident reporting flow is one-directional, from banks to regulators. To help reduce the stigma of incidents and facilitate reporting, the flow of information can be relaxed to make it more reciprocal.

Sharing Among Regulators

Sharing among regulators is the least frequent flow of information exchange given the less systematic nature of their sharing arrangements. When sharing does occur, it can be among domestic regulators or with other cross-border regulators, and information shared can include regulatory actions and responses. With the increasing sophistication of cyber incidents, however, it is becoming more critical that regulators improve dialogue among themselves to increase awareness and the timeliness of regulatory guidance. A recent example of information sharing between regulators includes the 2018 bilateral agreement between the Hong Kong Monetary Authority (HKMA) and the MAS in Singapore.

Sharing From Regulators to Banks

While sharing of cybersecurity information from regulators to banks is not yet widespread, several jurisdictions have established guidance through standards and practices around sharing. Regulators first receive information from banks, which allows

them to assess the risk and then share this information with the broader public. When regulators receive sensitive information, they first make it anonymous or only share on a summary basis.

Some form of guidance exists in select jurisdictions, including in the United States, United Kingdom, China, Korea, Singapore, Australia, Saudi Arabia, and Turkey. Only China has mandatory requirements for regulators to share information with banks. Information sharing from regulators in Singapore and the United Kingdom is done on a voluntary basis. The majority of jurisdictions have no clear guidance around sharing of information with banks. However, information sharing would improve preparedness for cyber threats, could facilitate appropriate responses, and would improve trust in the regulatory system.

Sharing with Security Agencies

Communication with security agencies can have significant benefits for both banks and regulators, since it creates broader awareness and can enhance effective countermeasures for cyber threats. Security agencies like the Computer Emergency Readiness Team (CERT) can be central to notification of cybersecurity incidents and sharing of this information with various sectors in a jurisdiction, including the public and civilian sectors and the computer (or broader technology) community.

Information sharing by banks and regulators with national security agencies is primarily done on a voluntary basis, although some jurisdictions have formal mandates. Mandatory sharing exists in Canada, Singapore, and in parts of the EU including in France and Spain, where information-sharing arrangements are typically bilateral. Information is exchanged voluntarily in the United Kingdom, where a framework exists that brings together relevant agencies, including the Bank of England and the Financial Conduct Authority (FCA) to coordinate responses to cyber incidents.

Sharing platforms exist in the United States and in Luxembourg. In the United States, cybersecurity information can be submitted through an online portal to the United States CERT and the National Cybersecurity and Communications Integration Center. In Luxembourg, information can be shared with the Computer Incident Response Center which reviews and analyzes computer security threats and incidents. The aim of exchanging information with the security agencies is to improve countermeasures and cyber threat detection and response.

Risks of Third-Party Service Providers

LO 42.e: Describe practices for the governance of risks of interconnected third-party service providers.

Use of third parties increases the cyber threat risk of financial institutions, because institutions lack control and visibility over these entities. Third parties encompass outsourcing (including cloud computing), other services typically not considered outsourcing (power supply, telecommunication lines, commercial hardware, and software), and financial and nonfinancial interconnected counterparties, including

payment and settlement systems, trading platforms, central securities depositories, and central counterparties. Analysis of third parties can be broken down into:

- Governance of third-party interconnections.
- Business continuity and availability.
- Information confidentiality and integrity.
- Expectations and practices around visibility of third-party interconnections.
- Auditing and testing.
- Resources and skills.

Governance of Third-Party Interconnections

Most regulations require that institutions establish a proper framework for outsourcing that defines the roles and responsibilities, the scope of activities that can be outsourced, risk analysis, and monitoring and risk assessment. The outsourcing framework should also define the specific roles, responsibilities, and rights of both the financial institution and the service provider. The risk analysis should specify the risks covered and their mitigants. Covered risks include primarily the following risks: strategic, compliance, security (e.g., security monitoring, patch management, authentication solutions), business continuity, vendor lock-in (ability to withdraw from the service provider and absorb or transfer activity to another service provider), counterparty, and access risks. Regulators expect that these risks are adequately analyzed in third-party data, including identifying and prioritizing interconnections and classifying incident responses.

Supervisors often conduct on-site cyber risk inspections of institutions on outsourcing to analyze the completeness and adequacy of risk assessments. Supervisors also perform ongoing off-site inspections by reviewing institutions' reports and statements on outsourcing policies and risk assessments.

International standards may consider that financial institutions often rely on third-party providers even outside of traditional outsourcing arrangements. Guidance typically includes requirements to identify and address cyber risks. Jurisdictions may also require that financial institutions enter into prior agreements with clients on how to authenticate clients and manage personalized data.

In the EU, the MiFID II Directive² provides supervisory authority and regulates interactions between institutions, supervisors, and third-party providers. Regulations in the EU may also require that institutions identify the location of some of their data centers for cloud computing services. Other jurisdictions include requirements for identifying and monitoring outsourcing agreements for control (Australia), location (France and Brazil), or the right to intervene (Germany, Switzerland, and Singapore).

Most jurisdictions also require prior notification or authorization of major outsourcing activities through questionnaires. While questionnaires are not yet harmonized across jurisdictions, they nevertheless improve and facilitate risk assessments. Jurisdictions are also increasingly looking to improve regulations through "security by design" by looking at the interconnectedness of systems and uncovering areas of potential risks and vulnerabilities.

In practice, supervision of outsourcing activities is done primarily using traditional tools. These include on-site supervisory reviews and inspections and off-site reviews through self-assessment questionnaires. Supervisors, for example in Australia, may also engage third-party service providers to assess their systemic role, risk capabilities and controls, providing for a more open form of discussion and leading to relevant insights that can both inform supervisory activities and enhance best practices. Supervisors may also work directly with cloud suppliers, audit contracts (in the Netherlands), and participate in summits.

Business Continuity and Availability

Regulators often request financial institutions to analyze risks and implement appropriate plans to mitigate the risks of cyber attacks. When dealing with third parties, regulators stress the need for financial institutions to align the policies of critical suppliers with their own. Institutions may also be required to define recovery for critical business activities. Italy requires that institutions include in their risk scenarios catastrophic events—including large cyber attacks—that could impact operators and third-party infrastructure. Plans and procedures should address incident management, response and recovery following disruptions, information needs regarding internal and external stakeholders, and resources required to transfer outsourcing activities to other parties in case of a disruption.

Regulators will require that institutions proactively test their processes and measures and that scenario analyses are done at least annually and are based on realistic or probable disruptive scenarios. These activities should be further evaluated through audits and ongoing monitoring. Commonalities in supervisory practices can also help with collaborations and coordination and to improve resilience to cyber threats.

Information Confidentiality and Integrity

Data protection requirements address confidentiality and integrity of information in third-party interactions, typically requiring confidentiality agreements and security requirements to protect bank and customer data. Banks need to verify, assess, and monitor security processes. Banks could also be required to transfer data to the cloud to ensure data security, however, regulations need to specify rules around data location and segregation, data use and access limitations, and security and exit. Cloud service providers, as is the case in Luxembourg, may be prohibited from accessing a bank's data without the bank's explicit consent and only in instances when the bank is unable to access the cloud.

Regulations may also specify that outsourcing arrangements comply with legal and regulatory provisions for protecting confidentiality and personal data. Other, more technical or operational requirements vary significantly, from explicit requirements to encrypt confidential data, to mandated client consent for disclosing their data to third parties.

Expectations and Practices Around Visibility of Third-Party Interconnections

Supervisors often require financial institutions to disclose details about their third-party outsourcing arrangements. Supervisors also typically require financial

institutions to maintain an inventory of outsourced functions and to obtain reports from third parties, and may require visibility into suboutsourcing activities.

Some jurisdictions, including in Luxembourg, focus on identification of hardware and software used in outsourcing activities. Jurisdictions may also focus on the information flows between the institutions and third parties. Other regulations may address configuration or information management processes or processes around terminating outsourcing arrangements, while others focus on the identification and classification of suppliers and contracts.

Auditing and Testing

Supervisory authorities require regulated institutions to guarantee the right to audit and inspect third parties. Jurisdictions may require this for the significant subcontractors, while other jurisdictions provide this right directly for the supervisory entities (including in France, Switzerland, and Singapore). Audit opinions by supervisors on the outsourcing arrangements may be based on reports by the service provider's external auditor, or on internal audit reports that comply with certain guidelines, or on pooled audits from multiple financial institutions. Regulations typically focus on traditional outsourcing or cloud computing. The right to audit and inspect third parties, however, usually focuses on the banking sector.

Nevertheless, regulations are not fully aligned globally when it comes to compliance testing and verification. One method is expected to include supervisor-led or bank-led exercises which focus on interconnectedness.

Resources and Skills

Basel Committee practices on the implications of fintech developments indicate that banks may require to have or obtain specialist competencies in assessing whether they maintain effective oversight of emerging risks from new technologies. It is generally accepted that entities have the relevant capabilities and appropriate staff to effectively monitor and manage the risks from outsourcing.

Regulations require that regulated institutions hire qualified and sufficient number of staff to adequately manage and monitor outsourcing arrangements and to proactively manage key personnel risk in the event that a key person leaves or is unavailable. Staffing shortages should be handled through consultants or specialists. Belgium, for example, requires financial institutions to provide a monitoring and replacement plan for employees to ensure adequately-functioning risk activities. Institutions may also be required to provide clients with documentation on security awareness and responsibilities.

Supervisors generally review the adequacy of institutions' practices through on-site inspections. In jurisdictions where the supervisor has the authority to inspect third parties directly, inspections focus on the qualification and number of staff and the appropriateness of background checks. Staff who are classified as *Certified Information Systems Security Professionals* or organizations which conform to the *ISO 9001 Quality Management System* can be viewed as evidence of required competencies to manage third-party connections.



1. Which of the following types of information-sharing practices is least common?
 - A. Sharing among banks.
 - B. Sharing among regulators.
 - C. Sharing with security agencies.
 - D. Sharing from banks to regulators.
2. Which of the following risks would least likely be covered in the risk analysis within a framework for outsourcing?
 - A. Strategic risk.
 - B. Liquidity risk.
 - C. Compliance risk.
 - D. Vendor lock-in risk.

KEY CONCEPTS

LO 42.a

Cybersecurity and cyber-resilience is typically addressed through IT and operational risk standards, with the goals to encourage good governance and risk management.

Some jurisdictions have specific guidance on cyber risk management, while others do not have specific cyber-related standards. Entities in all jurisdictions are encouraged to adopt and implement international standards.

LO 42.b

Regulators issue either prescriptive regulations or principles-based guidance addressing broader enterprise IT risk management. The five areas of cyber-related governance include:

1. Cybersecurity strategy.
2. Management roles and responsibilities.
3. Awareness.
4. Architecture and standards.
5. Workforce.

Cybersecurity strategy has three approaches: (1) regulators establish sector-specific or cross-sectoral cybersecurity requirements, (2) a regulated entity establishes its own cybersecurity strategy, or (3) regulators review whether financial institutions have appropriate IT strategies that cover cyber risk.

Management roles and responsibilities focus around the board of directors and senior management to address cyber risk strategies. Regulatory standards often include the three lines of defense model for cyber risk management.

Awareness focuses on management's and the board's responsibilities around proper training for employees and for cybersecurity awareness and on developing a common risk culture that improves the effectiveness of cyber risk management.

Architecture and standards address content storage and self-assessments around cybersecurity.

Workforce addresses training of the IT workforce, on-site inspections, defining the roles and responsibilities of IT staff, and guidelines around cybersecurity.

LO 42.c

The four areas of cyber risk management and incident response and recovery are:

1. Supervision of cyber-resilience.
2. Information security controls.
3. Incident response and recovery.
4. Cybersecurity and resilience metrics.

Supervision of cyber-resilience. The primary focus of supervision is on the complexity and business model of key risks. Cybersecurity reviews can be triggered by institutions' own risk assessments, by findings from inspections, or by analyses of cyber incidents. However, there are significant differences in jurisdictional approaches. Jurisdictions are increasingly engaging with industry, not only to address cyber risk, but to influence behavior and aid regulatory work.

Information security controls. Controls focus on threat detection, business impact analysis, recovery planning, or scoping for assessments. Supervisory reviews may be thematic or use international standards. Institutions test security controls for both hardware and software data to detect and prevent cybersecurity incidents, while regulators analyze survey responses and audit and control testing reports.

Jurisdictions may use risk taxonomies to identify gaps in controls and supervision, but taxonomies are not globally harmonized.

Incident response and recovery. Regulators generally require institutions to establish a risk framework or policies for risk detection and response and recovery, although these typically focus on overall risk management rather than directly on cybersecurity. Banks and supervisors may use training exercises on how to respond to incidents.

Cybersecurity and resilience metrics. Methodologies to test cybersecurity do not have standardized quantitative metrics. Backward-looking data may be useful in predicting future performance as long as institutions function in a stable operating and risk environment. However, institutions are now increasingly recognizing the importance of forward-looking indicators to improve resilience to attacks.

LO 42.d

The three most common types of information-sharing practices are sharing (1) among banks, (2) from banks to regulators, and (3) from banks and regulators to security agencies. Other types include sharing (4) among regulators and (5) from regulators to banks.

Sharing among banks. Banks share information on cyber threats, incidents, or other information. Sharing of cyber threat information among banks depends on the level of trust between banks.

Sharing from banks to regulators. Banks typically share information with regulators that has been mandated and is specifically linked to operational incidents, including cyber incidents, in order to (1) enable systemic risk monitoring, (2) enhance regulatory requirements, (3) improve regulatory oversight, and (4) facilitate information sharing. However, regulatory requirements vary.

Sharing among regulators. This form of sharing is not frequent and can be among domestic regulators or with other cross-border regulators. Improved dialogue among

regulators would increase awareness and the timeliness of regulatory guidance.

Sharing from regulators to banks. Sharing of cybersecurity information from regulators to banks is not common, and the majority of jurisdictions have no clear guidance around sharing of information with banks.

Sharing with security agencies. Sharing by banks and regulators with national security agencies is primarily done on a voluntary basis. Some jurisdictions, however, have formal mandates. Exchanging information with the security agencies improves countermeasures and cyber threat detection and response.

LO 42.e

Analysis of third parties can be broken down into:

- Governance of third-party interconnections.
- Business continuity and availability.
- Information confidentiality and integrity.
- Expectations and practices around visibility of third-party interconnections.
- Auditing and testing.
- Resources and skills.

Governance of third-party interconnections. Regulations typically require that institutions establish a proper framework for outsourcing that defines the roles and responsibilities, the scope of activities that can be outsourced, risk analysis, and monitoring and risk assessment. Supervision can be done on-site or off-site.

Business continuity and availability. Regulators typically request financial institutions to analyze risks and implement appropriate plans to mitigate the risks of cyber attacks and to align the policies of critical suppliers with their own. Procedures should address incident management, response and recovery, and internal and external stakeholders' needs.

Information confidentiality and integrity. Data protection requirements require that institutions have confidentiality agreements and security requirements to protect bank and customer data. Institutions need to verify, assess, and monitor security processes, and may be required to transfer data to the cloud to ensure data security. However, technical or operational requirements vary significantly.

Expectations and practices around visibility of third-party interconnections. Supervisors typically require financial institutions to disclose details about third-party outsourcing and to maintain an inventory of outsourced functions. They may also require visibility into suboutsourcing activities. Some jurisdictions focus on identification of hardware and software, while others focus on the information flows between the institutions and third parties.

Auditing and testing. The right to audit and inspect third parties is critical to regulators, which may obtain information from external or internal audit reports. Regulations typically focus on traditional outsourcing or cloud computing. However, regulations continue to vary globally regarding compliance testing and verification.

Resources and skills. Regulations require that regulated institutions hire qualified and adequate number of staff to manage and monitor risks from outsourcing arrangements.

Supervisors often conduct tests through on-site inspections.

ANSWER KEY FOR MODULE QUIZZES

Module Quiz 42.1

1. **A** One of the three approaches to cybersecurity strategy is by regulators to establish either sector-specific or cross-sectoral cybersecurity requirements. This is common in emerging markets with homogenous banking systems. (LO 42.b)
2. **A** The four areas of cyber risk management are (1) supervision of cyber-resilience, (2) information security controls, (3) incident response and recovery, and (4) cybersecurity and resilience metrics. (LO 42.c)

Module Quiz 42.2

1. **B** The five types of information-sharing practices include sharing (1) among banks, (2) from banks to regulators, (3) among regulators, (4) from regulators to banks, and (5) from banks and regulators to security agencies. The three most common sharing types are sharing among banks, sharing with security agencies, and sharing from banks to regulators. Sharing among regulators and from regulators to banks is less common. (LO 42.d)
2. **B** The risk analysis within an outsourcing framework should specify the risks covered and their mitigants. These include strategic risk, compliance risk, security risk, business continuity risk, vendor lock-in risk, counterparty risk, and access risks. Liquidity risk is not a risk covered in these risk analyses. (LO 42.e)

¹ European Framework for Threat Intelligence-Based Ethical Red Teaming (TIBER-EU).
<https://www.ecb.europa.eu/press/pr/date/2018/html/ecb.pr180502.en.html>

² https://ec.europa.eu/info/law/markets-financial-instruments-mifid-ii-directive-2014-65-eu_en

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 9.

READING 43

CASE STUDY: CYBERTHREATS AND INFORMATION SECURITY RISKS

Study Session 8

EXAM FOCUS

This reading discusses information security risks that firms face, including the types of threats, and the global frameworks and standards that have been put in place to provide guidance on how to mitigate these risks. The reading begins by categorizing risks by quadrants, including whether incidents are internal versus external and intentional versus unintentional. This is followed by a discussion of the three globally recognized and adopted cybersecurity standards and frameworks, which help firms identify and mitigate their information security risks and incident responses. The case study of Equifax describes an important 2017 cyberattack, including reasons for the failure of detecting and avoiding the threat, as well as important lessons learned.

MODULE 43.1: INFORMATION SECURITY RISKS AND FRAMEWORKS

LO 43.a: Provide examples of cyber threats and information security risks, and describe frameworks and best practices for managing cyber risks.

Information Security Risk Typology

Information security risk, which refers to more than just cyber risk, includes *intentional actions* and *unintentional actions*. Intentional actions can include employees stealing and leaking data, or external parties hacking an email. Unintentional actions include losing or accidentally disclosing private or secure information, or inadvertently sending sensitive data to external parties. Information security risk also includes the loss or theft of nondigital data, including paper documents. It is the responsibility of firms to implement adequate risk controls and mitigate incident risk.

One way to categorize information security risks is through a four-quadrant approach, as shown in Figure 43.1, with data incidents categorized as *internal* versus *external* and *intentional* versus *unintentional*.

Figure 43.1: Information Security Risks

Data Incident	Intentional (Theft or Corruption)	Unintentional (Loss or Involuntary Disclosure)
External causes (including third parties)	<i>Digital</i> (hacks, viruses, phishing) <i>Physical</i> (theft, social engineering)	Disaster, systems disruptions, failure by third parties
Internal causes	Theft, transfer of digital/physical information Taking proprietary information when leaving firm (mishandled exits)	<i>Digital</i> (errors when sending documents, loss of database/backups/devices) <i>Physical</i> (loss of printed materials, loss of archives, discussing confidential information)

In addition to the broader information security risks, the financial industry is particularly vulnerable to cyberattacks and information leaks. High-profile data hacks over the last few years, including the 2017 incident involving Equifax and Appleby (an offshore law firm and tax advisor) as well as significant data leaks (including in insurance, journalism, and cryptocurrencies), have highlighted the risk of inadequate risk defenses. The need to protect digital information has been especially pronounced during the COVID-19 pandemic, which sped up the pace of digitization (e.g., use of QR codes), accelerated social media use, and disrupted supply chains.

Cybersecurity Risk Frameworks and Standards

Cyber risk is one of the most important information security risks. There are three standards/frameworks that are globally recognized and adopted:

1. The U.S. National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF)
2. The Center for Internet Security (CIS) Critical Security Controls
3. The International Standards Organization (ISO) framework ISO 27001

NIST CSF

NIST was founded by U.S. Congress and operates under the U.S. Department of Commerce. The NIST CSF is a framework that was initially developed to help critical infrastructure (e.g., power plants) deal with cyberattacks, but it grew to help any business protect its networks and data against cybersecurity threats. The framework is voluntary.

The NIST framework helps businesses analyze and assess threats and vulnerabilities and reduce risks. The framework also assists with response and recovery following a cybersecurity incident, using root-cause analysis. The NIST is similar to an operational risk management framework (ORMF) that identifies, assesses, mitigates, and monitors risks. There are five key steps in the NIST framework, which are identify, protect, detect, respond, and recover:

- *Identify*. This first step begins by creating a list of all IT/technology equipment, software, and data (should include electronic, mobile, and point-of-sale devices). Businesses should create and share their cybersecurity policy including roles and

responsibilities of employees, vendors, and other third parties, and the steps taken in case of a cyberattack.

- *Protect.* Businesses should restrict who has access to their network and devices, and use security software to protect, encrypt, and back up their data. Policies should be in place to safely dispose of files and data. Security software should be updated regularly—and employees should be trained on their roles in understanding and mitigating risks.
- *Detect.* Businesses should monitor computers, software, and hardware for unauthorized access and unauthorized users or connections, and investigate unusual activities.
- *Respond.* It is important that businesses create a plan for keeping operations running in case of a cyberattack, and notify customers, employees, and other stakeholders. Any attack should be investigated, contained, and reported to law enforcement or authorities. Cybersecurity policies should be updated with lessons learned, and businesses should prepare for unpredictable events (e.g., power outage due to weather).
- *Recover.* Following an attack, businesses should repair and restore the impacted equipment or data, and ensure that employees and customers are continuously and adequately informed.

CIS

CIS is a set of detailed guidances for companies looking to establish or review their cybersecurity protocol. It can also be used to complement existing compliance standards including NIST, or to help with ISO 27001 cybersecurity certification.

The CIS framework helps protect firms from the most widespread cyberattacks and threats, and it includes key controls that are continuously updated by experts. CIS is mapped to and referenced by several other legal, regulatory, and policy frameworks. The most recent set of key controls have been refreshed to incorporate changes like cloud-based computing, virtualization, mobility, outsourcing, and the move to working from home.

ISO 27001

ISO 27001 is the key global standard for cybersecurity. The standard gives guidance on firms' organization of risk management activities, operational planning and control, and information security risk assessment and treatment. It also provides guidance on governance, policies, communications about the firm, management review, and audit.

ISO 27001 itself does not provide firms directly with implementable advice. Instead, it provides a checklist of what firms need to achieve to gain certification in ISO standards and adopt ISO 27001. Firms wanting certification must have an Information Security Management System (ISMS) that manages information security risks (e.g., identifies threats and vulnerabilities). Firms need to put in place effective and comprehensive controls to mitigate risks, and adopt a comprehensive risk management process with ongoing improvements.

Cybersecurity Protection and Monitoring

Protecting cybersecurity information has three components: **confidentiality**, **integrity**, and **availability** (or **CIA**). Confidentiality and integrity relate to information security, while availability relates to business continuity.

Furthermore, **information controls** can be categorized as behavioral controls and technical controls:

- **Behavioral controls** address human behavior and shortcomings. These controls aim at protecting information through awareness campaigns, rules of conduct, training, password management, and appropriate supervision and necessary sanctions.
- **Technical controls** address the technical side of risk through prevention, detection, and mitigation:
 - **Preventative controls** are directed at external threats, and include firewalls, encryption, passwords, and patching.
 - **Detective controls** try to generate early warnings of data incidents, including data loss prevention and detection (DLPD) solutions that monitor and identify unauthorized data disclosures.
 - **Mitigating controls** try to keep redundancies and backups offline.

Each firm must conduct its own cost-benefit analysis by weighing the cost of controls, convenience, and speed against the benefits of risk reduction. Most firms monitor cyberattacks and breaches within their IT department, although many firms have an *information security department* separate from IT, which designs, maintains, and monitors risk controls.

Equifax Case Study

LO 43.b: Describe lessons learned from the Equifax case study.

Equifax is one of the three main credit bureaus in the United States, analyzing consumer credit reports (that determine credit scores). Equifax experienced a major cyber breach in March 2017, one of the largest cyberattacks in recent years. The attack happened a few days after Equifax applied a patch to one of its open-source applications, Apache Struts. The attackers exploited a vulnerability in the patch and quickly gained access to other vulnerable parts of Equifax's network; they were able to steal information relating to customer names, addresses, birthdays, Social Security numbers, and credit cards. The attack was unnoticed by Equifax for three months. In total, the breach impacted 147 million customers.

So why was Equifax so vulnerable? In short, it used outdated cybersecurity frameworks and policies, and it did not adequately update its outdated security tools. In fact, its own internal audit from 2015 revealed that there was a backlog of some 8,500 unpatched vulnerabilities, which remained unresolved at the time of the cyberattack. In 2016, Equifax already experienced a major cyber breach when its website was hacked, impacting 430,000 customers. The NIST already assigned it a vulnerability score of 10 to Apache Struts, indicating maximum criticality.

Equifax's failures can be categorized into five areas of weakness:

1. It maintained insufficient inventory of its IT systems and assets, exposing it to vulnerabilities including the inability to patch systems quickly.
2. It failed to enforce its patch management policy (part of risk management).
3. Employee communication was inefficient and insufficient, as communications about the vulnerabilities missed key employees.
4. Equifax used an expired SSL certificate, which prevented it from adequately monitoring its encrypted traffic. It was only in late July 2017 that the breach was discovered—more than three months after it initially happened.
5. Public/external communication was poor, with weak crisis communication. Equifax did not alert the public until September 7, 2017.

As a result of its negligence, Equifax had suffered serious consequences. In addition to a drop in its share price and several high-profile resignations—including its CEO, CSO, and CIO—it was subject to several investigations, fines, and lawsuits. In the end, it paid \$700 million in fines and compensation, including \$300 million paid directly to individuals impacted by the breach. Subsequently, Equifax overhauled its IT security systems and management.



MODULE QUIZ 43.1

1. The four-quadrant approach categorizes information security risks as:
 - A. internal versus external and intentional versus unintentional.
 - B. internal versus external and in house versus third party.
 - C. intentional versus unintentional and digital versus physical.
 - D. intentional versus unintentional and theft versus corruption.
2. An employee inadvertently emails a sensitive and confidential file to a third-party recipient. The employee's action would most likely be categorized as:
 - A. internal and intentional.
 - B. external and unintentional.
 - C. internal and unintentional.
 - D. external and intentional.
3. Following a severe power outage, a firm is unable to recover one of its servers that had significant and sensitive client information. This incident would most likely be categorized as:
 - A. internal and intentional.
 - B. external and unintentional.
 - C. internal and unintentional.
 - D. external and intentional.
4. Which of the following issues was not identified as a key weakness in Equifax's information security management?
 - A. Poor public communication.
 - B. Using an expired digital certificate.
 - C. Lack of a comprehensive list of its IT assets.
 - D. Lack of sufficient internal phishing exercises.

KEY CONCEPTS

LO 43.a

Information security risk includes cyber risk as well as other intentional and unintentional actions:

- Intentional actions include information theft of physical or digital data, data leaks, and hacks.
- Unintentional actions include losing or accidentally disclosing or sending secure information.

Information security risks can be characterized through a four-quadrant approach, with data incidents categorized as internal versus external and intentional versus unintentional.

As recent high-profile incidents show, the financial industry is especially vulnerable to cyberattacks and information leaks. The COVID pandemic has also accelerated the use of digital data and digital information, which further highlights the need to protect such information.

There are three globally recognized and adopted cybersecurity standards and frameworks:

- The U.S. National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF) is a voluntary framework that helps businesses protect their networks and data against cybersecurity threats. The framework also assists with response and recovery following a cybersecurity incident. It is based on five key steps: identify, protect, detect, respond, and recover.
- The Center for Internet Security (CIS) Critical Security Controls provides a set of detailed guidances for companies looking to establish or review their cybersecurity protocol. The CIS framework is mapped to and referenced by several other legal, regulatory, and policy frameworks and includes key controls that are continuously updated by experts.
- The International Standards Organization (ISO) framework ISO 27001 provides guidance on firms' organization of risk management activities, operational planning and control, and information security risk assessment and treatment. It provides a checklist for certification in ISO standards, including the need to have an Information Security Management System (ISMS), effective and comprehensive controls to mitigate risks, and adoption of a comprehensive risk management process.

Cybersecurity information protection has three components: confidentiality, integrity, and availability (or CIA).

Information controls can be categorized as behavioral controls and technical controls. Behavioral controls address human behavior and shortcomings, including information via awareness campaigns, training, and password management. Technical controls address the technical side of risk through prevention, detection, and mitigation.

LO 43.b

Equifax's 2017 cyberattack exposed significant vulnerabilities. The attack was one of the largest cyberattacks in recent years and impacted 147 million customers.

The attack was possible because Equifax used outdated cybersecurity frameworks and policies, and it did not adequately update or patch its outdated security tools.

Equifax's failures can be categorized into five areas of weakness:

- An insufficient inventory of its IT systems and assets
- Failure to enforce its patch management policy
- Inconsistent employee communication
- Using an expired SSL certificate
- Poor public/external communication

ANSWER KEY FOR MODULE QUIZ

Module Quiz 43.1

1. **A** The four-quadrant approach analyzes information security risks with data incidents categorized as internal versus external and intentional versus unintentional. Theft and corruption are part of intentional data incidents. Both intentional and unintentional data incidents can be categorized as digital or physical. In-house and third-party incidents are just examples of internal and external data incidents, respectively. (LO 43.a)
2. **C** Errors when sending documents, including sending the wrong attachments or sending to the wrong email recipients, are examples of internal and unintentional data incidents. (LO 43.a)
3. **B** Disaster, systems disruptions, and third-party failures are examples of external and unintentional data incidents. (LO 43.a)
4. **D** A lack of sufficient phishing exercises was not one of the key concerns identified in the case of Equifax. Key weaknesses included the following:
 - An insufficient inventory of its IT systems and assets
 - Failure to enforce its patch management policy
 - Inconsistent employee communication
 - Using an expired SSL certificate
 - Poor public/external communication (LO 43.b)

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 assigned reading—Basel Committee on Banking Supervision.

READING 44

SOUND MANAGEMENT OF RISKS RELATED TO MONEY LAUNDERING AND FINANCING OF TERRORISM

Study Session 8

EXAM FOCUS

This reading focuses on the Basel Committee's recommendations for identifying, assessing, and managing the risks associated with money laundering and the financing of terrorism (ML/FT) through banks. The concept of customer due diligence (CDD) is important and focuses on the precautionary steps a bank must take to ensure it knows the true identities of the customers with which it is dealing. Because many of the higher risk situations arise out of international, cross-border transactions, much of the recommendations focus on the risks associated with these activities. For the exam, understand who bears the ultimate responsibility for customer identification and verification, even if a third party is hired to carry out CDD.

MODULE 44.1: MANAGEMENT OF MONEY LAUNDERING AND FINANCIAL TERRORISM RISKS

LO 44.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.

The Basel committee (referred to as the Committee) is committed to combating **money laundering (ML)** and the **financing of terrorism (FT)** as part of its mandate to enhance worldwide financial stability via a strengthening of regulation, supervision, and bank practices. The Committee has a long-standing commitment to sound **Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT)** policies and procedures in banks. Banks without sound ML/FT risk management practices are exposed to serious risks including, but not limited to: reputational, operational, compliance, and concentration risks. Costs associated with these risks include fines and sanctions by regulators, the termination of wholesale funding and facilities, claims against the bank, loan losses, asset seizures, asset freezes, and investigative costs.

Risk Assessment

The Committee's *Core Principles for Effective Banking Supervision* was updated in 2012 and requires that all banks, "have adequate policies and processes, including strict **customer due diligence (CDD)** rules to promote high ethical and professional standards in the banking sector and prevent the bank from being used, intentionally or unintentionally, for criminal activities." Sound risk management means the bank must identify and manage ML/FT risks, designing and implementing policies and procedures corresponding to the identified risks. These risks must be assessed at the country, sector, bank, and business relationship levels. The bank must have policies and procedures for:

- Customer identification.
- Customer due diligence.
- Customer acceptance.
- Monitoring of business relationships.
- Monitoring of business operations.

The bank must develop a thorough understanding of ML/FT risks present in:

- The customer base.
- The bank's products and services.
- The delivery channels for products and services, including products and services in the development stage.
- The jurisdictions within which the bank and the bank's customers do business.

The bank's understanding of inherent ML/FT risks is based on both internal and external data sources, including operational and transaction data (internal) and national risk assessments and country reports from international organizations (external).

Risk Management

Proper governance arrangements are necessary for the management of ML/FT risks. Prior publications from the Committee (specifically, *The Internal Audit Function in Banks*, June 2012, *Corporate Governance Principles for Banks*, July 2015, and *Compliance and the Compliance Function in Banks*, April 2005) describe proper governance arrangements. In particular, these publications require the board of directors to approve and oversee risk policies, risk management activities, and compliance. These functions are critical to the management and mitigation of ML/FT risks. ML/FT risk assessments must be communicated to the board of directors in a timely, complete, accurate, and understandable manner.

The board of directors and senior management should appoint a qualified chief AML/CFT officer with the stature and authority to garner the attention of the board, senior management, and business lines when ML/FT issues arise.

Risk Mitigation

First line of defense. The **business units** (e.g., the front office and customer facing activities) are the first line of defense in identifying, assessing, and controlling ML/FT risks. Policies and procedures should be specified in writing and communicated to bank personnel. Employees should know what they are supposed to do and how to comply with regulations. There should be procedures in place for detecting and reporting suspicious transactions. High ethical and professional standards are essential. The bank should carry out employee training on how to identify and report suspicious transactions.

Second line of defense. The **chief officer in charge of AML/CFT** is the second line of defense. The officer should engage in ongoing monitoring and the fulfillment of AML/CFT duties. The officer should be the contact person for AML/CFT issues both internally and externally (e.g., supervisory authorities and financial intelligence units [FIUs]). To avoid conflicts of interest, the officer should not have business line responsibilities or be responsible for data protection or internal audits. The officer may also be the chief risk officer and should have a direct reporting line to senior management and/or the board of directors.

Third line of defense. The third line of defense is **internal audits**. The bank should establish policies for conducting internal audits of the bank's AML/CFT policies. **External audits** may also play a role in evaluating a bank's policies and procedures with respect to the AML/CFT function.

Risk Monitoring

The bank's risk monitoring systems should be commensurate with the bank's size, activities, and complexity. For most banks, and especially for banks that are internationally active, some of the monitoring activities will be automated. A bank must document its decision to forgo information technology (IT) monitoring and demonstrate an effective alternative. Monitoring systems should be able to provide accurate information to senior management on issues such as changes in the transactional profiles of bank customers. The IT system should also enable a bank to determine its own criteria for monitoring and filing **suspicious transaction reports (STR)** or taking other steps to minimize ML/FT risks. Internal audits should evaluate the effectiveness of IT monitoring systems.

LO 44.b: Describe recommended practices for the acceptance, verification, and identification of customers at a bank.

Customer Acceptance

Banks must determine which customers pose a high risk of ML/FT. Factors the bank should consider include the customer's:

- Background.
- Occupation including public and/or high profile figures.
- Business activities.
- Sources of income and wealth.

- Country of origin.
- Country of residence, if different from country of origin.
- Choice and use of bank products and services.
- Nature and purpose of the bank account.
- Linked accounts.

For lower-risk customers, simplified assessment procedures may be used (e.g., a customer with low balances who uses the account for routine banking needs). Also, the customer acceptance standards must not be so restrictive that they deny access to the general public, especially financially or socially disadvantaged persons.

Enhanced due diligence may be required for:

- Accounts with large balances and regular cross-border wire transfers.
- A politically exposed person (PEP), especially foreign PEPs.

Banks must determine the risks they are willing to accept in order to do business with higher-risk customers. The bank must also determine the circumstances under which it will not accept a new business relationship or will terminate an existing relationship.

Customer Verification

The Financial Action Task Force (FATF) Recommendation 10 defines a *customer* as any person entering into a business relationship with a bank or carrying out an occasional financial transaction with a bank. Banks must, according to FATF standards, identify customers and verify their identity. Banks must establish a systematic procedure for identifying and verifying customers. In some cases, the bank must identify and verify a person acting on behalf of a beneficial owner(s).

In terms of verification of a person's identity, the bank must be aware that the best documentation is that which is difficult to forge or to obtain illicitly. A bank may require a written declaration of the identity of a beneficial owner but should not rely solely on such a declaration. A bank must not forgo identification and verification simply because the customer cannot be present for an interview. The bank should pay particular attention to customers from jurisdictions that are known to have AML/CFT deficiencies. Enhanced due diligence is called for in these circumstances.

Customer Identification

In order to develop customer risk profiles (or categories of customers), the bank should collect data pertaining to the:

- Purpose of the relationship or of the occasional banking transaction.
- Level of assets.
- Size of the transactions of the customer.
- Regularity or duration of the banking relationship.
- Expected level of activity.
- Types of transactions.
- Sources of customer funds, income, or wealth (if necessary).

The bank should identify “normal” behavior for particular customers or categories of customers and activities that deviate from normal and might be labeled unusual or suspicious.

Customer identification documentation may include:

- Passports.
- Identity cards.
- Driving licenses.
- Account files such as financial transaction records.
- Business correspondence.

If the bank cannot perform CDD, it should not open the account or perform a transaction. If the bank must, so as to not interrupt the normal conduct of business, engage in a business transaction prior to verification, and ultimately cannot verify the customer’s identity, then the bank should consider filing an STR. The customer should *not* be informed that the STR has been or will be filed, either directly or indirectly.

If the bank believes a customer has been refused banking services from another bank due to concerns about illicit activities, the bank should consider classifying the customer as high risk and engage in enhanced CDD or reject the customer altogether. If the customer insists on anonymity (or gives an obviously fictitious name), the bank should refuse to accept the customer. Numbered accounts may provide a level of confidentiality for a customer, but the bank must still verify the identity of the account holder.

Ongoing monitoring of customer accounts and vigilant record-keeping are necessary to ML/FT risk management.

ML/FT Risk Management for Cross-Border Banks

LO 44.c: Explain practices for managing ML/FT risks in a group-wide and cross-border context.

When a bank operates in multiple jurisdictions, it is subject to numerous country regulations. Each banking group (*group* refers to an organization’s one or more banks and the branches and subsidiaries of the bank[s]) should develop group-wide AML/CFT policies and procedures and consistently apply those policies across the group’s international operations. Policies should be consistently applied (and supportive of the group’s broader policies and procedures regarding ML/FT risks) even if requirements differ across jurisdictions. If the host jurisdiction’s requirements are stricter than the group’s home country, the branch or subsidiary should adopt the host jurisdiction requirements.

If a host country does not permit the proper implementation of FATF standards, then the chief AML/CFT officer should inform home supervisors. In some instances, the bank may need to close operations in the host country.

In a cross-border context, AML/CFT procedures are more challenging than other risk management processes because some jurisdictions restrict a bank's ability to transmit customer names and balances across national borders. However, for risk management purposes, it is essential that banks be able to, subject to legal protections, share information about customers with head offices or the parent bank.

Risk assessment and management activities, such as customer risk assessments, group-wide risk assessments, and internal and external audits, apply to multi-national banks. When business is being referred to a bank, the bank's own AML/CFT standards must be used in place of the jurisdiction of the referring bank, unless the introducer is in a jurisdiction with equal or stricter standards and requirements.

Banks involved in cross-border activities should:

- Integrate information on the customer, beneficial owners of the customer, and the funds involved in the transaction(s).
- Monitor significant customer relationships, balances, and activity on a consolidated basis whether the account is on- or off-balance sheet, as assets under management (AUM), or on a fiduciary basis.
- Appoint a chief AML/CFT officer for the whole group who must ensure group-wide compliance (across borders) of AML/CFT requirements.
- Oversee the coordination of group-wide information sharing. The head office should be informed of information regarding high-risk customers. Local data protection and privacy laws must be considered.

For larger banks, the ability to centralize bank processing systems and databases may allow for more effective and efficient risk management.

Role of Supervisors

Bank supervisors are expected to:

- Comply with FATF Recommendation 26 and apply the *Core Principles for Effective Banking Supervision* as it relates to the supervision of AML/CFT risks. FATF states the principles that are relevant to money laundering and the financing of terrorism.
- Set out supervisory expectations governing banks' AML/CFT policies and procedures.
- Adopt a risk-based approach to supervising banks' ML/FT risk management systems. To that end, supervisors must:
 - Understand the risks present in other jurisdictions and the impact on the supervised banks.
 - Evaluate the adequacy of the bank's risk assessment based on the jurisdiction's national risk assessments.
 - Assess the bank's risks in terms of the customer base, products and services, and geographical locations in which the bank and its customers do business.
 - Evaluate the effectiveness in implementation of the controls (e.g., CDD) designed by the bank to meet AML/CFT obligations.
 - Allocate resources to conduct effective reviews of the identified risks.

- Protect the integrity of the financial system by protecting the safety and soundness of banks relative to ML/FT risk management. This means making it clear that supervisors will take action, action that may be severe and public, against banks and their officers who fail to follow their own internal procedures and regulatory requirements.
- Make sure the stricter of two jurisdictions' requirements is applied.
- Verify a bank's compliance with group-wide AML/CFT policies and procedures during on-site inspections.
- Extend full cooperation and assistance to home-country supervisors who need to assess a bank's overseas compliance with group-wide AML/CFT policies and procedures.
- Ensure there is a group audit and determine the scope and frequency of audits of the group's AML/CFT risk management procedures.
- Ensure the confidentiality of customer information provided to supervisors.
- Make sure that supervisors are not classified as "third parties" in countries where there are restrictions on the disclosure of customer information to third parties.



MODULE QUIZ 44.1

1. Which of the following is an example of external data that the chief Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) officer should analyze and understand in order to manage and mitigate money laundering and the financing of terrorism (ML/FT) risks?
 - A. Transaction data.
 - B. Payment message streams.
 - C. Country reports.
 - D. Customer passports and identity card.
2. With respect to managing and mitigating money laundering and the financing of terrorism (ML/FT) risks in a bank, bank tellers and branch managers are examples of:
 - A. the first line of defense.
 - B. the second line of defense.
 - C. the most important line of defense.
 - D. lower level bank employees that have little to do with financial crimes risk management.
3. The risk manager of a large U.S. multi-national bank is attempting to put in greater risk controls. In keeping with recommendations from the Basel Committee on the sound management of risks related to money laundering and the financing of terrorism (ML/FT) she requires enhanced customer due diligence (CDD) for:
 - A. all accounts from customers initiated in countries outside the United States.
 - B. accounts with regular cross-border wire transfers.
 - C. individual accounts with balances less than the \$250,000 Federal Deposit Insurance Corporation (FDIC) insurance limit.
 - D. accounts of persons who reside in countries other than their countries of birth.
4. Which of the following is the role of a bank supervisor, acting in its role regarding the supervision of Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) risks?
 - A. Require all banks to use the same global payment systems to make detection of irregularities simpler.

- B. Make sure all banks have a chief AML/CFT risk manager that reports directly to the board of directors.
- C. Require all banks to provide daily documentation to the supervisor on any cross-border wire transfers.
- D. Make sure the stricter of the two jurisdictions' rules regarding ML/FT risks are applied by banks.

KEY CONCEPTS

LO 44.a

To assess money laundering and the financing of terrorism (ML/FT) risks, the bank must know the identities of its customers and must have policies and procedures for:

- Customer identification.
- Customer due diligence (CDD).
- Customer acceptance.
- Monitoring of business relationships.
- Monitoring of business operations.

To mitigate ML/FT risks, the first line of defense is the business units (e.g., the front office and customer facing activities). They identify, assess and control ML/FT risks through policies and procedures that should be specified in writing and communicated to bank personnel. The second line of defense is the chief officer in charge of anti-money laundering and countering financing of terrorism (AML/CFT). The officer should engage in ongoing monitoring and the fulfillment of AML/CFT duties. The third line of defense is internal audits. The bank should establish policies for conducting internal audits of the bank's AML/CFT policies.

LO 44.b

Banks must determine which customers pose a high risk of ML/FT. Factors the bank should consider include the customer's background, occupation, sources of income and wealth, the country of origin and the country of residence, the choice and use of the bank's products and services, the nature and purpose of the bank account, and any linked accounts. Banks must, according to the Financial Action Task Force (FATF) standards, identify customers and verify their identities. Banks must establish a systematic procedure for identifying and verifying customers. In some cases, the bank must identify and verify a person acting on behalf of a beneficial owner(s). Customer identification documentation may include passports, identity cards, driving licenses, and account files such as financial transaction records and business correspondence.

LO 44.c

Banks involved in cross-border activities should:

- Integrate information on the customer, beneficial owners of the customer (if one exists), and the funds involved in the transaction(s).
- Monitor significant customer relationships, balances, and activity on a consolidated basis whether the account is on- or off-balance sheet, as assets under management (AUM) or on a fiduciary basis.

- Appoint a chief AML/CFT officer for the whole group (the group of banks and branches that are part of one financial organization) who must ensure group-wide compliance (across borders) of AML/CFT requirements.
- Oversee the coordination of group-wide information sharing. The head office should be informed of information regarding high-risk customers. Local data protection and privacy laws must be considered.

Bank supervisors must comply with FATF Recommendation 26 and apply the *Core Principles for Effective Banking Supervision* as it relates to the supervision of AML/CFT risks. FATF states the principles that are relevant to money laundering and financing of terrorism. They must also set out supervisory expectations governing banks' AML/CFT policies and procedures and should adopt a risk-based approach to supervising banks' ML/FT risk management systems.

ANSWER KEY FOR MODULE QUIZ

Module Quiz 44.1

1. **C** The bank's understanding of inherent money laundering and the financing of terrorism (ML/FT) risks is based on both internal and external data sources including operational and transaction data (internal) and national risk assessments and country reports from international organizations (external). (LO 44.a)
2. **A** To mitigate ML/FT risks, the first line of defense is the business units (e.g., the front office and customer facing activities). They identify, assess, and control ML/FT risks through policies and procedures that should be specified in writing and communicated to bank personnel. The second line of defense is the chief officer in charge of AML/CFT. The third line of defense is internal audits. (LO 44.a)
3. **B** Banks must determine which customers pose a high risk of ML/FT. Factors the bank should consider include the customer's background, occupation, business activities, sources of income and wealth, country of origin, country of residence, if different from country of origin, choice and use of bank products and services, nature and purpose of the bank account, and any linked accounts. For lower-risk customers, simplified assessment procedures may be used (e.g., a customer with low balances who uses the account for routine banking needs). Enhanced due diligence may be required for:
 - Accounts with large balances and regular cross-border wire transfers.
 - A politically exposed person (PEP), especially foreign PEPs.
 (LO 44.b)
4. **D** Bank supervisors have many jobs in conjunction with ML/FT risks, including complying with FATF Recommendation 26 and applying the *Core Principles for Effective Banking Supervision* as it relates to the supervision of AML/CFT risks. Supervisors should make sure the stricter of two jurisdictions' requirements is applied. They do not, however, require banks to use the same payment systems, require daily documentation of cross-border wire transfers be submitted to the supervisor, or require banks to have a chief AML/CFT officer that reports to the

board (although it is recommended that banks have an officer that reports to the board and/or senior management). (LO 44.c)

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 11.

READING 45

CASE STUDY: FINANCIAL CRIME AND FRAUD

Study Session 8

EXAM FOCUS

In this reading, we look at the components of financial crimes and fraud. These include internal and external fraud, money laundering, and terrorism financing. The reading begins with defining each concept and discussing the key control steps. For the exam, be able to distinguish between the different types of financial crimes and fraud but do not get caught up in the small technical details. This section is followed by a detailed discussion of anti-money laundering (AML) risk management, before introducing the case study of USAA Federal Savings Bank and the reasons for the significant financial fines levied against the bank for material deficiencies in its AML risk management controls.

MODULE 45.1: FINANCIAL CRIME AND FRAUD RISK MANAGEMENT

LO 45.a: Describe elements of a control framework to manage financial fraud risk and money laundering risk.

Definitions of Financial Crime, Internal Fraud, and External Fraud

The definition of **financial crime** is broad and includes internal and external fraud, money laundering (ML), and terrorism financing (TF). The U.K. Financial Conduct Authority (FCA) defines financial crime as “any kind of criminal conduct relating to money or to financial services or markets, including any offense involving: (a) fraud or dishonesty; or (b) misconduct in, or misuse of information relating to, a financial market; or (c) handling the proceeds of crime; or (d) the financing of terrorism.”¹ Internal and external fraud, ML, and TF are also covered under the Basel Committee on Banking Supervision’s (BCBS) definition of operational risk.

The BCBS defines **internal fraud** as “losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy,

excluding diversity/discrimination events, which involve at least one internal party.”² In essence, internal fraud refers to dishonest or fraudulent acts committed by employees, and it can be categorized as **unauthorized activities** and **theft and fraud**. *Unauthorized activities* refers to employees knowingly disregarding or violating laws and internal policies (e.g., making unauthorized transactions, not reporting transactions, mismarking trading positions, sharing passwords, or sharing confidential client information with others). *Theft and fraud* refers to stealing or dishonest use of assets, including embezzlement, extortion, bribery, forgery, smuggling, and tax evasion.

The BCBS defines **external fraud** as “losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party.”² The definition of external fraud is similar to internal fraud except that the fraud is committed by an outside, third party. The two subcategories of external fraud are **theft and fraud** and **systems security**. Examples of *theft and fraud* include robbery and forgery, while examples of *systems security* include hacking and stealing information, and cybersecurity breaches. Managing cyber risk has become especially important for firms given the rise of digitization and remote work during the COVID-19 pandemic period, resulting in a significant increase in external fraud relating to wire transfers, email scams, and phishing exercises.

Definitions of Money Laundering and Terrorism Financing

The European Directive of the European Parliament and Council defines **money laundering (ML)** as the action of organizing, facilitating, or concealing criminal activities, and to convert funds in an effort to conceal their origin. **Terrorism financing (TF)** refers to providing or using funds with the intent or knowledge that they will be used for terrorist activities. **Anti-money laundering (AML)** and anti-TF activities deal with detecting and preventing these illegal activities from happening.

Financial Crime Risk Management

Many firms monitor financial crimes through internal audits and inspections with the goal of detecting, monitoring, and reporting fraud. Most firms have *zero tolerance* for internal fraud, meaning that if offenders are caught, they will be punished or sanctioned.

Internal Fraud Management

There are four key controls of an internal fraud risk management framework:

1. *Selection*: Banks need to adequately screen employees as well as contractors and third parties during the onboarding process, using proper due diligence practices. Selecting the right people with strong ethical standards reduces risk across the firm.
2. *Prevention*: By segregating specific duties, limiting access rights and authorizations, and delegating authorities to specific people, banks establish key controls relating to fraud prevention.
3. *Detection*: When internal controls and fraud detection are strong, the risk of being caught is high, and the incentive to commit fraud is low. Detection relies on strong

team supervision, and adequate monitoring, reconciliation, and reporting of unusual activity.

4. *Deterrents*: The key deterrents against fraud are sanctions, lawsuits, and disciplinary actions.

External Fraud Management

Managing external fraud is fairly similar to managing internal fraud management, with the key difference that the focus is not on employees but on criminals as well as potential fraud by customers, business partners, and other third parties. Examples of external fraud include bank robbery, fraudulent transactions, credit card fraud, and identity theft. It can also include intentionally misrepresenting or misstating income, assets, and collateral values (in loan applications).

External fraud management can focus on *first-party fraud* (fraud committed by customers and partners for their own gain) or *third-party fraud* (other external parties committing fraud). Banks often engage special teams to assist with fraud management, including hiring security to monitor ATMs and branches against robbery or partnering with law enforcement following an incident.

AML Risk Management

AML risk management is important for preventing criminals from using the banking system for money laundering. Before we discuss the steps in AML risk management, it is important to understand the three phases of money laundering:

1. *Placement*: The first step is to disguise the criminal origins of the funds by placing them in the legal financial system (typically using cash transfers and false invoicing) through trusts and offshore companies. Criminals often use **smurfing**, a technique involving a series of small transactions instead of a few large transactions, in order to remain undetected and below the threshold for AML reporting.
2. *Layering*: The second phase in money laundering involves trying to obscure the original source of funds and audit trail as much as possible, and to make AML controls difficult, through a series of complex transactions using multiple accounts.
3. *Integration*: The last phase in money laundering involves integrating the illegal funds back into the economy through legitimate means including asset purchases. Integration can also involve making fake payments to employees, fake loans, or fake dividend payments to create the illusion of legitimacy.

Similar to internal fraud management, the AML risk management framework also has four control steps in order to minimize the risk of money laundering:

1. *Selection*: Firms need to adequately profile and select their customers. One of the most critical steps is the **know your customer (KYC)** due diligence process, which involves verifying a customer's identity. Verifying the origins of customer funds and deposits is another key step, including verification that the funds are not connected to organized crime or other criminal activities.
2. *Prevention*: Prevention should follow a risk-based approach to AML risk, by implementing tight risk controls with proper employee training. Financial institutions will often categorize customers by level of risk (e.g., low, medium, or high risk). The factors that determine the risk classification include the customer's occupation, volume and frequency of activity, history with the bank, documentation,

and whether the customer is classified as a **politically exposed person (PEP)**, which requires additional due diligence.

3. *Detection*: Strong detection relies on strong overall governance, a good transaction monitoring system, and alerts of abnormal activity. Risk overview is often delegated to a dedicated money laundering risk officer, with monitoring aided by well-written and clear policies, proper training, and ongoing reviews of customer data. Customer data should be reconciled against external lists, including sanctions lists.
4. *Deterrents*: The key deterrents against money laundering include lawsuits, closing customer accounts, or referring customer information to financial and intelligence agencies.

These controls are especially important given the recent proliferation of **regulation technology (RegTech)** companies that use automated customer profiling, which relies on machine learning techniques in the KYC process. These automated techniques help speed up the verification and onboarding processes, especially relating to verifying lists for PEPs and detecting unexplained changes in customer behavior and banking patterns. Fully digitalized, online banks called **challenger banks**, greatly rely on these automation and machine learning techniques in the KYC process, although regulators have scrutinized the effectiveness and quality of their controls.

Several regulatory agencies publish **sanctions lists**, including The Office of Foreign Assets Control (OFAC, part of the U.S. Treasury Department). The list includes the names of sanctioned individuals and companies and terrorists and narcotics traffickers. All companies doing business in or with the United States must ensure that their clients are not on the sanctions list.

USAA Federal Savings Bank Case Study

LO 45.b: Summarize the regulatory findings and describe the lessons learned from the USAA case study.

In March 2022, **USAA Federal Savings Bank (USAA FSB)** was fined \$140 million by U.S. federal regulators, including the Financial Crimes Enforcement Network (FinCEN) and the Office of the Comptroller of the Currency (OCC), the national banking regulator. The penalty was in response to at least five years (between 2016 and 2021) of an ineffective AML program that did not meet the minimum requirements of the Bank Secrecy Act (BSA) and AML standards. In fact, the regulators noted that the bank “willfully” failed to ensure that it adequately monitored suspicious activities or reported them to regulators as its compliance program failed to keep pace with its account growth.



PROFESSOR'S NOTE

USAA FSB is a division of USAA (United Services Automobile Association), a Texas-based financial services group founded in 1922 and primarily servicing U.S. military members. USAA FSB provides the banking services of USAA.

Due to staffing shortages, the bank used third-party contractors to help monitor its accounts for suspicious and potentially criminal activity; however, it failed to

adequately train these contractors in AML compliance matters. In addition, the bank introduced a new transaction monitoring system in 2021 that would issue an alert of potentially suspicious activities and flag them for review. However, the new system proved to be overly sensitive and created an exceptionally high number of alerts that the bank could not manage. By the end of 2021, there were close to 90,000 unreviewed alerts and nearly 7,000 unreviewed cases.

What is interesting about the fines is that they were not imposed because of known thefts or AML cases at USAA FSB, but because of a lack of adequate controls over AML risk and an ineffective AML program. The USAA FSB case is one of a growing number of cases globally where regulators levied fines on financial institutions for failure to demonstrate adequate AML controls or for having poorly designed risk management systems. Following regulatory sanctions, institutions are often subject to costly AML remediation programs (called **lookbacks**) in which the institution is required to review and verify all client information and report suspicious activity or even close accounts.

Having adequate controls is especially important given that the COVID-19 pandemic altered consumer and business behavior, including a rise in remote transactions that are more difficult to monitor. When monitoring uses automated detection and alerts, institutions must ensure that these alerts do not create a large number of false positives or false negatives, and that the number of alerts are manageable with adequate monitoring, assessment, and feedback.



MODULE QUIZ 45.1

1. The risk manager of a regional U.S. commercial bank flags one of the business accounts for potential smurfing. Which of the following descriptions most likely reflects the activity that the manager flagged?
 - A. The account holder made a series of large withdrawals from the account.
 - B. The account holder made a series of frequent small deposits into the account.
 - C. The account was closed and reopened multiple times in a short period of time.
 - D. The account holder made a very large deposit into the account, well above the anti-money laundering (AML) reporting threshold.
2. Which of the following steps is not one of the phases in money laundering?
 - A. Conversion.
 - B. Integration.
 - C. Layering.
 - D. Placement.
3. Monitoring for abnormal activities and behavior is best associated with which of the following components of the risk management framework?
 - A. Detection.
 - B. Deterrents.
 - C. Prevention.
 - D. Selection.
4. Which of the following reasons best represents why USAA Federal Savings Bank (USAA FSB) was fined \$140 million by regulators in 2022?
 - A. A backlog of unreviewed cases and alerts led to a significant theft of funds in 2021.
 - B. Systematic money laundering by third parties led to a significant loss over a decade.

- C. Previously flagged deficiencies by the regulators have not been satisfactorily addressed.
- D. USAA FSB demonstrated a persistent deficiency in its anti-money laundering (AML) controls.

KEY CONCEPTS

LO 45.a

Financial crime includes internal and external fraud, money laundering, and terrorism financing, and is defined as “any kind of criminal conduct relating to money or to financial services or markets, including any offense involving: (a) fraud or dishonesty; or (b) misconduct in, or misuse of information relating to, a financial market; or (c) handling the proceeds of crime; or (d) the financing of terrorism.”

Internal fraud is defined as “losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/discrimination events, which involve at least one internal party.” Internal fraud includes unauthorized activities (e.g., employees knowingly disregarding or violating laws and policies) and theft and fraud (e.g., stealing or dishonest use of assets).

External fraud is defined as “losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party.” External fraud includes theft and fraud (e.g., robbery and forgery) and systems security (e.g., hacking and stealing information, and cybersecurity breaches).

Money laundering is defined as the action of organizing, facilitating, or concealing criminal activities and converting funds in an effort to conceal their origin. There are three distinct phases of money laundering: (1) placement, (2) layering, and (3) integration. Terrorism financing is defined as providing or using funds with the intent or knowledge that they will be used for terrorist activities.

Internal fraud management includes four key controls: (1) selection, (2) prevention, (3) detection, and (4) deterrents. External fraud management includes the same controls, with the key difference that the focus is on criminals and potential fraud by customers, business partners, and other third parties. External fraud management can focus on first-party fraud (i.e., fraud committed by customers and partners) or third-party fraud (i.e., other external parties committing fraud).

Anti-money laundering (AML) risk management deals with detecting and preventing money laundering and terrorism financing activities from happening, and preventing criminals from using the banking system for money laundering. The AML process has four control steps: (1) selection, which includes the know your customer (KYC) due diligence process, (2) prevention, (3) detection, and (4) deterrents.

AML controls are especially important given the rise of RegTech companies and challenger banks (fully digitalized, online banks), which use automated customer profiling that relies on automation and machine learning techniques in the KYC process. Regulators have scrutinized the effectiveness and quality of the controls of challenger banks.

Several regulatory agencies publish lists of sanctioned individuals and companies, and terrorists and narcotics traffickers. Companies must ensure that their customers are not on the sanctioned lists.

LO 45.b

The March 2022 regulatory fine of the USAA Federal Savings Bank (USAA FSB) was in response to the bank's failure to ensure that it met the minimum requirements of the Bank Secrecy Act (BSA) and AML standards, and its failure to ensure adequate monitoring and reporting of suspicious activities. The regulatory fines were imposed due to a lack of adequate controls over AML risk and an ineffective AML program, not because of known thefts or losses.

The number of regulatory sanctions globally is growing. Following sanctions, institutions typically need to undertake AML remediation programs (lookbacks) to review and verify all client information and report suspicious activity. Adequate AML controls are critical. When monitoring uses automated detection and alerts, the number of alerts must be manageable.

ANSWER KEY FOR MODULE QUIZ

Module Quiz 45.1

1. **B** Smurfing occurs within the placement phase of money laundering. It refers to making a series of small transactions (e.g., deposits) instead of a few large transactions to remain within the AML reporting threshold. (LO 45.a)
2. **A** The three phases in money laundering are placement, layering, and integration. (LO 45.a)
3. **A** The detection component of the risk management framework involves instituting adequate detection controls to limit fraud, including through proper team supervision and monitoring for abnormal activities and behavior. (LO 45.a)
4. **D** USAA FSB was fined by regulators in 2022 not because of any specific case of fraud or theft, but because it demonstrated inadequate risk controls including a persistent weakness in its AML practices and risk management that exposed it to significant risk. (LO 45.b)

¹ "Financial Crime," Financial Conduct Authority, accessed December 19, 2022, <https://www.handbook.fca.org.uk/handbook/glossary/G416.html>.

² "Operational Risk Data Collection Exercise – 2002," Basel Committee on Banking Supervision, accessed December 19, 2022, <https://www.bis.org/bcbs/oprdata.pdf>.

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 assigned reading—Board of Governors of the Federal Reserve System.

READING 46

GUIDANCE ON MANAGING OUTSOURCING RISK

Study Session 8

EXAM FOCUS

This short and nontechnical reading begins by examining the general risks arising from a financial institution's use of service providers. It then provides details on the key elements of an effective service provider risk management program. For the exam, focus on the three broad areas of due diligence. Also, be familiar with the details from the numerous contract provisions that should be addressed with third-party service providers.

MODULE 46.1: MANAGING OUTSOURCING RISK

LO 46.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.

Risks of Outsourcing Activities to Third-Party Service Providers

The following risks could arise when a financial institution outsources its operational functions to third-party service providers:

- **Compliance risk** refers to a service provider not operating in compliance with the relevant local laws and regulations.
- **Concentration risk** refers to having very few service providers to choose from or that the service providers are clustered in only a few geographic areas.
- **Reputational risk** refers to a service provider executing its tasks in a substandard manner, resulting in a negative public perception of the financial institution.
- **Country risk** refers to using a service provider based in a foreign country and subjecting the financial institution to potential economic and political risks in that country.

- **Operational risk** refers to potential losses sustained by a financial institution as a result of internal control breaches and human error caused by a service provider.
- **Legal risk** refers to subjecting the financial institution to lawsuits and other costs due to potentially negligent activities of a service provider.

Effective Program to Manage Outsourcing Risk

The risk management program with service providers needs to contain adequate oversight and controls over activities that have a material impact on the institution's finances and operations. In addition, importance must be placed on activities relating to sensitive customer information and new products and services. The depth and complexity of the program may be relatively low if there are few outsourced activities, and the service providers are established and reliable. Conversely, the depth and complexity may be relatively high if there are many service providers involved in outsourced activities.

Risk management programs should include (1) risk assessments, (2) due diligence in selecting service providers, (3) contract provisions, (4) incentive compensation review, (5) oversight and monitoring of service providers, and (6) business continuity and contingency plans.

The last five elements will be discussed in subsequent sections. The crucial first step is to perform **risk assessments** of the applicable business activities to determine whether these activities are best executed in-house or by a third party. Assuming the outsourcing option is consistent with the financial institution's business objectives, then a cost-benefit analysis and a risk analysis of the service provider should be performed. Two key questions to be answered include the following: (1) Do qualified and experienced service providers exist? (2) Is the financial institution sufficiently qualified to perform oversight duties and manage the relationship with the service provider? Risk mitigation techniques should be updated on a sufficiently regular basis as a result of updated risk assessments.

Due Diligence on Service Providers

LO 46.b: Explain how financial institutions should perform due diligence on third-party service providers.

In performing due diligence on a third-party service provider, a financial institution should involve any relevant technical specialists and/or important stakeholders. The three key areas of review include (1) business background, reputation, and strategy; (2) financial performance and condition; and (3) operations and internal controls. Ultimately, the financial institution must ensure that the service provider follows all relevant laws and regulations in performing services on the institution's behalf.

Business Background, Reputation, and Strategy

There should be a review of the potential service provider's past business history and of its key management personnel. The service provider should provide evidence of an

adequate background check system for its new employees.

A review of the service provider's experience, strategy and mission statement, service philosophy, methods of maintaining and improving quality, and company policies is needed. The flexibility and feasibility of the service provider's business model should be evaluated to determine the likelihood of providing services to the financial institution for the long term.

References should be contacted and confirmed, and any licenses and certifications necessary to perform the services should be confirmed. A search for any past or present legal and compliance problems should also be undertaken.

Financial Performance and Condition

The service provider's most recent financial statements (and annual report, if applicable) should be obtained to analyze its assets, liabilities, liquidity, and operating performance for sufficiency. Financial information of any subcontractors should be obtained and analyzed for the same reason. The expected financial impact of the potential contract on the service provider should be determined.

The service provider's long-term survival prospects should be analyzed by considering how long it has been operating as well as its market share growth. Furthermore, its ability to provide the service for the length of the contract in terms of capital and personnel needs to be ascertained. Finally, the amount of insurance coverage and any other issues that may impact the service provider's finances should be considered.

Operations and Internal Controls

The service provider's internal controls, IT systems development and support, IT security systems, and methods of securing confidential information should be evaluated. Additionally, there should be a review of the service provider's staff training, analysis of the service support provided, and confirmation that employee background checks are being performed. Finally, queries should be made about the process involved in maintaining records and any disaster recovery processes in place.

Contract Provisions

LO 46.c: Describe topics and provisions that should be addressed in a contract with a third-party service provider.

Considerations and contract provisions for third-party service providers should include the following elements:

Scope. A contract will state the rights and responsibilities of each party. Examples include (1) contract duration, (2) support, maintenance, and customer service, (3) training of financial institution employees, (4) policies regarding subcontracting, (5) insurance coverage, and (6) policies regarding the use of the financial institution's assets and employees.

Cost and compensation. A contract should indicate the party (or parties) responsible for the payment of any equipment purchases, legal fees, and audit fees pertaining to the service provider's activities. In addition, there should be a listing of all forms of compensation (i.e., fixed, variable, special charges).

Incentive compensation. A contract should include a provision to allow the financial institution to review the appropriateness of incentive compensation (if applicable). Specifically, the service provider may be involved in sales on behalf of the financial institution. Therefore, the incentives should be structured to ensure that the service provider places the interests of the customers (i.e., suitable financial products) over their own interests (i.e., earning higher fees) and to ensure that the service provider does not expose the financial institution to excessive risks.

Right to audit. A contract could optionally contain a provision to allow the financial institution to audit the service provider. It may also require the receipt of various audit reports (e.g., American Institute of Certified Public Accountants [AICPA] Service Organization Control 2 report, Federal Financial Institutions Examination Council [FFIEC] Technology Service Provider examination report) relating to the service provider at stipulated intervals.

Establishment and monitoring of performance standards. A contract should state specific and measurable performance standards (i.e., metrics) with regard to the service provider's work.

Oversight and monitoring. A contract should include a provision requiring the service provider to provide annual financial statements (and the annual report, if applicable) to the financial institution to allow the financial institution to monitor the service provider's ability to continue as a going concern. In addition, a provision should be included to allow the financial institution to increase monitoring and oversight activities when performance deficiencies, control weaknesses, and viability concerns are noted. With regard to higher-risk service providers, a contract could stipulate extra reporting by the service provider or additional monitoring by the financial institution.

Confidentiality and security of information. A contract must contain extensive provisions concerning the confidentiality and security of information pertaining to both the financial institution and its customers. The service provider should only be given such information that is necessary to perform its tasks. Specifically, in the United States, the FFIEC guidance and section 501(b) of the Gramm-Leach-Bliley Act must be followed and should be noted in the contract.

With regard to nonpublic personal information (NPPI) pertaining to the financial institution's customers, a contract should address access, security, and retention of NPPI data by the service provider (if applicable) to comply with privacy laws and regulations. A contract should also require the service provider to give notice to the financial institution of any breaches of data. In that regard, a contract needs to clarify the parties' roles and responsibilities pertaining to NPPI data.

Ownership and license. A contract should state when service providers are permitted to use the financial institution's property (i.e., data and equipment). In addition, clarification is needed regarding the ownership and control of data produced by a service provider. In the event of software purchased from a service provider, it could be

necessary to have escrow agreements in place so that the financial institution could access the source code and programs under certain conditions, such as discontinued product support or insolvency of a service provider.

Indemnification. A contract should require the service provider to indemnify (i.e., hold harmless) the financial institution in the event of any legal proceedings arising from the service provider's negligence.

Default and termination. A contract should clarify the types of actions that would constitute a default together with any reasonable remedies that could be undertaken by the financial institution and methods to overcome default by the service provider. In terms of termination, common reasons, such as change in control, poor performance, and nonperformance of duties, should be explained and measured. There should be a provision that requires the service provider to give sufficient notice of termination to the financial institution in the event of a termination by the service provider. Finally, it is important to include provisions detailing the service provider's requirement to return the financial institution's data, records, and any other property.

Dispute resolution. A contract should lay out an agreed-upon dispute resolution plan to resolve disputes quickly and minimize disruption during a dispute.

Limits on liability. A contract may allow for service providers to limit their liability subject to approval by the financial institution's board of directors and management team.

Insurance. A contract should stipulate the requirement of service providers to carry sufficient insurance and provide evidence of coverage. In addition, any significant changes in coverage should be communicated to the financial institution.

Customer complaints. A contract should state which party will deal with customer complaints. If it is the service provider, then they should be required to prepare reports to the financial institution listing the complaints and their status.

Business resumption and contingency plan of the service provider. A contract should detail how the service provider will continue to provide services should a major disaster occur. The focus should be on critical services and any necessary alternative arrangements. Other items, such as backups, disaster recovery and business continuity plans, responsibility for maintaining and testing of such plans, and frequency of testing of such plans, should be included.

Foreign-based service providers. A contract could attempt to provide for the law and regulations of only one jurisdiction (i.e., the financial institution's) to apply for the purposes of contract enforcement and resolution of disputes. This would avoid potentially confusing situations where the foreign laws differ substantially from local laws.

Subcontracting. The subcontractor should be held to the same contract terms in the event that subcontracting is permitted. The contract should explicitly state that the primary service provider is ultimately responsible for all the work performed by the service provider and its subcontractors. The contract should provide a list of acceptable tasks that may be subcontracted and how the primary service provider will supervise and review the subcontractor's work. Finally, the primary service provider's

method of performing financial due diligence on the subcontractor should be documented in the contract.



MODULE QUIZ 46.1

1. Bank Inc., (Bank) operates in the United States and has a service contract in place with Service Co. (Service), which operates in France. Service manages a significant amount of confidential customer data for Bank, and recently a computer glitch at Service resulted in the accidental public disclosure of confidential customer data. As a result of the data breach, which of the following risks is Bank least likely to face?
 - A. Compliance risk.
 - B. Country risk.
 - C. Legal risk.
 - D. Operational risk.
2. Which of the following statements regarding risk management programs with service providers to manage outsourcing risk is correct?
 - A. The program should focus on business continuity and contingency plans.
 - B. The program should contain more detail if there are only a few outsourced activities to established service providers.
 - C. The program should contain adequate oversight and controls over all activities that impact the financial institution.
 - D. The program should require risk assessments to be updated as a result of updated risk mitigation techniques on a sufficiently regular basis.
3. When performing due diligence on a service provider, ascertaining the sufficiency of its insurance coverage would most appropriately be covered under which of the following categories?
 - A. Business background, reputation, and strategy.
 - B. Financial performance and condition.
 - C. Operations and internal controls.
 - D. Oversight and monitoring.
4. The use of performance metrics to assist in determining an acceptable level of performance by a service provider would most appropriately be included in which of the following provisions of a contract with a financial institution?
 - A. Customer complaints.
 - B. Default and termination.
 - C. Indemnification.
 - D. Right to audit.
5. Which of the following provisions would a financial institution least likely include in a contract with a third-party service provider?
 - A. Establishment and monitoring of performance standards.
 - B. Indemnification.
 - C. Ownership and license.
 - D. Right to audit.

KEY CONCEPTS

LO 46.a

The following risks could arise when a financial institution outsources its operational functions to third-party service providers: (1) compliance risk, (2) concentration risk,

(3) reputation risk, (4) country risk, (5) operational risk, and (6) legal risk.

An effective program to manage outsourcing risk should include (1) risk assessments, (2) due diligence in selecting service providers, (3) contract provisions, (4) incentive compensation review, (5) oversight and monitoring of service providers, and (6) business continuity and contingency plans.

LO 46.b

In performing due diligence on a third-party service provider, a financial institution should involve any relevant technical specialists and/or important stakeholders. The three key areas of review include (1) business background, reputation, and strategy; (2) financial performance and condition; and (3) operations and internal controls.

LO 46.c

Considerations and provisions that should be addressed in a contract with a third-party service provider include the following: (1) scope, (2) cost and compensation, (3) incentive compensation, (4) right to audit, (5) establishment and monitoring of performance standards, (6) oversight and monitoring, (7) confidentiality and security of information, (8) ownership and license, (9) indemnification, (10) default and termination, (11) dispute resolution, (12) limits on liability, (13) insurance, (14) customer complaints, (15) business resumption and contingency plan of the service provider, (16) foreign-based service providers, and (17) subcontracting.

ANSWER KEY FOR MODULE QUIZ

Module Quiz 46.1

1. **B** Country risk refers to using a service provider based in a foreign country and subjecting the financial institution to potential economic and political risks in that country. Clearly, it is not a relevant risk arising from the breach of confidential customer data.

Compliance risk is a possibility given the apparent lack of security controls of the service provider that resulted in the data breach. Operational risk is clearly a relevant risk to the financial institution here given the data breach caused by the service provider. Legal risk is clearly a relevant risk given that the customers affected by the data breach may sue the financial institution as a result of the breach. (LO 46.a)

2. **A** Unexpected events could result in the inability of the service provider to provide its services to the financial institution. Depending on the nature and importance of the services provided, the financial institution may be exposed to substantial losses as a result of the inability of the service provider to provide its services. Therefore, business continuity and contingency plans should be a key focus in any risk management program with service providers.

The program should contain *less* detail if there are only a few outsourced activities to established service providers given that the risk to the financial institution would be reduced substantially as a result of the service provider being established. The program should *not* deal with all activities that impact the financial institution but instead focus only on those that have a material impact.

The program should require risk mitigation techniques to be updated on a sufficiently regular basis as a result of updated risk assessments. (LO 46.b)

3. **B** A review of a potential service provider's financial performance and condition would include queries regarding its level of insurance coverage.

The area of business background, reputation, and strategy takes a more global view of the service provider and would be far less concerned with financial matters such as insurance. Operations and internal controls deal with compliance with relevant laws and regulations, for example, and would be less concerned with financial matters such as insurance. Oversight and monitoring is not an element within the due diligence process, but it is one of the elements (together with due diligence) of an effective risk management program with service providers. (LO 46.b)

4. **B** With regard to the default and termination provision, common reasons include poor performance and nonperformance of duties, which would be detected through the use of performance metrics. The customer complaints provision deals with which party will deal with customer complaints. The indemnification provision deals with the service provider to indemnify the financial institution in the event of any legal proceedings arising from the service provider's negligence. The right to audit provision deals with allowing the financial institution to audit the service provider. (LO 46.c)

5. **D** The right to audit provision is optional and is the least important provision of the four listed. The use of performance standards is essential for monitoring and oversight purposes that may result in the determination of default by the service provider and possible termination of the contract. The indemnification provision is important because it deals with the service provider indemnifying (i.e., holding harmless) the financial institution in the event of any legal proceedings arising from the service provider's negligence. The ownership and license provision is crucial because it would state when service providers are permitted to use the financial institution's property (i.e., data and equipment) as well as clarify the ownership and control of data produced by a service provider. (LO 46.c)

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 13.

READING 47

CASE STUDY: THIRD-PARTY RISK MANAGEMENT

Study Session 8

EXAM FOCUS

Most firms deal with third parties in some capacity, whether relating to third-party vendor arrangements, contractors, or other service providers. This reading discusses the risk management of these relationships (defined as third-party risk management, or TPRM), and aims to assess, address, and monitor risks including service quality issues, fraud, compliance breaches, and leaks, among others. This is followed by a discussion of the life cycle stages of TPRM. The reading presents several recent case studies of breakdowns in TPRM relating to third-party vendor issues, such as data breaches. Note that although firms may transfer key functions to third (and fourth) parties, ultimate responsibility and accountability is not transferable.

MODULE 47.1: THIRD-PARTY RISK MANAGEMENT AND RESPONSIBILITIES

LO 47.a: Explain how risks related to the use of third parties can arise and describe characteristics of an effective third-party risk management framework.

Overview of Third-Party Risk Management

Most organizations have some component of their business that is outsourced to outside, or third-party, entities. Third-party entities include vendors, contractors, service providers (including cloud hosting services), suppliers, and business partners. Managing the risks that could arise from using third parties is part of **third-party risk management (TPRM)** and includes identifying, monitoring, and assessing these risks.

There are two key reasons to contract with third parties: (1) to save costs by outsourcing to firms that specialize in certain activities, and therefore have a competitive advantage in terms of systems and processes, and (2) to mitigate operational and other risks by contracting with experts that could reduce process and data errors.

TPRM does not just apply to third parties. It can apply to the entire supply chain, extending to *fourth parties* (third parties of third parties) and even *fifth parties* (third parties dealing with contractors who deal with other entities). Key third-party (and fourth-party, etc.) risks include the same risks that could impact any organization, including service quality issues, service disruptions, fraud, data and compliance breaches, leaks of sensitive or confidential information, intellectual property theft, and even espionage.

The risks of dealing with third parties, and therefore the importance of TPRM, has grown significantly in the last few years as organizations increasingly outsource their core processes to third parties. For example, financial firms like banks have been increasingly outsourcing to third parties their loan and mortgage processing and servicing, electronic fund transfer, payroll and treasury management operations, as well as electronic bill payments and account aggregation. Many of these third parties are located in countries external to the firm, which introduces additional layers of risks including country risk and legal and compliance risks.

The widespread application of Internet of Things (IoT) devices and the COVID-19 pandemic accelerated outsourcing arrangements and the use of third parties. Storing and protecting sensitive data has become complex—but as the case of the self-service convenience market Avanti Markets illustrates, which was hacked through its vending machines, ensuring data privacy protection and information security is critical to organizations. A recent study found that nearly 60% of firms surveyed experienced a data breach through their third parties, including vendors. Another study found that most (77%) firms have limited visibility into their third parties, and 80% have experienced at least one breach related to third parties in the last year.

The TPRM Life Cycle

The TPRM process has five life cycle stages:

1. Business model decision
2. Evaluation, risk rating, and due diligence
3. Contracts, service level agreements, and contract management
4. Ongoing monitoring
5. Remediation or termination

Business model decision. The first step in the TPRM process is to decide whether and which activities should be outsourced to third parties instead of keeping them in-house. This decision depends in part on the firm's risk appetite.

Evaluation, risk rating, and due diligence. Evaluating new third-party relationships requires proper due diligence, including an understanding of who is the firm's business partner. Due diligence should be done on the basis of proportionality, meaning that long-term, more complex third-party arrangements (e.g., with a cloud hosting vendor) would require more due diligence and verification than short-term, less complex arrangements (e.g., with a consultant doing a one-day training course for the firm's employees).

Contracts, service level agreements, and contract management. Contracts and service level agreements (SLAs, or vendor agreements) are important in TPRM when dealing with vendors and other third parties because they formally and clearly lay out the

responsibilities and expectations of each party. Clearly defined contracts reduce ambiguity by defining the quality and timing of agreements, what can and cannot be done, and who is responsible for specific tasks and functions.

Before contracts and agreements are signed, best practice is to assess and remediate all existing open issues. In addition, contracts should be periodically reviewed, and deficiencies should be addressed.

Contract management becomes especially important when managing offshore vendor relationships. For example, during the COVID-19 pandemic, many U.S. and European organizations with offshore call centers in India and the Philippines had to change their contracts to allow third-party employees to work fully remote. However, organizations should establish limits on outsourcing to third-party vendors, which should include limits on outsourcing to vendors and fourth parties. Organizations should have audit rights on vendors as part of their continuous monitoring.

Ongoing monitoring. Monitoring is an important component of TPRM to assess third-party and other outsourced relationships. The more robust the first few steps of the TPRM life cycle are, the less need there is for reassessment and review of the cycle. Within the monitoring step, reassessments should be tied not only to calendar reviews that occur at predetermined times—they should also be tied to triggers including data breaches and incidents, legal or regulatory changes, and changes in business circumstances including mergers or acquisitions. The COVID-19 pandemic also highlighted the need to include *acts of god*, defined as natural unavoidable circumstances, into the monitoring process. Triggers should also provide organizations with an effective exit strategy.

Remediation or termination. Third-party relationships typically end when contracts end. However, it is good practice to include a grievance period and an exit strategy or a termination clause, which allows firms to terminate contracts when processes wind down, when circumstances dictate, or when regulations change. The proper transfer of intellectual property from third parties to in-house should be well defined.

Third-Party Case Studies

LO 47.b: Describe the lessons learned from the case study involving a data breach caused by a third-party vendor employee.

There are two interesting case studies discussed in this section relating to vendor risk management: (1) a data breach at the bank **Capital One** by a former third-party vendor employee, and (2) weak third-party controls at the financial services company **Morgan Stanley**. Both cases highlight the relationship between data security and TPRM. They also illustrate that the ultimate responsibility for any risks rests with the institution using third-party vendors because that accountability is not transferable.

Capital One

The Capital One case relates to a breach of the bank's data through Amazon Web Services (AWS), the third-party cloud services provider used by Capital One. In July

2019, the bank reported that a former AWS employee had gained access and stole data from 100 million U.S. bank customers (and many international), including accessing 140,000 Social Security numbers and 80,000 bank accounts. The employee was able to gain access to files stored on the AWS database by taking advantage of a weakness in the system's firewall. While both Capital One and AWS knew that their systems were vulnerable to this type of attack, they continued to use unencrypted data, which enabled the employee to immediately use the stolen data.

Capital One was fined \$80 million in 2020 by a U.S. banking regulator, the Office of the Comptroller of the Currency (OCC), for failing to adequately identify and manage risks before the breach related to its vendor services, including moving data to the cloud involving AWS. The OCC noted that well before the breach, Capital One had weak risk management controls and failed to detect and address vulnerabilities—even a 2015 internal audit failed to detect several control weaknesses.

Morgan Stanley

In 2020, the OCC also fined Morgan Stanley \$60 million for risk management deficiencies relating to third-party vendors and relating to the decommissioning of two of its wealth management business data servers.

Specifically, the OCC noted that both in 2016 and in 2019, Morgan Stanley (1) failed to properly assess and address the risks related to decommissioning its hardware, (2) failed to properly assess the risk of using third-party vendors and subcontractors or adequately monitor their performance, and (3) failed to maintain a proper inventory of customer data. The fine was levied after Morgan Stanley began to notify its wealth management customers in July 2019 that the computer hardware the company disposed of still contained confidential customer data.



MODULE QUIZ 47.1

1. Establishing limits on third-party and fourth-party vendor outsourcing would be considered under which of the following third-party risk management (TPRM) steps?
 - A. Business model decision.
 - B. Remediation or termination.
 - C. Evaluation, risk rating, and due diligence.
 - D. Contracts, service level agreements, and contract management.
2. Which of the following tasks is not one of the life cycle stages of third-party risk management (TPRM)?
 - A. Business model decision.
 - B. Evaluation, risk rating, and due diligence.
 - C. Management of third- and fourth-party vendor relationships.
 - D. Contracts, service level agreements, and contract management.
3. A key conclusion from the Capital One and Morgan Stanley case studies is that accountability for operational risk:
 - A. is not transferable.
 - B. ultimately rests with the third-party vendor.
 - C. ultimately rests with either the third-party vendor or subcontractor, whichever experienced the risk control problem.

D. is a fully shared responsibility between the company using third-party vendors and the third-party vendors themselves.

KEY CONCEPTS

LO 47.a

Third-party risk management, or TPRM, relates to identifying, monitoring, and assessing the risks that arise from using third parties. Firms typically use third parties to save costs by outsourcing to third parties that specialize in certain activities, and to reduce risks by contracting with experts. TPRM applies to the entire supply chain and extends to fourth and fifth parties.

Key risks include service quality issues, service disruptions, fraud, data and compliance breaches, leaks of sensitive or confidential information, intellectual property theft, and even espionage. Third parties located in countries external to the firm introduce additional layers of risks, including legal and compliance risks—which should be monitored. TPRM should also include storing and protecting sensitive data and ensuring data privacy protection and information security.

The TPRM life cycle has five stages:

1. Business model decision: This is the first stage in the TPRM, and it determines whether and which activities should be outsourced to third parties.
2. Evaluation, risk rating, and due diligence: Due diligence is used to evaluate risks and relationships with third parties and should be done on the basis of proportionality (more complex and longer-term relationships should have more due diligence).
3. Contracts, service level agreements, and contract management: This stage lays out the responsibilities and expectations of each party to reduce ambiguity. Contracts should be periodically reviewed, and deficiencies should be addressed.
4. Ongoing monitoring: Continuous monitoring of third-party and other outsourced relationships is necessary. Reassessments should be tied to specific triggers.
5. Remediation or termination: Remediation strategies should include a grievance period and an exit strategy, or a termination clause that allows firms to terminate contracts.

LO 47.b

The case studies in this reading highlight risk management breakdowns relating to third-party vendor risk management and controls at Capital One and at Morgan Stanley. They underscore that although certain functions can be transferred to third parties, ultimate accountability is not transferable.

ANSWER KEY FOR MODULE QUIZ

Module Quiz 47.1

1. **D** The third phase in the life cycle of TPRM relates to contracts, service level agreements, and contract management. This phase includes establishing and defining the terms of contracts for third-party (or fourth-party) arrangements, including establishing standards or limits on outsourcing. (LO 47.a)

2. **C** The TPRM process has five steps: (1) business model decision, (2) evaluation, risk rating, and due diligence, (3) contracts, service level agreements, and contract management, (4) ongoing monitoring, and (5) remediation or termination. Management of third- and fourth-party vendor relationships is an overall component of TPRM and not a specific life cycle stage. (LO 47.a)
3. **A** The accountability for risk control problems rests with the company that uses third-party vendors. Although third-party vendors and subcontractors should share some of the blame for risk control breakdowns, the ultimate responsibility rests with the company that outsources its services to third parties. (LO 47.b)

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 14.

READING 48

CASE STUDY: INVESTOR PROTECTION AND COMPLIANCE RISKS IN INVESTMENT ACTIVITIES

Study Session 8

EXAM FOCUS

This reading looks at the nature of regulatory compliance globally and the key determinations when designing regulations, including investor protection, accountability against fraud, fostering global cooperation, and enhanced due diligence. Two key regulations discussed are the European Union (EU) regulation Markets in Financial Instruments Directive (MiFID) and its later update, MiFID II, and the U.S. Investor Protection Act as part of the broader Dodd-Frank Act. The reading concludes with three case studies of regulatory fines levied against global investment firms for compliance breaches, market manipulation, and failure to ensure best execution for customers.

MODULE 48.1: INVESTOR PROTECTION REGULATIONS

LO 48.a: Summarize important regulations designed to protect investors in financial instruments, including MiFID, MiFID II, and Dodd-Frank.

Investor protection regulations exist to ensure that investors are adequately informed about the parameters and risks of financial transactions. The United States and the EU have been at the forefront of not only creating and enacting legislation, but also imposing fines on entities that are not in compliance. Regulations are also designed to protect investors against misrepresentation, facilitate global cooperation, ensure accountability against fraud, and ensure that adequate know your customer (KYC) due diligence is followed to protect against improper business practices.

Regulatory compliance largely falls into two categories that focus on clients, products, and business practices: (1) suitability, disclosure, and fiduciary responsibilities, and (2) improper business and market practices.

Markets in Financial Instruments Directive

The EU **Markets in Financial Instruments Directive (MiFID)** was originally enacted in 2004 and was implemented across the EU in 2007. MiFID is an investor protection regulation that describes proper business and organizational conduct and prescribes regulatory disclosure and reporting requirements to prevent market abuse.

The original MiFID regulation was revised following the 2007–2009 financial crisis to improve public disclosure requirements for trading data to strengthen investor protection. The revised directive, **MiFID II**, came into force in 2014, with the accompanying regulation **Markets in Financial Instruments Regulation (MiFIR)**. MiFID II and MiFIR address trader and advisor pay, conflicts of interest, fair communication with customers, independent investment advice, sales and product governance, best execution of client trades, and dealing with counterparties.

Dodd-Frank: Investor Protection Act

The **Investor Protection Act** is part of the broader Dodd-Frank Wall Street Reform and Consumer Protection Act (commonly known as the **Dodd-Frank Act**), which was U.S. legislation enacted in 2009 to enhance financial stability and prevent the negative events of the 2007–2009 financial crisis from happening again. The act enhances investor protection by providing increased protection to whistleblowers and enhancing rules around over-the-counter (OTC) derivatives trading, including the requirement to use a clearinghouse. It also created a committee to consult with the Securities and Exchange Commission (SEC) around new financial products, fees, and trading strategies, and it gave the SEC greater oversight responsibilities around OTC derivatives.

The Dodd-Frank Act also includes the **Volcker Rule**, a regulation that prohibits commercial banks from engaging in speculative trading and proprietary trading (i.e., trading for their own accounts), specifically limiting their investments in hedge funds and private equity funds. The act also created the **Consumer Financial Protection Bureau (CFPB)**, a government agency responsible for consumer rights protection, including providing independent oversight of consumer finance markets (e.g., mortgages, student loans, and credit cards).

Compliance Risk Management

Compliance risk management deals with compliance breaches of investment activities, which can be *unintentional* as a result of human error or ineffective policies, or *intentional* due to fraud. Risk management mainly focuses on a framework aimed to prevent compliance breaches.

Compliance breaches can occur as a result of poor employee engagement with the firm, employee dissatisfaction or stress, a weak ethics culture within the firm, or insufficient resources allocated to the firm's business units. Broader drivers of compliance risks include asymmetric information between buyers and sellers (sellers know more), conflicts of interest of traders who trade both for their clients and for their own firm, and economic conditions which can increase trading errors and encourage insider trading (e.g., during times of increased market volatility).

Efficient regulation of investment activities includes effective supervision of employees and trades, enhanced middle-office and back-office functions, adequate employee training, and a strong ethics culture.

Investor Protection Case Studies

LO 48.b: Describe and provide lessons learned from the case studies involving violations of investor protection or compliance regulations.

The case studies in this section focus on regulatory fines levied against large investment banks (UBS, JPMorgan, and Deutsche Bank Securities Inc.) in response to investor protection violations. These fines tended to be punitive in nature to “punish” for past violations, while at the same time aimed to act as deterrents against future improper behavior and encourage other firms to improve their compliance practices. These fines were set at an amount that was high enough to offset any benefits that accrued to the firms from the breaches.

The largest penalty to date levied against a single organization was that of \$11.15 billion against UBS in 2008, in connection with misrepresenting securities to investors as safe—when, in fact, these securities had significant liquidity risk.

In 2020, the U.S. Commodity Futures Trading Commission (CFTC) fined JPMorgan, one of the largest global investment banks, \$920 million for market manipulation and deceptive conduct. The conduct primarily related to the practice of **spoofing**, which spanned a period of over eight years—in which the appearance of high trading volume was artificially created by entering and then canceling orders in rapid succession, and in the process, creating prices that benefited JPMorgan.

In 2022, the U.S. regulatory agency Financial Industry Regulatory Authority (FINRA) fined Deutsche Bank Securities Inc. \$2 million for violating best execution practices between 2014 and 2018. While the fine was small compared to the other fines discussed, it was unusual in that it did not relate to misrepresentation or manipulation—rather, it was to the bank’s failure to secure the most favorable trade terms for customer orders, including order price and speed. Deutsche Bank routed orders through an order system that caused some delays in execution and often resulted in only partial trade execution. Despite being aware of these problems, Deutsche Bank did not modify its order routing arrangement. In addition, the bank received trading rebates by routing orders through this system, although this arrangement was only vaguely disclosed in the bank’s public reports. Deutsche Bank settled the fine without explicitly admitting or denying responsibility.



MODULE QUIZ 48.1

1. Which of the following regulations limits commercial banks’ investments in hedge funds and private equity funds?
 - A. The Investor Protection Act.
 - B. The Markets in Financial Instruments Directive (MiFID).
 - C. The Markets in Financial Instruments Directive II (MiFID II).
 - D. The Volcker Rule.

2. Which of the following legislations explicitly deals with whistleblower protection?
 - A. The Investor Protection Act.
 - B. The Markets in Financial Instruments Directive (MiFID).
 - C. The Markets in Financial Instruments Directive II (MiFID II).
 - D. The Volcker Rule.
3. Which of the following reasons is least likely a consideration for regulators when imposing fines on financial institutions against financial breaches and violations?
 - A. To cover the cost of litigation.
 - B. To deter other firms against manipulative bank practices.
 - C. To ensure that fines cover at least the benefits of breaches.
 - D. To signal to other firms to change their compliance practices.

KEY CONCEPTS

LO 48.a

Investor protection regulations focus on improving firms' communication to investors, including adequate disclosure of risks. Regulators levied significant fines over the last few years against noncompliant firms.

Regulatory compliance broadly covers two categories: (1) suitability, disclosure, and fiduciary responsibilities, and (2) improper business and market practices. Efficient regulation of investment activities includes effective compliance risk management—including supervision of employees and trades, enhanced middle-office and back-office functions, adequate employee training, and a strong ethics culture.

Four key regulations/legislations are as follows:

1. MiFID is an EU investor protection regulation implemented in 2007 that focuses on business and organizational conduct and prescribes regulatory disclosure and reporting requirements to prevent market abuse.
2. MiFID was revised in 2014 as MiFID II along with the accompanying regulation MiFIR and addresses trader and advisor pay, conflicts of interest, fair communication with customers, independent investment advice, sales and product governance, best execution of client trades, and dealing with counterparties.
3. The Investor Protection Act is part of the broader 2009 Dodd-Frank Act in the United States aimed at ensuring financial stability in the post-global financial crisis world. The act enhances investor safety and provides increased whistleblower protection and stronger rules around OTC derivatives trading. It also gave the SEC greater oversight responsibilities around OTC derivatives.
4. The Dodd-Frank Act also includes the Volcker Rule, a regulation that prohibits commercial banks from engaging in speculative trading and proprietary trading. It also created the Consumer Financial Protection Bureau (CFPB), a government agency responsible for consumer rights protection.

LO 48.b

The three case studies discussed in this reading focus on regulatory fines levied against global investment banks (UBS, JPMorgan, and Deutsche Bank Securities Inc.) as a result of significant investor protection violations. The fines tended to be punitive to not only penalize for past violations, but also to deter against future improper practices and to

encourage other firms to improve their own compliance and trading practices. The size of the fines was high enough to offset any benefits that accrued to the firms from the breaches.

ANSWER KEY FOR MODULE QUIZ

Module Quiz 48.1

1. **D** The Volcker Rule is part of the Dodd-Frank Act that prohibits commercial banks from engaging in speculative trading and proprietary trading, and it limits their investments in hedge funds and private equity funds.

The *MiFID* is an EU investor protection regulation that describes proper business and organizational conduct and prescribes regulatory disclosure and reporting requirements. *MiFID II* is an update to MiFID and addresses trader pay, execution of client trades, conflicts of interest, communication with customers, investment advice, and governance. The *Investor Protection Act* is also part of the Dodd-Frank Act. It increases the powers of the SEC, and provides increased protection to whistleblowers and enhanced rules around OTC derivatives trading. (LO 48.a)

2. **A** The Investor Protection Act is part of the Dodd-Frank Act that increases the powers of the SEC and provides increased protection to whistleblowers and enhanced rules around OTC derivatives trading. (LO 48.a)
3. **A** Covering the cost of any litigation is not a direct consideration in imposing fines. All other reasons are valid considerations for regulators in determining fines. (LO 48.b)

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 assigned reading—Federal Deposit Insurance Corporation.

READING 49

SUPERVISORY GUIDANCE ON MODEL RISK MANAGEMENT

Study Session 8

EXAM FOCUS

This is a very specific reading on managing model risk from the perspective of a bank (or other financial institution). It begins with defining model risk and how to manage it. It then discusses the development and implementation of a model. In the concluding section on model validation, be familiar with the details surrounding the three elements of a strong validation process.

MODULE 49.1: MODEL RISK MANAGEMENT

LO 49.a: Describe model risk and explain how it can arise in the implementation of a model.

A model involves the use of concepts from statistics, economics, finance, and mathematics together with assumptions that are used to transform input data into potentially useful quantitative outputs. There are three distinct parts to a model: (1) *information inputs* to deal with data and assumptions, (2) *processing* to convert inputs to estimates, and (3) *reporting* to convert estimates into applied information. Models attempt to mimic real life, but due to cost-benefit constraints, models must resort to some simplifying assumptions. As a result, models will never be completely accurate and model risk will always be present.

Model risk raises the possibility of (negative) outcomes resulting from poor decisions made from using inaccurate model outputs. Such outcomes include financial and reputational losses. Model risk can arise in two distinct ways:

1. The model has significant errors and produces faulty outputs. Errors could be introduced anywhere from the initial design to the final implementation. Seemingly innocent modifications to simplify complex issues may end up sacrificing the accuracy of the outputs. In addition, the expression “garbage in, garbage out” holds in terms of the quality of the output being a function of the quality of the inputs and assumptions.

2. The model is not used properly, not used for its intended purpose, or used out of context. For example, models that were formerly appropriate may no longer be appropriate for new products or changed market environments. Therefore, it is crucial for those in charge to understand the limitations and/or purposes of the original model.

Effective Model Risk Management Elements

LO 49.b: Describe elements of an effective model risk management process.

Managing model risk requires the identification of all relevant risks and attempts to quantify the exposure. The amount of model risk is dependent on how complicated the model is, the level of uncertainty with its inputs and assumptions, and its potential impact on users. Additionally, risk must be analyzed not just for stand-alone models but also in aggregate for models that are related or used in conjunction with other models.

The notion of an “effective challenge” of models is fundamental to managing model risk. It is necessary to have an in-depth, third-party, and unbiased evaluation of the model by individuals with strong technical skills who can determine the weaknesses of the model and its assumptions and propose effective solutions. To be effective, the individuals involved in the challenge should be completely independent from model development to avoid a self-review threat. Finally, there should be a robust follow-through process of issues identified during the challenge. This would require the support and authority of upper management.

Other methods of managing model risk include setting restrictions on the use of models, analyzing model performance, continually calibrating and improving models, and placing model output in the context of other relevant information (as a check on the reasonability of the output).

The potential impact (or materiality) of the model is a key element that will drive the level of risk management. If there is a potentially significant impact on the firm’s profits and/or financial position, then the risk management process must be much more detailed and comprehensive.

Best Practices for Model Development and Implementation

LO 49.c: Explain best practices for the development and implementation of models.

At the outset, development of a model should have a clearly stated objective that is congruent with the model’s eventual use. All the background information supporting the model needs to be thoroughly described, noting relevant strengths and weaknesses. The developers need to be satisfied that the model is logical and based on technically-

correct mathematical theories. In addition, a comparison of the model with other alternative models may serve as a “reasonability check” on the model’s logic.

During development, it is crucial to ensure that the data and assumptions are robust and are relevant for the model. Any data proxies, data that is not representative, or adjustments to data (e.g., from external data sources) need to be clearly documented and made clear to users. That way users can judge for themselves the usefulness of the data.

Testing is a key component of model development to ensure the model is working as planned. Testing involves assessing the precision of the model, proving the model’s strength and consistency, and using input amounts over a reasonable range to assess the model. At the same time, potential weaknesses in the model or circumstances where the model does not work must be noted. Testing should occur in both normal states and extreme (stressed) market states. This would include unusual (but still plausible) conditions. In addition, if the given model’s outputs are used as inputs for other models, then an analysis of the other models is required. There should also be proper documentation, analysis, and summary of the testing process.

The testing process may vary given the type of the model and the context in which the model is used. In a quantitative context, the use of sampling introduces potential error in making conclusions. To avoid making Type I (rejecting null hypothesis when it is true) or Type II (failing to reject null hypothesis when it is false) testing errors when relying on a single test, multiple tests should be utilized in model development.

Although the testing process is focused on the quantitative aspects, the qualitative aspects must not be overlooked. For example, quantitative outputs might be taken and tempered with subjective and/or nonquantitative elements to make the outputs relevant. Care must be taken to ensure that any alterations have a reasonable or logical basis and are clearly documented. Additionally, a robust internal control system (involving both individuals and computers) will promote an effective model development and implementation process.



MODULE QUIZ 49.1

1. Which component of a model deals with converting estimates into useful or applied information?
 - A. Information inputs.
 - B. Processing.
 - C. Reporting.
 - D. Transformational.
2. Which of the following statements regarding model risk is correct?
 - A. Shortcuts and simplifications will increase model risk.
 - B. Managing model risk requires proper segregation of duties.
 - C. With the appropriate procedures and tools, model risk can be eliminated.
 - D. Like many other risks, model risk has both an upside and a downside component.
3. Which of the following items is least likely to be a key consideration when testing models?
 - A. Testing for potential weaknesses.
 - B. Testing with extreme values as inputs.
 - C. Testing under normal market conditions.

D. Testing other models that rely on the subject model.

MODULE 49.2: MODEL VALIDATION PROCESS

LO 49.d: Describe elements of a strong model validation process and challenges to an effective validation process.

Model validation involves a series of steps to ensure that models are achieving their intentions. There needs to be a segregation of duties, for example, in that those individuals who develop the models should generally not be the same ones to validate it. Some exceptions may apply in areas that are overly technical or specialized, but in those instances, there must be a rigorous and objective review of such validation.

Three elements of a strong validation process are (1) evaluation of conceptual soundness, (2) ongoing monitoring, and (3) outcomes analysis.

Evaluation of Conceptual Soundness

This step is an overall quality check on the model, which involves analyzing all the documentation and live test results that backup the construction of the model. The documentation of the development process should be analyzed prior to using the model as well as analyzed throughout the validation process. If a model undergoes significant change, the documentation of such developments should also be reviewed.

Therefore, the model development process must be well-documented in terms of formulation, major assumptions, computations, and inputs. A proper validation process would thoroughly examine the documentation and perform supplemental testing, if appropriate. In terms of specifics, evaluating the significant assumptions and factors chosen and their effect on the outputs of the model is important. Additionally, the data underlying the model needs to be assessed for relevance and for ensuring it is representative when attempting to model specific portfolio assets or economic environments. That is especially the case when the data is external or is being used to model for new business ventures.

Sensitivity analysis should be performed as part of validation. It can be done for single variables by testing a range of changes in values for inputs and then examining the corresponding outputs to ensure they are reasonable. Testing can be expanded to multiple variable changes at the same time to check for any previously unknown interrelationships between the variables. Finally, the testing can be in the form of stress testing, which takes on extreme values to determine if the model still functions properly or to determine at what point the model loses effectiveness or accuracy. Should it be determined that a model is not working properly, then a plan must be in place to make amendments to the model, limiting the use of the model, or even replacing the model.

The nonquantitative aspects of model development must also be validated to ensure that any subjective assessments made in model development make sense and have appropriate backup and documentation.

Ongoing Monitoring

Ongoing monitoring attempts to determine whether the model needs any changes, additional developments, or replacement. Once the model is put into use, monitoring begins and should be done on a frequent basis, taking into account factors such as the purpose of the model and the risk exposures involved. Process verification and benchmarking should be part of the monitoring process.

Process verification looks at data inputs to ensure they remain error-free and complete. When implementing a model, the computer code must be verified for accuracy and there must exist an internal control to ensure computer code can only be changed by authorized individuals and that all changes be recorded for potential future audit. Process verification is very important in context of system integration because model processing takes in different data sources and eventually transfers processed data for data storage and reporting purposes. Also, within the firm, some users will develop their own spreadsheets or databases for quantitative analysis purposes, which are fraught with model risk. Ultimately, as the data changes with time, the corresponding systems need to be updated accordingly.

The same kinds of tests used for developing models would also be applicable for monitoring. The same goes for sensitivity analysis as part of monitoring. The monitoring process would review any overrides together with the supporting documentation. Human judgment is important and may necessitate the overriding of output from a model. The existence of overrides does suggest problems with the performance of the model and requires a deeper understanding for why the overrides are occurring, especially if the overrides are frequent. In some cases, it means the model needs to be amended or completely overhauled.

Benchmarking compares a model's inputs and outputs with other comparable data or models. If there are significant variances between the model's outputs and benchmarks, then the question is whether such variances fall within an acceptable range. If the variances between the model and benchmark are small, then it suggests the model is reliable, but it should not be thought of as absolute confirmation. On the other hand, the existence of significant variances does not automatically mean that the model is faulty; it could be that the benchmark uses a different methodology and therefore is not a good comparison.

Outcomes Analysis

The validation process must also examine the outputs from the model in context of what actually happened. Frequently, there is a determination of the level of precision of the estimates as a means of assessing the performance of the model. If it is determined through outcomes analysis that the model is weak, then the model must be revised.

Outcomes analysis includes both quantitative and qualitative methods; as an example of the latter, expert judgment is used to assess whether the results are logical. Whichever method is used should be based on the nature of the model, its level of complexity, the availability of data, and the level of model risk to the firm. Testing must be tailored to the specific circumstances and should include multiple tests since a single test will have inherent limitations and therefore most likely be insufficient.

Parallel outcomes analysis considers that models are frequently amended for new information or because they are not effective. Such analysis involves a side-by-side examination of the first model and the amended model's estimates to the actual outcomes. If the amended model is not noticeably better than the first model, then further amendments to the model are required before fully replacing the first model.

Backtesting looks at the variances between the actual results and the estimates from the model. The time period under examination is different from that used in developing the model but is consistent with the model's forecast horizon. Confidence intervals are established based on the model estimates; results that lie beyond the intervals are considered significant and must be monitored. The point is to ascertain whether the outliers resulted from not including important factors in the model or whether there were errors in the model specification. Assessing value at risk (VaR) is a good example of backtesting, although only one value (e.g., 5% VaR) could be supplemented with other values (e.g., 1% VaR) to consider the possibility for larger losses.

Unfortunately, trying to understand backtesting results is usually a complex task of reviewing many forecasts in various economic environments and various time periods. Although statistical testing is used, the difficulty lies in selecting the right tests and how to decipher the results.

Long forecasting periods require backtesting which comes with the inherent disadvantage of obtaining the right amount of data. In such instances, there needs to be additional testing over shorter periods. "Early warning" signals that measure model performance on a more timely basis could be used to supplement backtesting.

Should the results of outcomes analysis show major problems or poor performance with the models, then amendments and/or reconstruction may be required. In the case of significant changes and reconstruction, validation is required prior to implementation.

Vendor and Other Third-Party Products

Vendor products are very commonly used; they can range from providing data to full models. They make the validation process trickier because the modeling activities are external and some parts of the modeling may be confidential. As a result, the validation process will need to be changed somewhat from that used for internally developed models. For example, vendors need to provide details regarding the construction of their models to ensure that the model is appropriate for the user. In addition, testing results would need to be provided by the vendor to demonstrate that the models are effective at what they are supposed to do. Because the use of an external model may mean limited access to information on coding and implementation, the validation process will likely have to focus more on sensitivity analysis and benchmarks. If a vendor model is modified to suit the institution's needs, then the modifications should be noted and explained during the validation process. Overall, in-depth knowledge of the vendor product is necessary from the perspective of the institution's internal controls.



MODULE QUIZ 49.2

1. Backtesting is most appropriately classified in which element of the validation process?
 - A. Evaluation of conceptual soundness.

- B. Ongoing monitoring.
 - C. Outcomes analysis.
 - D. Postvalidation review.
2. Comparing a model's inputs and outputs to estimates from other data or models is best described as:
- A. benchmarking.
 - B. ongoing monitoring.
 - C. process verification.
 - D. sensitivity analysis.

KEY CONCEPTS

LO 49.a

Model risk raises the possibility of (negative) outcomes resulting from poor decisions made using inaccurate model outputs. Model risk can arise in two distinct ways: (1) the model has significant errors and produces faulty outputs, and (2) the model is not used properly, not used for its intended purpose, or used out of context.

LO 49.b

Managing model risk requires the identification of all relevant risks and attempts to quantify the exposure. The amount of model risk is dependent on how complicated the model is, the level of uncertainty with its inputs and assumptions, and its potential impact on users.

Other methods of managing model risk include setting restrictions on use of models, analyzing model performance, continually calibrating and improving models, and placing model output in the context of other relevant information.

LO 49.c

At the outset, development of a model should have a clearly stated objective that is congruent with the model's eventual use. All the background information supporting the model needs to be thoroughly described, noting relevant strengths and weaknesses.

Testing is a key component of model development to ensure the model is working as planned. Although the testing process is focused on the quantitative aspects, the qualitative aspects must not be overlooked.

LO 49.d

Three elements of a strong model validation process are (1) evaluation of conceptual soundness, (2) ongoing monitoring, and (3) outcomes analysis.

Evaluation of conceptual soundness is an overall quality check on the model, which involves analyzing all the documentation and live test results that backup the construction of the model. A proper validation process would thoroughly examine the documentation and perform supplemental testing, if appropriate. Sensitivity analysis should also be performed as part of validation and it can be done for single or multiple variables.

Ongoing monitoring attempts to determine whether the model needs any changes, additional developments, or replacement. Process verification and benchmarking

should be part of the monitoring process. Process verification looks at data inputs to ensure they remain error-free and complete. Benchmarking compares a model's inputs and outputs with other comparable data or models. If there are significant variances between the model's outputs and benchmarks, then the question is whether such variances fall within an acceptable range.

The validation process must also examine the outputs from the model in context of what actually happened. Parallel outcomes analysis considers that models are frequently amended for new information or because they are not effective. Backtesting looks at the variances between the actual results and the estimates from the model. The time period under examination is different from that used in developing the model but is consistent with the model's forecast horizon. Confidence intervals are established based on the model estimates; results that lie beyond the intervals are considered significant and must be monitored.

ANSWER KEY FOR MODULE QUIZZES

Module Quiz 49.1

1. **C** The reporting component essentially transforms estimates into useful business information. In contrast, the processing components transforms inputs into estimates. (LO 49.a)
2. **B** A proper "effective challenge" of models is a key part of managing model risk and would require proper segregation of duties. In that regard, the model development process and the critical review of the model must be done by different parties in order to maintain proper independence and objectivity. (LO 49.b)
3. **C** Although testing is done under normal market conditions, a more accurate statement would be that testing is done under a wide variety of market conditions, including those that are unusual or extreme. Testing for potential weaknesses, using extreme values as inputs, and testing other models that use the outputs of the subject model as inputs are all important considerations when testing models. (LO 49.c)

Module Quiz 49.2

1. **C** Backtesting is a specific type of outcomes analysis. (LO 49.d)
2. **A** Ongoing monitoring is the general term used to describe various activities that constitute the second key aspect of the validation process. Those activities include benchmarking, process verification, and sensitivity analysis. However, benchmarking is the specific term that applies to comparing a model's input and outputs to relevant estimates. (LO 49.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 16.

READING 50

CASE STUDY: MODEL RISK AND MODEL VALIDATION

Study Session 8

EXAM FOCUS

This short reading provides contextual importance to model risk management. For the exam, focus on the sources of model risk, approaches to model risk management, and what the presented case studies teach us about model risk management.

MODULE 50.1: MODEL RISK AND MODEL VALIDATION

Model Risk Exposure

LO 50.a: Define a model and describe different ways that financial institutions can become exposed to model risk.

Models are sophisticated tools used widely in finance. An example of a financial model is the value at risk (VaR) computation. Various definitions exist for models, such as the U.S. Federal Reserve's model risk guidance definition, from Supervision and Regulation 11-7: "The term *model* refers to a quantitative method, system, or approach that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into quantitative estimates."¹

In other words, a model generates an estimate or forecast using a set of inputs, an underlying theory, and under a certain set of assumptions. The inputs can be quantitative as well as qualitative. It is critical to recognize that the estimate or forecast (i.e., the model output) is not definitive, but rather subject to estimation error.

Model risk can occur in the following two types:

1. *Execution risk* refers to the risk of models not functioning as intended due to errors in input data or in coding of the model.
2. *Conceptual errors* arise when the assumptions are invalid (i.e., they do not represent reality) or when incorrect modeling techniques are used.

Conceptual errors are more difficult to identify. A model that works in some economic environments may not perform well when used in other environments. Model assumptions and limitations should be documented and effectively communicated to users. For example, risk measurement models often rely on correlations between portfolio assets as an input. Correlation estimates from normal times often underestimate correlations during more volatile market conditions. Model validation techniques will verify whether the model is performing as expected.

Model Risk Management

LO 50.b: Describe the role of the model risk management function and explain best practices in the model risk management and validation processes.

A **model risk management (MRM)** team comprises of experts who are independent of the original model developers and are charged with mitigating model risk. MRM teams set the standards for model documentation, data quality, and model version control. Not all models pose the same organizational risks. Cost-benefit considerations call for more scrutiny for those models that pose a higher level of risk. Therefore, models can be assigned to risk tiers.

The level of model risk tier depends on (1) materiality of model output (e.g., dollar value of loss if the model fails), (2) model complexity, (3) whether the model will be client facing, and (4) whether the model is used for regulatory compliance. The highest tiers of model risk require more frequent validation (usually every 2–3 years) and comprehensive backtesting for reliability of model output. Regardless of their risk tier, all models should be reviewed annually regarding changes in the environment, input data quality, and other important elements such that there are no material changes that would affect model performance.

Additionally, MRM teams review the periodic model performance reports prepared by model owners. It is important that MRM should be a continuous, ongoing process rather than a scheduled, periodic review to limit the damage done by models that no longer generate reliable forecasts. The existence of an MRM team should not result in complacency among the model users and developers, who are the first line of defense against unnecessary risk that the institution is exposed to.

Model Risk Case Studies

LO 50.c: Describe lessons learned from the three case studies involving model risk.

Gaussian Copula and CDO Pricing

In the 2000s, David X. Li developed a collateralized debt obligation (CDO) pricing model known as the **Gaussian copula function**. Li assumed that markets were efficient and, therefore, credit default swap (CDS) prices, which were used for the model, were correctly set by the market. The model used current CDS prices to infer correlations

among assets in a collateral pool known as the Gaussian constant (recall that lower correlations among assets in a collateral pool indicate a lower risk for the CDO). The model was quickly adopted by major market participants, and its use became entrenched—without regard for the model’s limitations.

Historical correlations of residential mortgage defaults tended to be low; homeowners do not systematically default together. However, as housing prices fell in 2008, CDS prices started shooting up (reflecting higher credit risk and higher correlations). The model incorporated changing correlations with a lag, leading to a collapse in the CDO market. Essentially, the model encouraged both quantitative analysts and their managers to ignore that the real world is full of randomness, uncertainty, and noise.

MRM in this context would aim to increase the transparency regarding assumptions and limitations of this CDO pricing model. Given that the model users lacked the necessary quantitative background, effective communication would have been critical to minimize the misuse of the model.

The Barclays Acquisition of Lehman Brothers’ Assets and Spreadsheet Error

The recent global financial crisis was triggered by the collapse of Lehman Brothers, at the time, the fourth-largest investment bank in the United States. During the liquidation of Lehman Brothers, Barclays made an offer to purchase some of Lehman’s assets and trading positions. A few hours before the deadline to submit bids to the bankruptcy court, Barclays sent a spreadsheet consisting of 1,000 rows to their lawyers at Cleary Gottlieb indicating the positions that they wanted to purchase as well as those they did not want.

The 179 positions that Barclays was not interested in were in hidden rows. To conform to the bid submission guidelines, a junior law associate converted the spreadsheet into a PDF—unaware that the hidden rows were now revealed. The mistake was realized several days later—after the bid was approved, requiring Barclays to file a legal motion to exclude those contracts.

This is an example of an implementation error. The spreadsheet is not a model, but the failure to delete the unneeded rows posed a large potential loss to the user of the software.

NASA Mars Orbiter

The Mars Orbiter is an example of a rather innocuous mistake, which led to the loss of a \$125 million satellite. In this case, the engineering team at Lockheed Martin used English units of measurement (commonly used in the United States), while NASA’s convention was to use the metric system. This mistake in measurement of model inputs led to the loss of a multi-million-dollar satellite.

MRM, in this context, would have rigorously tested all assumptions and inputs. Oftentimes, small mistakes result in losses—some of those losses, however, can be quite large. The case for rigor of MRM, often considered to be a bureaucratic hurdle, cannot be overstated.



1. Which one of the following items is least likely associated with a model?
 - A. Qualitative inputs.
 - B. Mathematical theories.
 - C. Precise output.
 - D. Assumptions.
2. Which of the following statements describes model execution risk?
 - A. Inaccurate model inputs.
 - B. Model coding that is consistent with model assumptions.
 - C. Inappropriate model assumptions.
 - D. Incorrect modeling techniques.
3. What is the most likely reason for the failure of the Gaussian copula function to price CDOs?
 - A. Model computation error.
 - B. Inappropriate model for the task.
 - C. Invalid model assumption.
 - D. Invalid use of model output.
4. The Barclays bankruptcy court bid for Lehman assets most likely suffered from:
 - A. ongoing monitoring.
 - B. improper model use.
 - C. invalid model assumptions.
 - D. implementation error.
5. The failure of NASA's Mars Orbiter mission can be directly attributed to:
 - A. model inaccuracy.
 - B. model assumptions.
 - C. incorrect model choice.
 - D. incorrect model inputs.

KEY CONCEPTS

LO 50.a

Models generate an estimate or forecast using a set of inputs under a certain set of assumptions. Two types of model risk are (1) execution risk and (2) conceptual errors.

LO 50.b

A model risk management (MRM) team sets the standards for model documentation, data quality, and model version control consistent with the model's risk tier. The model risk tier depends on (1) materiality of model output, (2) model complexity, (3) whether the model will be client facing, and (4) whether the model is used for regulatory compliance.

LO 50.c

The model risk case studies presented in this reading highlight the risk of using models given (1) invalidity of assumptions, (2) implementation error, or (3) input measurement error.

ANSWER KEY FOR MODULE QUIZ

Module Quiz 50.1

1. **C** Model outputs are forecasts or estimates, which are not precise. Model inputs can be qualitative or quantitative. Also, models rely on a set of assumptions, and use economic and mathematical theories. (LO 50.a)
2. **A** Execution risk arises due to errors in input data or in coding of the model. (LO 50.b)
3. **C** The Gaussian copula function relied on the Gaussian constant input, which was based on an assumption of static (constant) asset correlations in a collateral pool. (LO 50.c)
4. **D** The failure to delete spreadsheet rows representing assets that Barclays did not want to bid on represented an implementation error. (LO 50.c)
5. **D** The units of measurement for model inputs were inaccurate, which led to the failure of the model and a very large loss. (LO 50.c)

¹ <https://www.federalreserve.gov/supervisionreg/srletters/sr1107.htm>

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 assigned reading—Schuermann.

READING 51

STRESS TESTING BANKS

Study Session 8

EXAM FOCUS

This reading focuses on the use of bank stress testing to determine if liquidity and capital are adequate. The discussion focuses primarily on capital adequacy but notes that the issues are similar with respect to liquidity. For the exam, understand the details of the 2009 Supervisory Capital Assessment Program (SCAP), the first stress testing required after the 2007–2009 financial crisis. Also, be able to explain the issue of coherence in stress testing and describe the challenges with modeling the balance sheet using stress tests in the context of the stress test horizon. Finally, understand the differences in disclosure between United States and European stress tests and the way that stress test methodologies and disclosure have changed since the 2009 SCAP.

MODULE 51.1: STRESS TESTING

In the wake of the 2007–2009 financial crisis, regulators and other policymakers realized that standard approaches to risk assessment, such as regulatory capital ratio requirements, were not sufficient. At that point, supervisory **stress testing** became a popular tool for measuring bank risk. There was a “pop-quiz” quality to the post-financial crisis stress tests. They were difficult to manipulate because they were sprung on banks at short notice. As a result, the information provided by the stress tests to regulators and the market was truly new. This allowed financial markets to better understand bank risks and, as a result, regain a level of trust in the banking sector.

The goal of stress testing, as well as capital/liquidity and “economic capital/liquidity” (i.e., internal, bank-specific) models, is to assess how much capital and liquidity a financial institution needs to support its business (i.e., risk taking) activities. It is relatively easy for banks to swap out of lower risk assets and into higher risk assets. Stress testing provides clarity about the true risk and soundness of banks.

Stress testing is an old tool that banks and other firms have used to examine risk. It asks the question “what is the institution’s resilience to deteriorating conditions?” and simulates financial results given various adverse scenarios. Stresses are generally of two basic types: scenarios or sensitivities. An example of a scenario is a severe recession. An example of sensitivity is a significant increase in interest rates. Risk managers can stress test the sensitivity of a single position or loan or an entire portfolio.

Supervisory Capital Assessment Program (SCAP)

LO 51.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.

In the wake of the financial crisis, there was much uncertainty about the soundness of the U.S. banking system. Regulators needed to assess the capital strength of financial institutions. If there was a gap between what a bank needed in terms of capital and what it had, regulators had to find a credible way to “fill the hole.” The 2009 U.S. bank stress test, known as the **Supervisory Capital Assessment Program (SCAP)**, was meant to serve that purpose. It was the first macro-prudential stress test after the 2007–2009 financial crisis. Macro-prudential regulation focuses on the soundness of the banking system as a whole (i.e., focuses on systematic risks) while micro-prudential regulation focuses on the safety and soundness of the individual institution.

At this point the federal government planned to infuse equity capital into banks that were undercapitalized based on stress testing. The Treasury intended to borrow money and “downstream” it as equity in banks via the Treasury’s Capital Assistance Program (CAP). If banks could not convince investors to fill the hole (i.e., infuse banks with needed equity capital), current investors would be diluted by the government’s equity investment. In the end, 19 SCAP banks were required to raise \$75 billion within six months. The undercapitalized banks raised \$77 billion of Tier 1 common equity and did not need to draw on the CAP funds.

Prior to 2009, stress testing was relatively simple. Figure 51.1 summarizes the differences in stress testing pre-SCAP and post-SCAP.

Figure 51.1: Comparison of Stress Testing Pre-SCAP and Post-SCAP

Pre-SCAP	Post-SCAP
Primarily assessed exposure to single-shocks (e.g., volatility increases OR interest rate increases OR increasing unemployment).	Considers broad macro-scenarios and market-wide stresses with multiple factors occurring/changing at once, as evidenced in the 2007–2009 financial crisis.
Focused on specific bank products or business units (e.g., lending or trust).	Focuses on the whole firm, a more comprehensive look at the effect of the stress scenarios on the institution.
Typically focused on earnings shocks (i.e., losses) but not on capital adequacy.	Explicitly focuses on capital adequacy. Considers the post-stress common equity threshold to ensure that a bank remains viable.
Focused exclusively on losses.	Focuses on revenues, costs, and projected losses.
Stress testing was static in nature.	Stress testing is now dynamic and path dependent.

We will compare and contrast SCAP, CCAR, and EBA stress tests later in this reading.

Challenges in Designing Stress Tests

LO 51.b: Explain challenges in designing stress test scenarios, including the problem of coherence in modeling risk factors.

One of the challenges of designing useful stress tests is **coherence**. The sensitivities and scenarios must be extreme but must also be reasonable or possible (i.e., coherent). Problems are inherently multi-factored, making it more difficult to design a coherent stress test. For example, an increase in volatility can lead to credit markets freezing. High unemployment and falling equity prices often go hand-in-hand. It is not sufficient to specify one potential problem (i.e., risk factor) because the others do not remain fixed. The supervisor's key challenge is to specify the joint outcomes of all relevant risk factors.

Additionally, not everything goes bad at once. For example, if some currencies are depreciating, others must be appreciating. If there is a "flight to quality," there must also be safe haven assets in the stress model. So while it is important to look at, for example, what happens if U.S. Treasury debt becomes riskier and is no longer a safe haven, the model would at the same time have to identify the "risk-free" asset(s) in which capital would flee under those circumstances.

The problem is even greater when designing stress scenarios for marked-to-market portfolios of traded securities and derivatives. Risk is generally managed with a value at risk (VaR) system. Hundreds of thousands of positions in the trading book must be mapped to thousands of risk factors, tracked on a daily basis. The data that results is used to estimate volatility and correlation parameters. It is very difficult to find coherent outcomes in such a complex, multi-dimensional universe.

The 2009 SCAP tested rather simple scenarios with three variables: growth in GDP, unemployment, and the house price index (HPI). Historical experience was used for the market risk scenario (i.e., the financial crisis—a period of "flight to safety," the failure of Lehman, and higher risk premiums). While the market risk scenario did not test for something new, the overall framework achieved coherence of financial and other stresses of the time period.

One thing to note is that prior to 2011 all supervisory stress tests imposed the same scenarios on all banks (i.e., a one-size-fits-all approach to stress testing). In recognition of the problem, the 2011 and 2012 Comprehensive Capital Analysis and Review (CCAR) asked banks to submit results from their own stress scenarios in addition to the supervisory stress scenario in an attempt to reveal bank-specific vulnerabilities. This was an important step forward from the 2009 SCAP as it gave supervisors a sense of what banks think are the high risk scenarios. This provides regulators with not only bank-specific (i.e., micro-prudential) insight but also improves macro-prudential supervision as it highlights common risks across banks that may have been underemphasized or unnoticed before.



MODULE QUIZ 51.1

1. Which of the following changes in stress testing was not the result of the 2009 Supervisory Capital Assessment Program (SCAP)?
 - A. Banks are now required to provide the results of their own scenario stress tests.
 - B. Stress scenarios are now broader in nature.
 - C. Stress testing now focuses on the whole firm.
 - D. Stress testing now focuses on revenues, costs, and projected losses.

MODULE 51.2: CHALLENGES IN MODELING LOSSES AND REVENUES

LO 51.c: Explain challenges in modeling a bank's revenues, losses, and its balance sheet over a stress test horizon period.

Current stress tests are based on macro-scenarios (e.g., unemployment, GDP growth, the HPI). One concern is how to translate the macro-risk factors employed in stress testing into micro (i.e., bank-specific) outcomes related to revenues and losses. Supervisors need to map from macro-factors into intermediate risk factors that drive losses in specific products and geographic areas. Although not limited to these products, geographic differences are especially important in modeling losses in both commercial and residential real estate lending.

Credit card losses are particularly sensitive to unemployment figures. For example, unemployment was 12.9% in Nevada in July 2011, 3.3% in North Dakota, and the national unemployment rate was 9.1%. Credit card loss rates varied dramatically from region to region during this period. The geographic diversity with respect to macro-factors makes a “one-size-fits-all” stress testing regime less meaningful.

Geography is not the only difference supervisors must contend with. Risks affect different asset classes in different ways. For example, during recessions people buy fewer automobiles overall. However, if a person needs a car during a recession, he is more likely to buy a used car. Thus, if default rates increase, loss given default (LGD) (i.e., loss severity) may not increase as much.

The business cycle also affects different industries at different times. Consider the airline industry versus the healthcare industry during a recession. Airplanes are collateral for loans to airlines. If the airline industry is depressed, the bank gets stuck with collateral that is very difficult to sell except at extremely depressed prices. Healthcare is somewhat recession-proof but that doesn't mean the bank can transform an airplane it is stuck with into a hospital. These factors increase the difficulty of mapping broader macro-factors to bank-specific stress results.

Modeling revenues over a stress test horizon period is much less developed than modeling losses. The 2009 SCAP did not offer much clarity on how to calculate revenue during times of market stress. The main approach to modeling revenue is to divide a bank's total income into interest and noninterest income. The yield curve can be used to estimate interest income, and it can reflect credit spreads during stress testing scenarios; however, it remains unclear how bank profitability is directly influenced by

the net impact of changing interest rates. Estimating noninterest income, which includes fees and service charges, is even more difficult to model. This is alarming given the steady increase in noninterest income among U.S. banks.

Challenges in Modeling the Balance Sheet

The typical stress test horizon is two years. Over this period, both the income statement and balance sheet must be modeled to determine if capital is adequate post-stress. Generally speaking, capital is measured as a ratio of capital to assets. There are different types of capital (e.g., Tier 1 and Tier 2) but in general (and for the sake of simplicity), capital can be defined as common equity. **Risk-weighted assets (RWA)** are computed based on the Basel II risk weight definitions. For example, agency securities have a lower risk weight than credit card loans.

In a stress model, the beginning balance sheet generates the first quarter's income and loss from the stressed scenario, which in turn determines the quarter-end balance sheet. At that point, the person modeling the risk must consider if any assets will be sold or originated, if capital is depleted due to other actions such as acquisitions or conserved as the result of a spin-off, if there are changes made to dividend payments, if shares will be repurchased or issued (e.g., employee stock or stock option programs), and so on. These decisions make modeling the balance sheet over the stress horizon quite difficult. The stress model doesn't determine if it would be a good time to sell a subsidiary or lower dividend payments.

The challenges of balance sheet modeling exist under both static and dynamic modeling assumptions. The bank must maintain its capital (and liquidity) ratios during all quarters of the stress test horizon. At the end of the stress horizon the bank must estimate the reserves needed to cover losses on loans and leases for the next year. This means that a two-year horizon stress test is actually a three-year stress test (i.e., a T-year stress test requires the bank to estimate required reserves to cover losses for T+1 years).

Stress Test Comparisons

Disclosure was a significant feature of the 2009 SCAP. It disclosed projected losses for each of the 19 participating banks for eight asset classes. It also disclosed resources the bank had to absorb losses other than capital (e.g., pre-provision net revenue and reserve releases if available). This high level of disclosure created transparency. It allowed investors and the market to check the severity of stress tests and to comprehend stress test outcomes at the individual bank level. Before the 2009 SCAP, banks only reported realized losses, not forecasted losses (i.e., possible losses given the stress scenario).

The 2011 CCAR required only that macro-scenario results be published, not bank level results. This differed dramatically from the 2009 SCAP requirements. The market had to figure out whether a bank had passed the test or not (i.e., market participants had to "do the math" themselves). For example, if a bank increased its dividend, it was assumed by the market to have "passed" the stress test. However, the 2012 CCAR disclosed virtually the same amount and detail of bank level stress data as the 2009 SCAP (i.e., bank level loss rates and losses by major asset classes). The regulatory asset classes are:

1. First and second lien mortgages.
2. Commercial and industrial (C&I) loans.
3. Commercial real estate loans.
4. Credit card lending.
5. Other consumer loans.
6. Other loans.

One of the key contributions of the CCAR was that in both 2011 and 2012 the CCAR required banks to submit the results of their own scenarios, both baseline and stress, not just supervisory stress test results. The Fed also reported dollar pre-provision net revenue (PPNR), gains and losses on available-for-sale and held-to-maturity securities, and trading and counterparty losses for the six institutions with the largest trading portfolios. These firms were required to conduct the trading book stress test. The numbers that were reported were supervisory estimates, not bank estimates, of losses under the stress scenario.

In contrast, the 2011 European Banking Authority (EBA) Irish and 2011 EBA European-wide stress tests, both disclosed after the CCAR, contained considerable detail. In the Irish case, the report contained a comparison of bank and third party estimates of losses. The EBA data was available in electronic, downloadable form. Ireland needed credibility, having passed the Committee of European Bank Supervisors (CEBS) stress test in July 2010 only to need considerable aid four months later. In general, the faith in European supervisors was harmed and only by disclosing detailed information on bank-by-bank, asset-class, country, and maturity bucket basis could the market interpret the data and draw its own conclusions about individual bank risks. Figure 51.2 summarizes the differences among the various stress test regimes.

Figure 51.2: Comparison of Macro-Prudential Stress Tests

Stress Test	Methodologies	Disclosure	Findings
SCAP (2009). All banks with \$100 billion or more in assets as of 2008 year end were included.	Tested simple scenarios with three dimensions, GDP growth, unemployment, and the house price index (HPI). Historical experience was used for the market risk scenario (i.e., the financial crisis—a period of “flight to safety,” the failure of Lehman, and higher risk premiums). A “one-size-fits-all” approach.	First to provide bank level projected losses and asset/product level loss rates.	19 SCAP banks were required to raise \$75 billion within six months. The undercapitalized banks actually raised \$77 billion of Tier 1 common equity and none of the banks were forced to use the Treasury’s Capital Assistance Program funds.
CCAR (2011)	In recognition of “one-size-fits-all” stress testing, CCAR asked banks to submit results from their own baseline and stress scenarios.	Only macro-scenario results were published.	
CCAR (2012)	Banks were again asked to submit their own baseline and stress test results.	Similar in detail to SCAP 2009—bank level and asset/product level loss rates disclosed.	

Stress Test	Methodologies	Disclosure	Findings
EBA Irish (2011)	Similar in design to EBA Europe 2011.	Comparison of bank and third party projected losses; comparison of exposures by asset class and geography. Data is electronic and downloadable.	After passing the 2010 stress tests, 2011 stress tests revealed Irish banks needed €24 billion. Greater disclosure in 2011 resulted in tightening credit spreads on Irish sovereign and individual bank debt.
EBA Europe (2011). [formerly the Committee of European Bank Supervisors (CEBS)] 90 European banks were stress tested.	Specified eight macro-factors (GDP growth, inflation, unemployment, commercial and residential real estate price indices, short and long-term government rates, and stock prices) for each of 21 countries. Specified over 70 risk factors for the trading book. It also imposed sovereign haircuts across seven maturity buckets.	Bank level projected losses. Comparisons of exposures by asset class and geography. Data is electronic and downloadable.	Eight banks were required to raise €2.5 billion.

The key benefit of greater disclosure is transparency. Transparency is especially important in times of financial distress. However, during “normal” times, the costs of disclosure may outweigh the benefits. For example, banks may “window dress” portfolios, making poor long-term investment decisions to increase the likelihood of passing the test. Traders may place too much weight on the public information included in stress test disclosure and be disincentivized to produce private information about financial institutions. This harms the information content of market prices and makes prices less useful to regulators making policy decisions.

One thing to note is that prior to the CCAR 2011 requirements, all supervisory stress tests imposed the same scenarios on all banks (i.e., a one-size-fits-all approach to stress testing). In recognition of the problem, the 2011 and 2012 CCAR asked banks to submit results from their own scenarios in addition to the supervisory stress scenario in an attempt to reveal bank-specific vulnerabilities.



MODULE QUIZ 51.2

1. Piper Hook, a bank examiner, is trying to make sense of stress tests done by one of the banks she examines. The stress tests are multi-factored and complex. The bank is using multiple extreme scenarios to test capital adequacy, making it difficult for Hook to interpret the results. One of the key stress test design challenges that Hook must deal with in her examination of stress tests is:
 - A. multiplicity.
 - B. efficiency.
 - C. coherence.
 - D. efficacy.
2. Greg Nugent, a regulator with the Office of the Comptroller of the Currency, is presenting research on stress tests to a group of regulators. He is explaining that macro-variable stress testing can be misleading for some banks because of geographical differences in macro risk factors. He gives the example of the wide range of unemployment rates across the United States following the 2007–2009 financial crisis. Which type of loan did Nugent most likely identify as having losses tied to unemployment rates?
 - A. Residential real estate loans.
 - B. Credit card loans.
 - C. Commercial real estate loans.
 - D. Industrial term loans.
3. A risk modeler has to make assumptions about acquisitions and spinoffs, if dividend payments will change, and if the bank will buy back stock or issue stock options to employees. These factors make it especially challenging to:
 - A. get a CAMELS rating of 2 or better.
 - B. determine if the bank has enough liquidity to meet its obligations.
 - C. meet the Tier 1 equity capital to risk-weighted assets ratio.
 - D. model a bank’s balance sheet over a stress test horizon.
4. One of the key differences between the 2011 CCAR stress test and the 2011 EBA Irish stress test is that:
 - A. the CCAR did not require banks to provide results from their own stress scenarios.
 - B. the EBA Irish did not find any banks in violation of capital adequacy requirements.
 - C. the CCAR required disclosure of macro-level, not bank level, scenario results.
 - D. the EBA Irish allowed for 1-year stress horizons.

KEY CONCEPTS

LO 51.a

After the 2007–2009 financial crisis, it was clear that traditional risk measures such as regulatory capital ratios were insufficient. Supervisory stress-testing became an important risk-assessment tool at that point.

The goal of stress testing is to assess how much capital and liquidity a financial institution needs to support its business (i.e., risk taking) activities.

The 2009 U.S. bank stress test, known as the Supervisory Capital Assessment Program (SCAP), was the first macro-prudential stress test after the 2007–2009 financial crisis.

Disclosure was a significant feature of the 2009 SCAP. This high level of disclosure led to transparency and allowed investors and the market the ability to check the severity of the stress tests and the outcomes of the stress at the individual bank level.

In 2011, CCAR required only macro-scenario results be published, not bank level results, differing significantly from the 2009 SCAP requirements. The 2012 CCAR disclosed virtually the same amount and detail of bank level stress data as the 2009 SCAP. The EBA Irish and the EBA Europe required significant disclosures as well. The disclosures were needed to increase trust in the European banking system.

LO 51.b

One of the challenges regulators face is designing coherent stress tests. The sensitivities and scenarios must be extreme but must also be reasonable and possible (i.e., coherent). Problems are inherently multi-factor, making it more difficult to design a coherent stress test.

LO 51.c

Current stress tests are based on macro-scenarios (i.e., unemployment, GDP growth, the HPI). One concern is how to translate the macro-risk factors employed in stress tests into micro (i.e., bank specific) outcomes related to revenues and losses. Supervisors must be able to map from macro-factors into intermediate risk factors that drive losses in specific products and geographic areas.

In a stress model, the starting balance sheet generates the first quarter's income and loss from the stressed scenario, which in turn determines the quarter-end balance sheet. The bank must maintain its capital (and liquidity) ratios during all quarters of the stress test horizon, typically two years.

ANSWER KEY FOR MODULE QUIZZES

Module Quiz 51.1

1. **A** The 2009 U.S. bank stress test, known as the Supervisory Capital Assessment Program (SCAP), was the first macro-prudential stress test after the 2007–2009 financial crisis. (LO 51.a)

Module Quiz 51.2

1. **C** One of the challenges of designing useful stress tests is coherence. The sensitivities and scenarios must be extreme but must also be reasonable or possible (i.e., coherent). Problems are inherently multi-factored, making it more difficult to design a coherent stress test. Hook is dealing with the possibly incoherent results of the bank's stress tests. (LO 51.b)
2. **B** Credit card losses are particularly sensitive to unemployment figures. For example, unemployment was 12.9% in Nevada in July 2011, 3.3% in North Dakota, and the national unemployment rate was 9.1%. Credit card loss rates varied dramatically from region to region during this period. Residential mortgages are affected by unemployment as well but people are generally more likely to quit paying credit card bills before mortgages. (LO 51.c)
3. **D** In a stress model, the starting balance sheet generates the first quarter's income and loss from the stressed scenario, which in turn determines the quarter-end balance sheet. At that point, the person modeling the risk must consider if any assets will be sold or originated, if capital is depleted due to other actions such as acquisitions or conserved as the result of a spin-off, if there are changes made to dividend payments, if shares will be repurchased or issued (e.g., employee stock or stock option programs), and so on. This makes it challenging to model the balance sheet over the stress horizon. (LO 51.c)
4. **C** The 2011 CCAR required banks to provide results from their own stress scenarios but the EBA Irish did not. After the 2011 EBA Irish tests, €24 billion was required to increase the capital of several banks. The 2011 CCAR, unlike the SCAP and the 2012 CCAR, only required the disclosure of macro-level scenario results. The EBA Irish did not change the stress horizon from two years to one year. (LO 51.c)

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 assigned reading—Crouhy, Galai, and Mark, Chapter 17.

READING 52

RISK CAPITAL ATTRIBUTION AND RISK-ADJUSTED PERFORMANCE MEASUREMENT

Study Session 9

EXAM FOCUS

This reading covers the application of the risk-adjusted return on capital (RAROC) approach to the allocation of economic capital. The application of a hurdle rate for capital budgeting decisions as well as an adjusted version of the traditional RAROC approach is also presented. For the exam, know the differences between economic capital and regulatory capital, and be able to compute RAROC for capital budgeting as well as adjusted RAROC. Also, be familiar with the qualitative concepts discussed, such as reasons for using economic capital to allocate risk capital, the benefits of RAROC, and best practices in implementing the RAROC approach.

MODULE 52.1: RISK-ADJUSTED RETURN ON CAPITAL

Risk Capital, Economic Capital, and Regulatory Capital

LO 52.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.

Risk capital provides protection against risk (i.e., unexpected losses). In other words, it can be defined as a (financial) buffer to shield a firm from the economic impact of risks taken. Should a disastrous event occur, those impacts could otherwise jeopardize the firm's financial security and its ability to remain a going concern. In short, risk capital provides assurance to the firm's stakeholders that their invested funds are safe. In most cases, risk capital and **economic capital** are treated synonymously, although an alternative definition of economic capital exists (discussed further in LO 52.c):

$$\text{economic capital} = \text{risk capital} + \text{strategic risk capital}$$

On the other hand, there are at least three distinct differences between risk capital and **regulatory capital** as follows:

1. Unlike risk capital, regulatory capital is relevant only for regulated industries such as banking and insurance.
2. Regulatory capital is computed using general benchmarks that apply to the industry. The result is a minimum required amount of capital adequacy that is usually far below the firm's risk capital.
3. Assuming that risk capital and regulatory capital are the same for the overall firm, the amounts may be different within the various divisions of the firm. From a risk capital allocation perspective, one solution is to allocate the greater of risk capital and regulatory capital to a certain division.



PROFESSOR'S NOTE

We will examine the regulatory capital charges for credit, market, and operational risk in Reading 55.

Given that Basel III requirements are sufficiently robust, it is probable that in certain areas (e.g., securitization), regulatory capital will be substantially higher than risk/economic capital. Although the two amounts may conflict, risk/economic capital must be computed in order to determine the economic viability of an activity or division. Assuming that regulatory capital is substantially higher than risk/economic capital for a given activity, then that activity will potentially move over to shadow banking (i.e., unregulated activities by regulated financial institutions) in order to provide more favorable pricing.

Using Economic Capital Approaches

From the perspective of financial institutions, the motivations for using economic capital are as follows:

Capital is used extensively to cushion risk. Compared to most other nonfinancial institutions, financial institutions can become highly leveraged (i.e., riskier) at a relatively low cost simply by accepting customer deposits or issuing debt. All of this may occur without having to issue equity. Additionally, many of the financial institutions will participate in transactions involving derivatives, guarantees, and other commitments that only require a relatively small amount of funding but always involve some risk. As a result, all of the firm's activities must be allocated an economic capital cost.

Financial institutions must be creditworthy. A unique aspect of financial institutions is that their main customers are also their main liability holders. Customers who deposit funds to a financial institution will be concerned about the default risk of the financial institution. With over-the-counter (OTC) derivatives, the concern is counterparty risk. As a result, a sufficient amount of economic capital must be maintained to provide assurance of creditworthiness.

There is difficulty in providing an external assessment of a financial institution's creditworthiness. It is challenging to provide an accurate credit assessment of a financial institution because its risk profile is likely to be constantly evolving. For example, an institution may engage in complicated hedging and derivatives transactions

that could rapidly impact its liquidity. Therefore, having a sufficient store of economic capital could mitigate this problem and provide assurance of financial stability.

Profitability is greatly impacted by the cost of capital. Economic capital is similar to equity capital in the sense that the invested funds do not need to be repaid in the same manner as debt capital, for instance. In other words, economic capital serves as a reserve or a financial cushion in case of an economic downturn. As a result, economic capital is more expensive to hold than debt capital, thereby increasing the cost of capital and reducing the financial institution's profits. A proper balance between holding sufficient economic capital and partaking in risky transactions is necessary.

Risk-Adjusted Return on Capital

LO 52.b: Describe the risk-adjusted return on capital (RAROC) methodology and its use in capital budgeting.

The **risk-adjusted return on capital (RAROC)** methodology provides users with information pertaining to the risk-adjusted performance of the firm and its business units as opposed to merely the “raw” performance numbers. In measuring economic performance, this methodology involves allocating risk capital to the firm's business units and to specific transactions.

Benefits of RAROC include:

1. Performance measurement using economic profits instead of accounting profits. Accounting profits include historical and arbitrary measures such as depreciation, which may be less relevant.
2. Use in computing increases in shareholder value as part of incentive compensation (e.g., scorecards) within the firm and its divisions. The flexibility of RAROC may also allow for deferred/contingent compensation or clawbacks for subsequent poor performance.
3. Use in portfolio management for buy and sell decisions and use in capital management in estimating the incremental value-added through a new investment or discontinuing an existing investment.
4. Using risk-based pricing, which will allow proper pricing that takes into account the economic risks undertaken by a firm in a given transaction. Each transaction must consider the expected loss and the cost of economic capital allocated. Many firms use the “marginal economic capital requirement” portion of the RAROC equation for the purposes of pricing and determining incremental shareholder value.

LO 52.c: Compute and interpret the RAROC for a project, loan, or loan portfolio and use RAROC to compare business unit performance.

The necessary amount of economic capital is a function of credit risk, market risk, and operational risk. The RAROC for a project or loan can be defined as risk-adjusted return divided by risk-adjusted capital. The basic RAROC equation is as follows:

$$\text{RAROC} = \frac{\text{after-tax expected risk-adjusted net income}}{\text{economic capital}}$$

There is a tradeoff between risk and return per unit of capital with the numerator acting as return and the denominator acting as risk. For example, a business unit's RAROC needs to be greater than its cost of equity in order to create shareholder value.

Furthermore, measures such as return on equity (ROE) or return on assets (ROA) are based on accounting book values only, and therefore are unable to account for the relevant risks. RAROC has two specific adjustments to these measures. In the numerator, it deducts expected loss (the risk factor) from the return. In the denominator, it replaces accounting capital with economic capital.

The underlying principles of the RAROC equation are similar to two other common measures of risk/return: (1) the Sharpe ratio, which equals: (expected return – risk-free rate) / standard deviation, and (2) the net present value (NPV), which equals the discounted value of future expected after-tax cash flows. The discount rate for the NPV is a risk-adjusted expected return that uses beta (captures systematic risk only) from the capital asset pricing model (CAPM). In contrast to NPV, RAROC takes into account both systematic and unsystematic risk in its earnings figure.

A more detailed RAROC equation to use for capital budgeting decisions is as follows:

$$\text{RAROC} = \frac{\left(\begin{array}{l} \text{expected revenues} - \text{costs} - \text{expected losses} \\ - \text{taxes} + \text{return on economic capital} \pm \text{transfers} \end{array} \right)}{\text{economic capital}}$$

where:

- *Expected revenues* assume no losses and *costs* refer to direct costs. *Taxes* are computed using the firm's effective tax rate and *transfers* include head office overhead cost allocations to the business unit as well as transactions between the business unit and the Treasury group, such as borrowing and hedging costs.
- *Expected losses* (EL) consist mainly of expected default losses (i.e., loan loss reserve), which are captured in the numerator (i.e., higher funding cost) so there is no adjustment required in the denominator. Expected losses also arise due to market, operational, and counterparty risks.
- *Return on economic capital* refers to the return on risk-free investments based on the amount of allocated risk capital.
- *Economic capital* includes both risk capital and strategic risk capital.

Risk capital serves as a buffer against unexpected losses. It is the amount of funds that the firm must hold in reserve to cover a worst-case loss (an amount over the expected loss) at a specific confidence level that is usually 95% or more. Therefore, it is very similar to the annual value at risk (VaR).

Strategic risk capital pertains to the uncertainty surrounding the success and profitability of certain investments. An unsuccessful investment could result in financial losses and a negative reputational impact on the firm. Strategic risk capital includes goodwill and burned-out capital.

- **Goodwill** is the excess of the purchase price over the fair value (or replacement value) of the net assets recorded on the balance sheet. A premium price may exist

because of the existence of valuable but unrecorded intangible assets.

- **Burned-out capital** represents the risk of amounts spent during the start-up phase of a venture that may be lost if the venture is not pursued because of low projected risk-adjusted returns. The venture may refer to a recent acquisition or an internally generated project. Burned-out capital is amortized over time as the strategic failure risk decreases.

Finally, firms may allocate risk capital to any unused risk limits (e.g., undrawn amounts on a line of credit) because risk capacity could be utilized any time. If risk capacity is utilized, the firm would then have to adjust the risk capital amount.

As mentioned, economic capital is designed to provide a cushion against *unexpected losses* at a specified confidence level. The confidence level at which economic capital is set can be viewed as the probability that the firm will be able to absorb unexpected losses over a specified period. A simple example can help illustrate the concept of unexpected loss and how it is equal to the risk capital allocation. Assume for a given transaction that the expected loss is 20 basis points (bps) and the worst-case loss is 190 bps at a 95% confidence level over one year. Based on this information, the unexpected loss is 170 bps (excess of worst-case loss over expected loss). There is also still a 5% probability that the actual loss will exceed 190 bps.

EXAMPLE: RAROC calculation

Assume the following information for a commercial loan portfolio:

- \$1.5 billion principal amount
- 7% pre-tax expected return on loan portfolio
- Direct annual operating costs of \$10 million
- Loan portfolio is funded by \$1.5 billion of retail deposits; interest rate = 5%
- Expected loss on the portfolio is 0.5% of principal per annum
- Unexpected loss of 8% of the principal amount, or \$120 million of economic capital required
- Risk-free rate on government securities is 1% (based on the economic capital required)
- 25% effective tax rate
- Assume no transfer pricing issues

Compute the RAROC for this loan portfolio.

Answer:

First, calculate the following RAROC components:

Expected revenue = $0.07 \times \$1.5 \text{ billion} = \105 million

Interest expense = $0.05 \times \$1.5 \text{ billion} = \75 million

Expected loss = $0.005 \times \$1.5 \text{ billion} = \7.5 million

Return on economic capital = $0.01 \times \$120 \text{ million} = \1.2 million

Then, apply the RAROC equation:

$$\text{RAROC} = \frac{(105 - 10 - 75 - 7.5 + 1.2 + 0) \times (1 - 0.25)}{120} = 8.56\%$$

Therefore, maintenance of the commercial loan portfolio requires an after-tax expected rate of return on equity of at least 8.56%.

Note that for capital budgeting projects, *expected* revenues and losses should be used in the numerator since the analysis is being performed on an ex ante (or before the fact) basis. In contrast, for performance evaluation purposes on an ex post (or after the fact) basis, *realized* (or actual) revenues and losses should be used.



MODULE QUIZ 52.1

1. Which of the following statements regarding the risk-adjusted return on capital (RAROC) methodology is correct?
 - A. In the context of performance measurement, RAROC uses accounting profits.
 - B. In the numerator of the RAROC equation, expected loss is added to the return.
 - C. If a business unit's cost of equity is greater than its RAROC, then the business unit is not adding value to shareholders.
 - D. RAROC is useful for determining incentive compensation but it lacks the flexibility to consider deferred or contingent compensation.
2. Assume the following information for a commercial loan portfolio:
 - \$1.2 billion principal amount
 - 6% pre-tax expected return on loan portfolio
 - Direct annual operating costs of \$8 million
 - Loan portfolio funded by \$1.2 billion of retail deposits; interest rate = 4%
 - Expected loss on the portfolio is 0.4% of principal per annum
 - Unexpected loss of 7% of the principal amount
 - Risk-free rate on government securities is 1%
 - 30% effective tax rate
 - Assume no transfer pricing issuesBased on the information provided, which of the following amounts is closest to the RAROC?
 - A. 9.33%.
 - B. 10.03%.
 - C. 12.33%.
 - D. 14.66%.

MODULE 52.2: RAROC, HURDLE RATE, AND ADJUSTED RAROC

RAROC for Performance Measurement

LO 52.d: Explain challenges that arise when using RAROC for performance measurement, including choosing a time horizon, measuring default probability, and choosing a confidence level.

Time Horizon

In computing RAROC, the focus so far has been on one period (i.e., one-year time horizon) since it is convenient from a business planning cycle perspective and it

represents the probable amount of time needed for a firm to recover from a significant unexpected loss. At the same time, it is possible to look at multi-period RAROC to obtain a more accurate RAROC measure for longer-term transactions and loans. One issue that arises is how much economic capital to allocate if the risk of a transaction changes dramatically in subsequent periods. For example, using an averaging method would give rise to periods of overcapitalization and periods of undercapitalization.

Risk capital could be thought of as the firm's one-year VaR at a specific confidence level (e.g., 95% or 99%). For both credit risk and operational risk, no adjustments are required from one-year VaR to compute risk capital. For market risk, short time horizons such as one day (risk monitoring) or 10 days (regulatory capital) require adjustments to determine the correct one-year risk capital allocation.

One basic approach is the "square root of time" rule whereby one-year VaR is estimated by multiplying the one-day VaR by the square root of 252 business days in the year. This approach needs to be fine-tuned by considering that even in a worst-case scenario, the firm might only be able to reduce its risk to a core risk level to retain its status as a financially viable business for the rest of the year. Furthermore, the computation must also factor in the time needed to lower the current risk level to the core risk level (i.e., "time to reduce"). That amount of time corresponds to the relative liquidity (during difficult market conditions) of the firm's investment positions taken. As a result, a large amount of time may be required for a reasonable liquidation of the positions.

EXAMPLE: Risk capital for market risk

Assume the following information where the core risk level is below the current risk level:

- Daily value at risk (VaR) = 80
- Core risk level = 60
- Days needed to reduce current risk level to core risk level = 10 (i.e., risk reduction of 2 VaR per day)
- Number of business days per year = 252

Compute the required risk capital as a percentage of annualized VaR.

Answer:

Risk capital =

$$\begin{aligned}
 & \text{square root} \left\{ \begin{array}{l} \text{sum of squares +} \\ \left[\text{core risk level squared} \times (\text{number of business days per year} - \right. \right. \\ \left. \left. \text{days needed to reduce current to core}) \right] \end{array} \right\} \\
 &= \text{square root} \left\{ (80^2 + 78^2 + 76^2 + 74^2 + 72^2 + 70^2 + 68^2 + 66^2 + 64^2 + 62^2) + \right. \\
 & \quad \left. [60^2 \times (252 - 10)] \right\} \\
 &= \text{square root} [50,740 + (3,600 \times 242)] \\
 &= \sqrt{921,940} = 960.18
 \end{aligned}$$

Note that annualized VaR = 80 × square root of 252 = 1,269.96

Therefore, the risk capital required is approximately 75.6% of annualized VaR (= 960.18 / 1,269.96).

There is a lot of subjectivity in selecting the time horizon for RAROC calculation purposes. A longer time horizon could be selected to account for the full business cycle; it may not always increase the risk capital required since the confidence level required to maintain a firm's solvency will fall as the time horizon is increased. A key consideration with the selection of a time horizon is the fact that risk and return data for periods over one year is likely to be of questionable reliability.

Default Probability

A **point-in-time (PIT)** probability of default could be used to compute short-term expected losses and to price financial instruments with credit risk exposure. A **through-the-cycle (TTC)** probability of default is more commonly used for computations involving economic capital, profitability, and strategic decisions.

A firm's rating is more likely to change when analyzed under the PIT approach versus the TTC approach. As a result, the TTC approach results in a lower volatility of economic capital versus the PIT approach. From time to time, it is advisable to compare the result of PIT versus TTC for RAROC computations at a stable portion of the economic cycle and at the lowest portion of the cycle.

Confidence Level

In computing economic capital, the confidence level chosen must correspond with the firm's desired credit rating. A high rating such as AA or AAA would require a confidence level in excess of 99.95%, for example. Choosing a lower confidence level will reduce the amount of risk capital required/allocated and it will impact the risk-adjusted performance measures. The reduction may be dramatic if the firm is primarily exposed to operational, credit, and settlement risks where large losses are rare.

Hurdle Rate for Capital Budgeting Decisions

LO 52.e: Calculate the hurdle rate and apply this rate in making business decisions using RAROC.

Similar to internal rate of return (IRR) analysis, the use of a **hurdle rate** (i.e., after-tax weighted average cost of equity capital) is compared to RAROC in making business decisions. In general, the hurdle rate should be revised perhaps once or twice a year or when it has moved by over 10%.

The hurdle rate, h_{AT} , is computed as follows:

$$h_{AT} = \frac{[(CE \times R_{CE}) + (PE \times R_{PE})]}{(CE + PE)}$$

where:

CE = market value of common equity

PE = market value of preferred equity

R_{CE} = cost of common equity (could be derived from the capital asset pricing model [CAPM])

R_{PE} = cost of preferred equity (yield on preferred shares)

Recall, that the CAPM formula is as follows:

$$R_{CE} = R_F + \beta_{CE}(R_M - R_F)$$

where:

R_F = risk-free rate

R_M = expected return on market portfolio

β_{CE} = firm's common equity market beta

Once the hurdle rate and the RAROC are calculated, the following rules apply:

- If RAROC > hurdle rate, there is value creation from the project and it should be accepted.
- If RAROC < hurdle rate, there is value destruction from the project and it should be rejected/discontinued.

Obviously, a shortcoming of the above rules is that higher return projects that have a RAROC > hurdle rate (accepted projects) also come with high risk that could ultimately result in losses and reduce the value of the firm. In addition, lower return projects that have a RAROC < hurdle rate (rejected projects) also come with low risk that could provide steady returns and increase the value of the firm. As a result, an adjusted RAROC measure should be computed.

Adjusted RAROC

LO 52.f: Compute the adjusted RAROC for a project to determine its viability.

RAROC should be adjusted to consider systematic risk and a consistent hurdle rate.

$$\text{Adjusted RAROC} = \text{RAROC} - \beta_E (R_M - R_F)$$

where:

R_F = risk-free rate = hurdle rate

R_M = expected return on market portfolio

β_E = firm's equity beta

$(R_M - R_F)$ = excess return over risk-free rate to account for the nondiversifiable systematic risk of the project

Therefore, the revised business decision rules are as follows:

- If adjusted RAROC > R_F , then accept the project
- If adjusted RAROC < R_F , then reject the project

EXAMPLE: Adjusted RAROC

Suppose RAROC is 12%, the risk-free rate is 5%, the market return is 11%, and the firm's equity beta is 1.5. Use ARAROC to **determine** whether the project should be accepted or rejected.

Answer:

$$\text{Adjusted RAROC} = \text{RAROC} - \beta_E (R_M - R_F)$$

$$= 0.12 - 1.5(0.11 - 0.05) = 0.12 - 0.09 = 0.03$$

The project should be rejected because the ARAROC of 3% is less than the risk-free rate of 5%.



MODULE QUIZ 52.2

1. Which of the following statements regarding the computation of economic capital is correct?
 - I. Selecting a longer time horizon for RAROC calculations is preferable because risk and return data is more reliable with more time.
 - II. Choosing a lower confidence level will not likely reduce the amount of risk capital required if the firm has little exposure to operational, credit, and settlement risks.

A. I only.
B. II only.
C. Both I and II.
D. Neither I nor II.
2. Which of the following statements regarding the choice of default probability approaches in computing economic capital is correct?
 - A. A through-the-cycle (TTC) approach should be used to price financial instruments with credit risk exposure.
 - B. A point-in-time (PIT) approach is more commonly used for computations involving profitability and strategic decisions.
 - C. A TTC approach is more likely to result in a lower volatility of capital compared to the PIT approach.
 - D. A firm's rating will not change when analyzed under the PIT approach versus the TTC approach.

MODULE 52.3: DIVERSIFICATION BENEFITS AND RAROC BEST PRACTICES

Risk Capital and Diversification

LO 52.g: Explain challenges in modeling diversification benefits, including aggregating a firm's risk capital and allocating economic capital to different business lines.

The overall risk capital for a firm should be less than the total of the individual risk capitals of the underlying business units. That is because the correlation of returns between the business units is likely to be less than +1. Such risk reduction due to diversification effects over risk types and business activities is very difficult to measure in practice. Instead of using an extremely high overall confidence level for the firm, the various business units may use lower confidence levels to avoid an excessively high aggregate risk capital amount.

For example, assume a firm is subject to only the following four types of risk (risk capital amounts are provided for each risk):

- Market risk = \$400

- Credit risk = \$300
- Liquidity risk = \$200
- Operational risk = \$500

Aggregate risk capital for the firm could be as high as \$1,400 assuming a perfect correlation (i.e., sum of the four risk capital amounts). Or it could be as low as \$734 assuming zero correlation (square root of the sum of squares of the four risk capital amounts). In taking into account the diversification effects, the firm's overall VaR should be computed as some value between \$734 and \$1,400, which is a very wide range. In addition, there is a lot of subjectivity involved in allocating the diversification benefits back to the business units in a fair manner especially since the allocation will impact the respective business units' performance measures (i.e., reduction of risk capital required).

It makes sense that a business unit with earnings or cash flows that are highly correlated to the overall firm would need to be allocated more risk capital than a business unit with earnings or cash flows that are negatively correlated (assuming similar volatility). Having business lines that are countercyclical in nature allows the overall firm to have stable earnings and to attain a given desired credit rating using less risk capital. In practice, the easiest allocation method is a pro-rata allocation based on stand-alone risk capital amounts.

For example, assume the following information pertaining to a business unit that engages in only two activities, A and B:

- Activity A alone requires \$50 of risk capital
- Activity B alone requires \$60 of risk capital
- Activities A and B together require a total of \$90 of risk capital

Stand-alone capital looks at each activity independently and ignores any diversification benefits. Therefore, the stand-alone capital for Activities A and B are \$50 and \$60, respectively. The stand-alone capital for the business unit is \$90.

Fully diversified capital takes into consideration the diversification benefits, which equal \$20 ($= \$50 + \$60 - \90). For simplicity, the diversification benefit can be done on a pro-rata basis as follows: $(\$20 \times \$50) / \$110 = \9.1 is allocated to Activity A and $(\$20 \times \$60) / \$110 = \10.9 is allocated to Activity B. Therefore, Activities A and B have fully diversified capital of \$40.9 and \$48.1, respectively. Fully diversified capital should be used to determine a firm's solvency and to determine the minimum amount of risk capital required for a given activity.

Marginal capital is the extra capital needed as a result of a new activity added to the business unit. Diversification benefits are fully considered. The marginal risk capital for Activity A is \$30 ($= \$90 \text{ total} - \$60 \text{ for Activity B}$) and the marginal risk capital for Activity B is \$40 ($= \$90 \text{ total} - \$50 \text{ for Activity A}$). Total marginal risk capital (\$70) is below the full risk capital of the business unit (\$90). The general method for computing marginal capital of a new activity is to start with the total risk capital required for the business unit minus all of the risk capital required for the other activities. Marginal capital is useful for making active portfolio management and business mix decisions; such decisions need to fully consider diversification benefits.

In a performance measurement context, stand-alone risk capital is useful to determine incentive pay and fully diversified risk capital is useful to determine the incremental benefit due to diversification. In allocating the diversification benefits, caution must be taken especially since correlations between the risk factors usually change over time. In a more extreme situation such as a market crisis, correlations could move to -1 or $+1$, thereby reducing diversification benefits.

RAROC Best Practices

LO 52.h: Explain best practices in implementing an approach that uses RAROC to allocate economic capital.

Recommendations for implementing a RAROC approach are as follows:

Senior Management

The management team (including the CEO) needs to be actively involved with the implementation of a RAROC approach within the firm and promote it as a means of measuring shareholder value creation. The emphasis should be on the level of profits earned by the firm in relation to the level of risks taken as opposed to merely earning as much profit as possible.

Communication and Education

The RAROC process needs to be clearly explained to all levels of management of the firm in order to have sufficient “buy in” from management. Specifically, the process of allocating economic capital to the various business units needs to be fair and transparent in order to minimize the common concerns of excessive economic capital attribution to a given business unit. An open dialogue and debate with the various business unit leaders of issues concerning how economic capital is computed would also be helpful.

Ongoing Consultation

There are key metrics that impact the computation of economic capital. A committee consisting of members from the various business units as well as the risk management group should review these metrics periodically in order to promote fairness in the capital allocation process.

Metrics involving credit risk include: probability of default, credit migration frequencies, loss given default, and credit line usage given default. The metrics will change with time and will need to be updated accordingly. The historical period over which the metrics are adjusted is debatable—a shorter period may result in fluctuating economic capital amounts and a longer period may result in more stable amounts.

Metrics involving market risk focus on volatility and correlation, and should be updated at least monthly. Metrics involving operational risk are not as defined as they are for credit and market risk, so therefore, involve a significant amount of subjectivity and debate. Other key metrics, like core risk level and time to reduce, should be updated annually.

Data Quality Control

Information systems collect data (e.g., risk exposures and positions) required to perform the RAROC calculations. The data collection process should be centralized with built-in edit and reasonability checks to increase the accuracy of the data. In subdividing the general duties surrounding data, the RAROC team should be responsible for the data collection process, the computations, and the reporting. The business units and the accounting department should be responsible for putting controls in place to ensure the accuracy of the data being used for the RAROC calculations.

Complement RAROC With Qualitative Factors

A qualitative assessment of each business unit could be performed using a four-quadrant analysis. The horizontal axis would represent the expected RAROC return and the vertical axis would represent the quality of the earnings based on the importance of the business unit's activities to the overall firm, growth opportunities, long-run stability and volatility of earnings, and any synergies with other business units. There are four resulting possibilities:

- Low quality of earnings, low quantity of earnings: the firm should try to correct, reduce, or shut down the activities of any of its business units in this category.
- Low quality of earnings, high quantity of earnings (managed growth): the firm should maintain any business units that currently produce high returns but have low strategic importance to the firm.
- High quality of earnings, low quantity of earnings (investment): the firm should maintain any business units that currently produce low returns but have high strategic value and high growth potential.
- High quality of earnings, high quantity of earnings: the firm should allocate the most resources to business units in this category.

Active Capital Management

Business units should submit their limit requests (e.g., economic capital, leverage, liquidity, risk-weighted assets) quarterly to the RAROC team. The RAROC team performs the relevant analysis and sets the limits in a collaborative manner that allows business units to express any objections. Senior management will then make a final decision. The Treasury group will ensure the limits make sense in the context of funding limits. The restriction placed on a firm's growth due to leverage limitations helps promote the optimal use of the limited amount of capital available.



MODULE QUIZ 52.3

1. Which of the following statements regarding best practices in implementing a RAROC approach is correct?
 - A. A successful RAROC approach is focused on maximizing profits earned by the firm.
 - B. A restriction on the firm's growth due to leverage limitations may result in higher profits.
 - C. The data collection process throughout the firm should be decentralized to allow the various business units to ensure the utmost accuracy of data.

D. Metrics involving credit risk, market risk, and operational risk to compute economic capital are generally clearly defined and may be computed objectively.

KEY CONCEPTS

LO 52.a

Risk capital is a buffer to shield a firm from the economic impacts of the risks that it takes (i.e., protect against unexpected losses). In short, it provides assurance to the firm's stakeholders that their invested funds are safe.

In most cases, risk capital and economic capital are identical; however, strategic risk capital may be added to economic capital as follows:

$$\text{economic capital} = \text{risk capital} + \text{strategic risk capital}$$

Regulatory capital is relevant only for regulated industries such as banking and insurance. It is computed using general benchmarks that apply to the industry. Assuming that risk capital and regulatory capital are the same for the overall firm, the amounts may be different within the various divisions of the firm.

For financial institutions, there are four major reasons for using economic capital to allocate risk capital:

- Capital is used extensively to cushion risk.
- Financial institutions must be creditworthy.
- Difficulty in providing an external assessment of a financial institution's creditworthiness.
- Profitability is greatly impacted by the cost of capital.

LO 52.b

Benefits of using the risk-adjusted return on capital (RAROC) approach include:

1. Performance measurement using economic profits instead of accounting profits.
2. Use in computing increases in shareholder value as part of incentive compensation (e.g., scorecards) within the firm and its divisions.
3. Use in portfolio management for buy and sell decisions and use in capital management in estimating the incremental value-added through a new investment or discontinuing an existing investment.
4. Using risk-based pricing, which will allow proper pricing that takes into account the economic risks undertaken by a firm in a given transaction.

LO 52.c

The basic RAROC equation is as follows:

$$\text{RAROC} = \frac{\text{after-tax expected risk-adjusted net income}}{\text{economic capital}}$$

A more detailed RAROC equation for capital budgeting decisions is as follows:

$$\text{RAROC} = \frac{\left(\begin{array}{l} \text{expected revenues} - \text{costs} - \text{expected losses} \\ - \text{taxes} + \text{return on economic capital} \pm \text{transfers} \end{array} \right)}{\text{economic capital}}$$

LO 52.d

In computing RAROC, the focus is often on a one-year time horizon. However, it is possible to look at multi-period RAROC to obtain a more accurate RAROC measure for longer-term transactions and loans. One issue that arises is how much economic capital to allocate if the risk of a transaction changes dramatically in subsequent periods. There is a lot of subjectivity in selecting the time horizon for RAROC calculation purposes. A longer time horizon could be selected to account for the full business cycle, for example. A key consideration with the selection of a time horizon is the fact that risk and return data for periods over one year is likely to be of questionable reliability.

A point-in-time (PIT) probability of default could be used for short-term expected losses and to price financial instruments with credit risk exposure. A through-the-cycle (TTC) probability of default is more commonly used for computations involving economic capital, profitability, and strategic decisions.

In computing economic capital, the confidence level chosen must correspond with the firm's desired credit rating. Choosing a lower confidence level will reduce the amount of risk capital required/allocated and it will impact risk-adjusted performance measures.

LO 52.e

The hurdle rate is computed as follows:

$$h_{AT} = \frac{[(CE \times R_{CE}) + (PE \times R_{PE})]}{(CE + PE)}$$

Once the hurdle rate and the RAROC are calculated, the following rules apply:

- If RAROC > hurdle rate, there is value creation from the project and it should be accepted.
- If RAROC < hurdle rate, there is value destruction from the project and it should be rejected/discontinued.

LO 52.f

RAROC should be adjusted to take into account systematic risk and a consistent hurdle rate as follows:

$$\text{Adjusted RAROC} = \text{RAROC} - \beta_E (R_M - R_F)$$

LO 52.g

The overall risk capital for a firm should be less than the total of the individual risk capitals of the underlying business units. This is because the correlation of returns between business units is likely to be less than +1.

A business unit with earnings or cash flows that are highly correlated to the overall firm should be allocated more risk capital than a business unit with earnings or cash flows that are negatively correlated (assuming similar volatility). Having business lines that are countercyclical in nature allows the overall firm to have stable earnings and to attain a given desired credit rating using less risk capital.

LO 52.h

The management team needs to be actively involved with the implementation of a RAROC approach within the firm and promote it as a means of measuring shareholder

value creation.

The RAROC process needs to be clearly explained to all levels of management of the firm in order to have sufficient “buy in” from management.

A committee consisting of members from the various business units as well as the risk management group should periodically review the metrics that impact economic capital calculations in order to promote fairness in the capital allocation process.

The RAROC team should be responsible for the data collection process, the computations, and the reporting. The business units and the accounting department should be responsible for putting controls in place to ensure the accuracy of the data being used for the RAROC calculations.

A qualitative assessment of each business unit could be performed using a four-quadrant analysis. The horizontal axis would represent the expected RAROC return and the vertical axis would represent the quality of the earnings based on the importance of the business unit’s activities to the overall firm, growth opportunities, long-run stability and volatility of earnings, and any synergies with other business units.

Business units should submit their limit requests (e.g., economic capital, leverage, liquidity, risk-weighted assets) quarterly to the RAROC team. The RAROC team performs the relevant analysis and sets the limits in a collaborative manner that allows business units to express any objections.

ANSWER KEY FOR MODULE QUIZZES

Module Quiz 52.1

1. **C** The cost of equity represents the minimum rate of return on equity required by shareholders. Therefore, if RAROC is below the cost of equity, then there is no value being added.

Response A is not correct because RAROC uses economic profits, not accounting profits. Response B is not correct because in the numerator of the RAROC equation, expected loss is deducted from the return. Response D is not correct because RAROC has the flexibility to consider deferred or contingent compensation. (LO 52.c)

2. **B** Unexpected loss (\$1.2 billion × 7% = \$84 million) is equal to the amount of economic capital required. The return on economic capital is then \$84 million × 1% = \$0.84 million. Also, expected revenues = 0.06 × \$1.2 billion = \$72 million; interest expense = 0.04 × \$1.2 billion = \$48 million; expected losses = 0.004 × \$1.2 billion = \$4.8 million.

$$\text{RAROC} = \frac{\left(\begin{array}{l} \text{expected revenues} - \text{costs} - \text{expected losses} \\ - \text{taxes} + \text{return on economic capital} \pm \text{transfers} \end{array} \right)}{\text{economic capital}}$$
$$\text{RAROC} = \frac{(72 - 8 - 48 - 4.8 + 0.84 + 0) \times (1 - 0.3)}{84} = 10.03\%$$

(LO 52.c)

Module Quiz 52.2

1. **B** Choosing a lower confidence level will not likely reduce the amount of risk capital required if the firm has little exposure to operational, credit, and settlement risks. The reduction would be much more dramatic only if the firm has significant exposure to such risks because large losses would be rare.

In selecting a time horizon for RAROC calculations, risk and return data for periods over one year is likely to be of questionable reliability. (LO 52.d)

2. **C** A firm's rating is more likely to change when analyzed under the point-in-time (PIT) approach compared to the through-the-cycle (TTC) approach. As a result, the TTC approach results in a lower volatility of economic capital compared to the PIT approach.

A PIT approach should be used to price financial instruments with credit risk exposure and to compute short-term expected losses. A TTC approach is more commonly used for computations involving profitability, strategic decisions, and economic capital. (LO 52.d)

Module Quiz 52.3

1. **B** A restriction on the firm's growth due to leverage limitations may result in higher profits because it requires the firm to be "creative" and to optimize a scarce resource (the limited amount of capital available).

Response A is not correct. A successful RAROC approach is focused on the level of profits earned by the firm in relation to the level of risks taken. Response C is not correct. The data collection process should be the responsibility of the RAROC team; the process should be centralized with built-in edit and reasonability checks to increase the accuracy of the data. Response D is not correct. Metrics involving operational risk are not as defined as credit and market risk, therefore, there is often a significant amount of subjectivity involved in the computations. (LO 52.h)

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 assigned reading—Basel Committee on Banking Supervision.

READING 53

RANGE OF PRACTICES AND ISSUES IN ECONOMIC CAPITAL FRAMEWORKS

Study Session 9

EXAM FOCUS

This reading requires an understanding of many risk management concepts that you have already covered at FRM Part I, as well as in earlier readings in the FRM Part II curriculum. Specifically, this reading expands on the concept of economic capital, which is the capital required to absorb unexpected losses for a given time horizon and confidence interval. For the exam, pay attention to the terminology and attempt to integrate this material to the sections pertaining to market risk and credit risk so as to reinforce your understanding.

MODULE 53.1: RISK MEASURES AND RISK AGGREGATION

LO 53.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**
-

For this LO, it would be helpful to recall the properties of a **coherent risk measure** from the Part I curriculum. The properties are as follows:

1. **Monotonicity:** A portfolio with greater future returns will likely have less risk.
2. **Subadditivity:** The risk of a portfolio is at most equal to the risk of the assets within the portfolio.
3. **Positive homogeneity:** The size of a portfolio will impact the size of its risk.

4. **Translation invariance:** The risk of a portfolio is dependent on the assets within the portfolio.

Defining and Calculating Risk Measures

It is not always apparent how risk should be quantified for a given bank, especially when there are many different possible risk measures to consider. Prior to defining specific measures, one should be aware of the general characteristics of ideal risk measures. They should be: intuitive, stable, easy to compute, easy to understand, coherent, and interpretable in economic terms. In addition, the risk decomposition process must be simple and meaningful for a given risk measure.

Standard deviation, value at risk (VaR), expected shortfall (ES), as well as spectral (i.e., coherent) and distorted risk measures could be considered, each with their respective pros and cons. Obviously, no one measure would perfectly consider all of the necessary elements in measuring risk. In practice, VaR and ES are the most commonly used measures. The following section is a summary of challenges encountered when considering the appropriateness of each risk measure.

Standard Deviation

- Not stable because it depends on assumptions about the loss distribution.
- Not coherent because it violates the monotonicity condition.
- Simple, but not very meaningful in the risk decomposition process.

VaR (The Most Commonly Used Measure)

- Not stable because it depends on assumptions about the loss distribution.
- Not coherent because it violates the subadditivity condition (could cause problems in internal capital allocation and limit setting for sub-portfolios).

Expected Shortfall

- May or may not be stable, depending on the loss distribution.
- Not easy to interpret, and the link to the bank's desired target rating is not clear.

Spectral and Distorted Risk Measures

- Not intuitive nor easily understood (and rarely used in practice).
- May or may not be stable, depending on the loss distribution.

In defining or using such risk measures, banks often consider several of them and for different purposes. For example, absolute risk and capital allocation within the bank are most commonly measured using VaR, but increasingly, the latter is being measured using ES. The VaR measure of absolute risk tends to be easier to communicate to senior management than ES, but ES is a more stable measure than VaR for allocating total portfolio capital. The challenge for the bank is to determine if and when one or the other, or both, should be used.

Among the commonly used measures to calculate economic capital, regulators do not have a clear preference for one over another. If different risk measures are implemented by a bank for external versus internal purposes, then there must be a logical connection between the two risk measures. For regulators, merely comparing a bank's internal and

regulatory capital amounts is insufficient when determining the underlying risks in its portfolio. Therefore, such a task presents an analytical challenge to regulators.

Risk Aggregation

Risk aggregation involves identifying the individual risk types and making certain choices in aggregating those risk types. Classification by risk types (market, credit, operational, and business) may be approximate and prone to error. For example, the definitions of risk types may differ across banks or within a given bank, which complicates the aggregation process.

Even though one or more of the previously mentioned four risk types may be found at the same time within a given bank portfolio, the portfolio will often be represented by one risk type for the bank's classifications purposes. Such a simplistic distinction may result in inaccurate measurements of the risk types and this may bias the aggregation process.

Most banks begin by aggregating risk into silos by risk-type across the entire bank. Other banks prefer using business unit silos, while others combine both approaches. There is no one unanimously accepted method, as each approach has its specific advantages.

Before risk types can be aggregated into a single measure, they must be expressed in comparable units. There are three items to consider: risk metric, confidence level, and time horizon.

1. **Risk metric:** Relies on the metrics used in the quantification of different risk types. Must consider whether the metric satisfies the subadditivity condition.
2. **Confidence level:** Loss distributions for different types of risk are assumed to have different shapes, which implies differences in confidence intervals. The lack of consistency in choosing confidence levels creates additional complexity in the aggregation process.
3. **Time horizon:** Choosing the risk measurement time horizon is one of the most challenging tasks in risk measurement. For example, combining risk measures that have been determined using different time horizons creates problems irrespective of actual measurement methods used. Specifically, there will be inaccurate comparisons between risk types.

A common belief is that combining two portfolios will result in lower risk per investment unit in the combined portfolio versus the weighted average of the two separate portfolios. However, when we consider risk aggregations across different portfolios or business units, such a belief does not hold up with VaR because it does not necessarily satisfy the subadditivity condition. Also, there may be a false assumption that covariance always fully takes into account the dependencies between risks. Specifically, there could be times where the risk interactions are such that the resulting combinations represent higher, not lower, risk. These points highlight an additional challenge in the computation of risk.

There are five commonly used aggregation methodologies. The following is a brief description of them, as well as the challenges associated with using them.

1. Simple summation

- Adding together individual capital components.
 - Does not differentiate between risk types and therefore assumes equal weighting. Also, does not take into account the underlying interactions between risk types or for differences in the way the risk types may create diversification benefits. In addition, complications arising from using different confidence levels are ignored.
2. Constant diversification
- Same process as simple summation except that it subtracts a fixed diversification percentage from the overall amount.
 - Similar challenges as simple summation.
3. Variance-covariance matrix
- Summarizes the interdependencies across risk types and provides a flexible framework for recognizing diversification benefits.
 - Estimates of inter-risk correlations (a bank-specific characteristic) are difficult and costly to obtain, and the matrix does not adequately capture nonlinearities and skewed distributions.
4. Copulas
- Combines marginal probability distributions into a joint probability distribution through copula functions.
 - More demanding input requirements and parameterization is very difficult to validate. In addition, building a joint distribution is very difficult.
5. Full modeling/simulation
- Simulate the impact of common risk drivers on all risk types and construct the joint distribution of losses.
 - The most demanding method in terms of required inputs. Also, there are high information technology demands, the process is time consuming, and it may provide a false sense of security.

The variance-covariance approach is commonly used by banks. Frequently, however, bank-specific data is not available or is of poor quality. As a result, the items in the variance-covariance matrix are completed on the basis of expert judgment. On a related note, banks often use a “conservative” variance-covariance matrix where the correlations are reported to be approximate and biased upward. In order to reduce the need for expert judgment, banks may end up limiting the dimensionality of the matrix and aggregating risk categories so that there are only a few of them, not recognizing that such aggregations embed correlation assumptions. Clearly, a disadvantage of such a practice is that each category becomes less homogenous and therefore, more challenging to quantify.

One potential disadvantage of the more sophisticated methodologies is that they often lead to greater confidence in the accuracy of the output. It is important to consider robustness checks and estimates of specification and measurement error so as to prevent misleading results.



MODULE QUIZ 53.1

1. Which of the following risk measures is the least commonly used measure in the practice of risk management?
 - A. Value at risk.

- B. Standard deviation.
 - C. Expected shortfall.
 - D. Spectral risk measures.
2. Which of the following aggregation methodologies is characterized by great difficulty in validating parameterization and building a joint distribution?
- A. Copulas.
 - B. Constant diversification.
 - C. Variance-covariance matrix.
 - D. Full modeling/simulation.

MODULE 53.2: VALIDATION, DEPENDENCY, COUNTERPARTY CREDIT RISK, AND INTEREST RATE RISK

Validation of Models

Validation is the “proof” that a model works as intended. As an example, while it is a useful tool to test a model’s risk sensitivity, it is less useful for testing the accuracy of high quantiles in a loss distribution.

The validation of economic capital models differs from the valuation of an IRB (internal-ratings based) model because the output of economic capital models is a distribution rather than a single predicted forecast against which actual outcomes may be compared. Also, economic capital models are quite similar to VaR models despite the longer time horizons, higher confidence levels, and greater lack of data.

There are six *qualitative* validation processes to consider. The following is a brief description of them, as well as the challenges associated with using them (where applicable).

1. Use test

- If a bank uses its measurement systems for internal purposes, then regulators could place more reliance on the outputs for regulatory capital.
- The challenge is for regulators to obtain a detailed understanding of which model’s properties are being used and which are not.

2. Qualitative review

- Must examine documentation and development work, have discussions with the model’s developers, test and derive algorithms, and compare with other practices and known information.
- The challenge is to ensure that the model works in theory and takes into account the correct risk drivers. Also, confirmation of the accuracy of the mathematics behind the model is necessary.

3. Systems implementation

- For example, user acceptance testing and checking of code should be done prior to implementation to ensure implementation of the model is done properly.

4. Management oversight

- It is necessary to have involvement of senior management in examining the output data from the model and knowing how to use the data to make business decisions.
- The challenge is ensuring that senior management is aware of how the model is used and how the model outputs are interpreted.

5. Data quality checks

- Processes to ensure completeness, accuracy, and relevance of data used in the model. Examples include: qualitative review, identifying errors, and verification of transaction data.

6. Examination of assumptions—sensitivity testing

- Assumptions include: correlations, recovery rates, and shape of tail distributions. The process involves reviewing the assumptions and examining the impact on model outputs.

There are also six *quantitative* validation processes to consider. The following is a brief description of them, as well as the challenges associated with using them (where applicable).

1. Validation of inputs and parameters

- Validating input parameters for economic capital models requires validation of those parameters not included in the IRB approach, such as correlations.
- The challenge is that checking model inputs is not likely to be fully effective because every model is based on underlying assumptions. Therefore, the more complex the model, the more likely there will be model error. Simply examining input parameters will not prevent the problem.

2. Model replication

- Attempts to replicate the model results obtained by the bank.
- The challenge is that the process is rarely enough to validate models and in practice, there is little evidence of it being used by banks. Specifically, replication simply by re-running a set of algorithms to produce the same set of results is not considered enough model validation.

3. Benchmarking and hypothetical portfolio testing

- The process is commonly used and involves determining whether the model produces results comparable to a standard model or comparing models on a set of reference portfolios.
- The challenge is that the process can only compare one model against another and may provide little comfort that the model reflects “reality.” All that the process is able to do is provide broad comparisons confirming that input parameters or model outputs are broadly comparable.

4. Backtesting

- Considers how well the model forecasts the distribution of outcomes—comparison of outcomes to forecasts.
- The challenge is that the process can really only be used for models whose outputs can be characterized by a quantifiable metric with which to compare an outcome. Obviously, there will be risk measurement systems whose outputs

cannot be interpreted this way. Also, backtesting is not yet a major part of banks' validation practices for economic purposes.

5. Profit and loss attribution

- Involves regular analysis of profit and loss—comparison between causes of actual profit and loss versus the model's risk drivers.
- The challenge is that the process is not widely used except for market risk pricing models.

6. Stress testing

- Involves stressing the model and comparing model outputs to stress losses.

Overall, although these validation processes may be highly effective in areas such as risk sensitivity, they may not be effective in areas such as overall absolute accuracy.

Additionally, there is difficulty in validating the conceptual soundness of a capital model. The development of a model almost always requires assumptions to be made. However, some of the assumptions may not be testable, so it could be impossible to be absolutely certain of the conceptual soundness of a model. Even though the underlying points may appear reasonable and logical, that may not be the case in practice.

From a regulator's perspective, some industry validation practices are weak, especially for total capital adequacy of the bank and the overall calibration of models. Such a validation project is challenging because it usually requires evaluation of high quantiles of loss distributions over long periods of time. In addition, there are data scarcity problems plus technical difficulties, such as tail estimation. Therefore, it is important for senior management and model users to understand the limitations of models and the risks of using models that have not been fully validated.

Dependency Modeling in Credit Risk

Modeling the dependency structure between borrowers is crucial, yet challenging. Both linear and nonlinear dependency relationships between obligors need to be considered.

In general, dependencies can be modeled using: credit risk portfolio models, models using copulas, and models based on the asymptotic single-risk factor (ASRF) model. With the ASRF approach, banks may use their own estimates of correlations or may use multiple systematic risk factors to address concentrations. Such an approach would result in questioning the method used to calibrate the correlations and the ways in which the bank addressed the infinite granularity and single-factor structure of the ASRF model. ASRF can be used to compute the capital requirement for credit risk under the IRB framework.

There are many issues to consider regarding the challenges in coming up with reliable dependency assumptions used in credit risk portfolio models. Regulators may need to test the accuracy and strength of correlation estimates used by banks given their heavy reliance on model assumptions and the significant impact on economic capital calculations.

In the past, the validity of the following assumptions have been questioned: (1) the ASRF Gaussian copula approach, (2) the normal distribution for the variables driving default, (3) the stability of correlations over time, and (4) the joint assumptions of

correctly specified default probabilities and doubly-stochastic processes, which suggest that default correlation is sufficiently captured by common risk factors.

Doubts have been raised about the ability of some models using such assumptions in terms of their ability to explain the time-clustering of defaults that is seen in certain markets. Insufficiently integrating the correlation between probability of default (PD) and loss given default (LGD) in the models, coupled with insufficiently modeling LGD variability, may lead to underestimating the necessary economic capital. Furthermore, it will create challenges in identifying the different sources of correlations and the clustering of defaults and losses.

Rating changes are greatly impacted by the business cycle and are explained by different models during expansionary and recessionary periods. As a result, the sample period and approach used to calibrate the dependency structure could be important in assessing whether correlation estimates are overestimated or underestimated.

Furthermore, some models assume that unobservable asset returns may be approximated by changes in equity prices but fail to consider that the relationship between asset returns and equity prices are unobservable and may be nonlinear. Also, the use of equity prices to estimate credit default probability is problematic because such prices may include information that is irrelevant for credit risk purposes. As a result, using equity prices may result in some inaccuracy in the correlation estimates.

In contrast, when banks use a regulatory-type approach, the assumptions of such an approach create other challenges for both banks and regulators:

- Correlation estimates need to be estimated, but there may be limited historical data on which to base the correlation estimates. Also, the assumptions used to generate the correlations may not be consistent with the underlying assumptions of the Basel II credit risk model.
- A bank's use of the Basel II risk weight model requires concentration risk to be accounted for by other measures and/or management methods. It will also require regulators to evaluate such measures/methods.

A key challenge to overcome is the use of misspecified or incorrectly calibrated correlations and the use of a normal distribution (which does not replicate the details of the distribution of asset returns). This may lead to large errors in measuring portfolio credit risk and economic capital.

Evaluating Counterparty Credit Risk

Such a task is a significant challenge because it requires: obtaining data from multiple systems, measuring exposures from an enormous number of transactions (including many that exhibit optionality) spanning a wide range of time periods, monitoring collateral and netting arrangements, and categorizing exposures across many counterparties. As a result, banks need to have well-developed processes and trained staff to deal with these challenges.

Market-Risk-Related Challenges to Counterparty Exposure at Default (EAD) Estimation

- Counterparty credit exposure requires simulation of market risk factors and the revaluation of counterparty positions under simulated risk factor shocks, similar to

VaR models. Consider the following two challenges that occur when attempting to use VaR model technology to measure counterparty credit exposure.

- Market risk VaR models combine all positions in a portfolio into a single simulation. Therefore, gains from one position may fully offset the losses in another position in the same simulation run. However, counterparty credit risk exposure measurement does not allow netting across counterparties. As a result, it is necessary to compute amounts at the netting set level (on each set of transactions that form the basis of a legally enforceable netting agreement), which increases computational complexity.
- Market risk VaR calculations are usually performed for a single short-term holding period. However, counterparty credit exposure measurement must be performed for multiple holding periods into the future. Therefore, market risk factors need to be simulated over much longer time periods than in VaR calculations, and the revaluation of the potential exposure in the future must be done for the entire portfolio at certain points in the future.

Credit-Risk-Related Challenges to PD and LGD Estimation

- Some material transactions are performed with counterparties with which the bank does not have any other exposures. Therefore, the bank must calculate a probability of default (PD) and loss given default (LGD) for the counterparty and transaction.
- For hedge funds, the measurement challenge occurs when there is little information provided on underlying fund volatility, leverage, or types of investment strategies employed.
- Even for counterparties with which the bank has other credit exposures, the bank still needs to calculate a specific LGD for the transaction.

Interaction Between Market Risk and Credit Risk—Wrong-Way Risk

- Identifying and accounting for wrong-way risk (exposures that are negatively correlated with the counterparty's credit quality) is a significant challenge because it requires an understanding of the market risk factors to which the counterparty is exposed. That would be difficult to do in the case of a hedge fund, for example, which would be less transparent.
- It also requires a comparison of those factor sensitivities to the factor sensitivities of the bank's own exposures to the counterparty.
- The magnitude of wrong-way risk is difficult to quantify in an economic capital model since it requires a long time horizon at a high confidence level.

Operational-Risk-Related Challenges in Managing Counterparty Credit Risk

- The challenge is that managing such risk requires specialized computer systems and people. Complicated transactions, such as daily limit monitoring, marking-to-market, collateral management, and intraday liquidity and credit extensions, increase the risk of measurement errors.
- The quantification of operational risks is a significant challenge, especially when it pertains to new or rapidly growing businesses, new products or processes, intraday extensions of credit, and infrequently occurring but severe events.

Differences in Risk Profiles Between Margined and Non-Margined Counterparties

- The modeling difference between the two types of counterparties is primarily concerned with the future forecasting period. For margined counterparties, the forecasting period is short, and for non-margined counterparties, it is usually much longer.
- As a result of the difference in time periods, the aggregation of risk between these two types of counterparties is a challenge because the usual procedure is to use a single time period for all positions.

Aggregation Challenges

- In general, the challenges are increased significantly when moving from measuring credit risk of one counterparty to measuring credit risk of the firm in general for economic capital purposes.
- When counterparties have both derivatives and securities financing activities, the problem is especially challenging because the systems in place may not be able to handle such aggregation.
- Further aggregation challenges exist when high-level credit risk measures are required to be aggregated with high-level market risk and operational risk measures in order to calculate economic capital.
- Breaking down counterparty credit risk into detailed component parts (as is often done with market risk) is another challenge. The sheer computational complexities and enormous amounts of data required would generally be cost prohibitive to perform on a frequent basis. The challenge still remains for many banks due to outdated or ineffective computer systems.

Assessing Interest Rate Risk in the Banking Book

The computation challenge arises from the long holding period assumed for a bank's balance sheet and the need to model indeterminate cash flows on both the asset and liability side due to the embedded optionality of many banking book items.

Optionality in the Banking Book

- A major measurement challenge is found with nonlinear risk from long-term fixed-income obligations with embedded options for the borrower to prepay and from embedded options in non-maturity deposits.
- In considering the asset side of the balance sheet, prepayment risk options (i.e., mortgages, mortgage-backed securities, and consumer loans) are the main form of embedded options. The prepayment option results in uncertain cash flows and makes interest rate risk measurement a difficult task.
- In considering the liability side, there are two embedded options in non-maturity deposits: (1) the bank has an option to determine the interest rate paid to depositors and when to amend the rate, and (2) the depositor has the option to withdraw up to the entire balance with no penalty. The interaction between these two embedded options creates significant valuation and interest rate sensitivity measurement problems.

- Sufficiently modeling optionality exposures requires very complex stochastic-path evaluation techniques.

Banks' Pricing Behavior

- This factor contributes to the challenges in measuring the interest rate risk of banking book items. For example, it would require a model to analyze the persistence of the many different non-maturity banking products, as well as a model to determine bank interest rates that consider general market conditions, customer relationships, bank commercial power, and optimal commercial policies.
- Determining bank interest rates would require the pricing of credit risk. The price of credit risk applied to different banking products creates a challenge because it would require a pricing rule that links the credit spread to changes in macroeconomic conditions and interest rate changes. Also, it means that interest rate stress scenarios should consider the dependence between interest rate and credit risk factors.

The Choice of Stress Scenarios

- The drawbacks of using simple interest rate shocks pose interest rate measurement challenges because the shocks:
 - Are not based on probabilities and, therefore, are difficult to integrate into economic capital models based on VaR.
 - Are not necessarily sensitive to the current rate or economic environment.
 - Do not take into account changes in the slope or curvature of the yield curve.
 - Do not allow for an integrated analysis of interest rate and credit risks on banking book items.



MODULE QUIZ 53.2

1. Which of the following model validation processes is specifically characterized by the limitation that it provides little comfort that the model actually reflects reality?
 - A. Backtesting.
 - B. Benchmarking.
 - C. Stress testing.
 - D. Qualitative review.

MODULE 53.3: BIS RECOMMENDATIONS, CONSTRAINTS AND OPPORTUNITIES, AND BEST PRACTICES AND CONCERNS

BIS Recommendations for Supervisors

LO 53.b: Describe the recommendations by the Bank for International Settlements (BIS) that supervisors should consider making effective use of internal risk measures, such as economic capital, that are not designed for regulatory purposes.

There are 10 Bank for International Settlements (BIS) recommendations to consider:

1. **Use of economic capital models in assessing capital adequacy.** The bank should show how such models are used in the corporate decision-making process so as to assess the model's impact on which risks the bank chooses to accept. In addition, the board should have a basic understanding of the difference between gross (stand-alone) and net (diversified) enterprise-wide risk in assessing the bank's net risk tolerance.
2. **Senior management.** The economic capital processes absolutely require a significant commitment from senior management. They should understand its importance in the corporate planning process and should ensure that there is a strong infrastructure in place to support the processes.
3. **Transparency and integration into decision-making.** Economic capital results need to be easy to trace and understand in order to be useful. Careful attention must be given to obtaining reliable estimates on an absolute basis in addition to developing the flexibility to conduct firm-wide stress testing.
4. **Risk identification.** This is the crucial starting point in risk measurement. The risk measurement process must be very thorough to ensure that the proper risk drivers, positions, and exposures are taken into account in measuring economic capital. That will ensure that there is little variance between inherent (actual) and measured risk. For example, risks that are difficult to quantify should be considered through sensitivity analysis, stress testing, or scenario analysis.
5. **Risk measures.** No given risk measure is perfect, and a bank must understand the strengths and weaknesses of its chosen risk measures. No one risk measure for economic capital is universally preferred.
6. **Risk aggregation.** The reliability of the aggregation process is determined by the quality of the measurement risk components, plus the interrelationships between such risks. The aggregation process usually requires consistency in the risk measurement parameters. The aggregation methodologies used should mirror the bank's business composition and risk profile.
7. **Validation.** The validation process for economic capital models must be thorough and corroborating evidence from various tests must show that the model "works" as intended. In other words, within an agreed-upon confidence interval and time period, the capital level determined must be enough to absorb the (unexpected) losses.
8. **Dependency modeling in credit risk.** Banks must consider the appropriateness of the dependency structures used within their credit portfolio. Specifically, credit models need to be assessed for their limitations, and such limitations need to be dealt with via appropriate supplementary risk management approaches, such as sensitivity or scenario analysis.
9. **Counterparty credit risk.** There are tradeoffs to be considered in deciding between the available methods of measuring counterparty credit risk. Additional methods, such as stress testing need to be used to help cover all exposures. Measuring such risk is complicated and challenging. Specifically, the aggregation process needs to be vetted prior to a bank having a big picture perspective of counterparty credit risk.
10. **Interest rate risk in the banking book.** Specifically, financial instruments with embedded options need to be examined closely in order to control risk levels. Certainly, there are tradeoffs between using earnings-based versus economic value-based models to measuring interest rate risk. For example, the former has

aggregation problems because other risks are measured using economic value. Also, using economic value-based models could be inconsistent with business practices.

Economic Capital Constraints and Opportunities

LO 53.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**
-

Credit Portfolio Management

Constraints Imposed

- Credit quality of each borrower is determined in a portfolio context, not on a stand-alone basis.
- A loan's incremental risk contribution is used to determine the concentration of the loan portfolio.

Opportunities Offered

- The process allows one to determine appropriate hedging strategies to use in reducing portfolio concentration.
- Credit portfolio management becomes a means for protecting against risk deterioration.

Risk-Based Pricing

Constraints Imposed

- Pricing decisions are based on expected risk-adjusted return on capital (RAROC), so deals will be rejected if they are lower than a specific RAROC. The proposed interest rate is determined by the amount of economic capital allocated to the deal.
- Pricing decisions include: (1) cost of funding, (2) expected loss, (3) allocated economic capital, and (4) additional return required by shareholders. Therefore, a minimum interest rate is determined that will increase shareholder value.

Opportunities Offered

- Can be used to maximize the bank's profitability. For example, some pricing decisions may need to be overridden because certain customer relationships are more profitable (at a lower price/interest rate) or desirable from a reputational point of view. Of course, such overrides are not taken lightly and require upper management approval, as well as rigorous subsequent monitoring.

Customer Profitability Analysis

Constraints Imposed

- The analysis is complicated in that many risks need to be aggregated at the customer level.

- Customers need to be segmented in terms of ranges of (net) return per unit of risk; the underlying information is difficult to measure and allocate.

Opportunities Offered

- Assuming that the measurement obstacles have been overcome, the analysis can be easily used to determine unprofitable or only slightly profitable customers. Such customers could be dropped and economic capital allocated to the more profitable customers.
- Economic capital is used in maximizing the risk-return tradeoff (through relative risk-adjusted profitability analysis of customers).

Management Incentives

Constraints Imposed

- Studies show that compensation schemes are a minor consideration in terms of the actual uses of economic capital measures at the business unit level.

Opportunities Offered

- It is suggested that management incentives is the issue that motivates bank managers to participate in the technical aspects of the economic capital allocation process.

Best Practices and Concerns for Economic Capital Governance

LO 53.d: Describe best practices and assess key concerns for the governance of an economic capital framework.

The soundness of economic capital measures relies on strong controls and governance. Senior management is responsible for making sure these controls are in place and that governance covers the entire economic capital process. Adopting an economic capital framework will improve a bank's capital adequacy, strategic planning, risk appetite documentation, and risk-adjusted performance measurement. In order for an economic capital framework to be effective it should include:

- Strong controls for changing risk measurements.
- Comprehensive documentation for measuring risk and allocation approaches.
- Policies for making sure economic capital practices follow outlined procedures.
- View of how economic capital measures apply to daily business decisions.

Best practices for the governance of an economic capital framework cover:

1. *Senior management commitment.* The successful implementation of an economic capital framework depends on the involvement and experience of the senior management group. They are one of the main drivers for adopting this framework.
2. *The business unit involved and its level of expertise.* Governance structures differ among banks. Some banks opt for a centralized approach where economic capital responsibilities are assigned to one function (e.g., Treasury), while others opt for a

decentralized approach that shares responsibilities between functions (e.g., finance and risk functions). Each business unit within the bank will manage its risk in accordance with the amount of allocated capital. The responsibilities for allocating capital within business units will also vary among banks as will the flexibility to reallocate capital during the budgeting period.

3. *The timing of economic capital measurement and disclosures.* Most banks will compute economic capital on either a monthly or quarterly basis. Pillar 3 of the Basel II Accord encourages the disclosure of information about how capital is allocated to risks.
4. *Policies and procedures for owning, developing, validating, and monitoring economic capital models.* Formal policies and procedures encourage the consistent application of economic capital across the bank. The owner of the economic capital model will usually oversee the economic capital framework.

Key concerns related to governance and the application of economic capital measures involve:

1. *Senior management commitment.* The level of management buy-in contributes to the meaningfulness of the economic capital process. The senior management group must understand the importance of applying economic capital measures for strategic planning purposes.
2. *The role of stress testing.* Many banks currently apply stress tests; however, using more integrating stress tests will allow banks to better assess the impact of a stress scenario on certain economic capital measures.
3. *Measuring risk on either an absolute or relative basis.* Correctly interpreting economic capital as an estimate of risk depends on either measuring the absolute level of capital or measuring risk on a relative basis. Some issues within this measurement concern include assumptions regarding diversification and management involvement as well as how the economic model captures risks.
4. *Not using economic capital as the only measure that determines required capital.* Most banks align economic capital with external credit ratings. Shareholders desire profitability via lower capital levels while rating agencies encourage solvency via higher capital levels.
5. *Defining available capital resources.* Currently, there is no definition for available capital among banks. Most banks adjust Tier 1 capital to determine available capital resources.
6. *Transparency of economic capital measures.* Economic capital models are more useful for senior managers when they are transparent. Increased documentation will improve the validity of using the model when making business decisions.



MODULE QUIZ 53.3

1. Which of the following categories of BIS recommendations specifically refers to the need to consider using additional methods, such as stress testing, to help cover all exposures?
 - A. Risk aggregation.
 - B. Counterparty credit risk.
 - C. Dependency modeling in credit risk.
 - D. Interest rate risk in the banking book.
2. The use of which of the following items is meant more for protecting against risk deterioration?
 - A. Risk based pricing.

- B. Management incentives.
- C. Credit portfolio management.
- D. Customer profitability analysis.

KEY CONCEPTS

LO 53.a

A multitude of challenges exist within the economic capital framework that involve: (1) defining risk measures, (2) risk aggregation, (3) validation of models, (4) dependency modeling in credit risk, (5) evaluating counterparty credit risk, and (6) assessing interest rate risk in the banking book.

LO 53.b

There are 10 BIS recommendations that supervisors should consider to make effective use of risk measures.

LO 53.c

A number of specific constraints imposed and opportunities offered by economic capital exist within the areas of credit portfolio management, risk based pricing, customer profitability analysis, and management incentives.

LO 53.d

Best practices for the governance of an economic capital framework cover: (1) senior management commitment, (2) the business unit involved and its level of expertise, (3) the timing of economic capital measurement and disclosures, and (4) policies and procedures for owning, developing, validating, and monitoring economic capital models.

Key concerns related to governance and the application of economic capital measures involve: (1) senior management commitment, (2) the role of stress testing, (3) measuring risk on either an absolute or relative basis, (4) not using economic capital as the only measure that determines required capital, (5) defining available capital resources, and (6) transparency of economic capital measures.

ANSWER KEY FOR MODULE QUIZZES

Module Quiz 53.1

1. **D** Spectral and distorted risk measures are the least used of the four measures and are mainly of academic interest only. (LO 53.a)
2. **A** Copulas have two notable disadvantages: (1) parameterization is very difficult to validate, and (2) building a joint distribution is very difficult. (LO 53.a)

Module Quiz 53.2

1. **B** With benchmarking and hypothetical portfolio testing, the process has its limitations because it can only compare one model against another and may provide little comfort that the model actually reflects “reality.” All that the process is able to do is provide broad comparisons confirming that input parameters or model outputs are broadly comparable. (LO 53.a)

Module Quiz 53.3

1. **B** There are tradeoffs to be considered when deciding between the available methods of measuring counterparty credit risk. Additional methods, such as stress testing, need to be used to help cover all exposures. (LO 53.b)
2. **C** Credit portfolio management is used as a means to protect against risk deterioration. In contrast, risk based pricing is used to maximize the bank's profitability; customer profitability analysis is used to determine unprofitable or only slightly profitable customers; and management incentives are used to motivate managers to participate in the technical aspects of the economic capital allocation process. (LO 53.c)

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 assigned reading—Board of Governors of the Federal Reserve System.

READING 54

CAPITAL PLANNING AT LARGE BANK HOLDING COMPANIES: SUPERVISORY EXPECTATIONS AND RANGE OF CURRENT PRACTICE

Study Session 9

EXAM FOCUS

To protect the smooth functioning of bank holding companies (BHCs), the Federal Reserve's Capital Plan Rule requires BHCs to implement an ongoing internal capital plan for thoroughly assessing and enhancing their capital adequacy under stress scenarios on a firm-wide basis. For the exam, know the fundamental principles and key practices to develop and implement an effective internal control plan, including: risk identifications, model valuation and review, oversight and governance, contingency planning, stress testing and scenario designing, loss estimation and projections methodologies, and evaluating the impact of capital adequacy, including risk-weighted assets and balance sheet projections.

MODULE 54.1: THE FEDERAL RESERVE'S CAPITAL PLAN RULE

LO 54.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.

Bank holding companies (BHCs) must have adequate and sufficient capital for their survival and growth. Capital provides a cushion against unexpected losses and allows BHCs to continue to operate. The failure of BHCs (i.e., liabilities exceed assets, resulting in negative capital) would most likely be a burden on taxpayers and deposit insurance funds. An effective and sound capital management policy is critical for the health of BHCs, as well as the smooth functioning and stability of the entire financial system.

The Federal Reserve maintains its interest in survivability and smooth functioning BHCs through its **Capital Plan Rule** and the annual Comprehensive Capital Analysis and Review (CCAR). The CCAR is the Federal Reserve's supervisory program for evaluating capital plans.

The Capital Plan Rule mandates that BHCs develop and put in place a capital plan and a process to evaluate and monitor their capital adequacy. The capital plan covers all U.S. domiciled BHCs with total consolidated assets equal to \$50 billion or more.

The Capital Plan Rule lists the principles that the Federal Reserve uses to evaluate the adequacy and appropriateness of a BHC's internal capital planning processes and practices. The principles on which the Federal Reserve assesses BHCs for managing and allocating their capital resources is referred to as the **capital adequacy process (CAP)**. The seven principles of the CAP are as follows:

1. **Risk management foundation.** A BHC has an effective capital risk management plan to encompass all key risk exposures on a firm-wide basis in terms of identification, evaluation, measurement, and control.
2. **Resource estimation methods.** A BHC has a capital resource estimation plan to clearly define and estimate available capital resources over a stress scenario time horizon.
3. **Loss estimation methods.** A BHC has a process for estimating potential losses and aggregating them on a firm-wide basis over a given stress scenario time horizon.
4. **Impact on capital adequacy.** A BHC has a process to evaluate the combined impact on capital adequacy—given loss estimates and capital resources combined—in light of the stated goals with respect to capital level and composition.
5. **Capital planning policy.** A BHC has a sound capital policy to develop capital goals, determine appropriate capital levels and composition as well as capital distributions (actions) and contingency plans.
6. **Internal controls.** A BHC has a vigorous internal controls policy in place for independent review, model validation, documentation, and internal audit of the capital adequacy process.
7. **Effective oversight.** A BHC has a board and senior management responsible for an effective and thorough oversight of multiple dimensions of the internal capital risk plan, including methods, processes, assessments, validations, reviews, documentation, infrastructure, resources, goals, limitations, and approval of capital decisions.



MODULE QUIZ 54.1

1. The seven principles of an effective capital adequacy process for bank holding companies (BHCs) subject to the Capital Plan Rule include which of the following?
 - I. Oversight from peer BHCs
 - II. Annual reporting to the stock exchange (where their stock is listed)
 - A. I only.
 - B. II only.
 - C. Both I and II.
 - D. Neither I nor II.
2. The Federal Reserve's Capital Plan Rule requires BHCs to maintain an effective process for assessing their capital adequacy for:
 - A. BHCs, U.S. or non-U.S. domiciled.

- B. BHCs with more than five years of operational history.
- C. BHCs with a net annual income of more than \$5 billion.
- D. BHCs with total consolidated assets of \$50 billion or greater.

MODULE 54.2: CAPITAL ADEQUACY PROCESS

LO 54.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
-

For this LO, we detail the seven key practices that can result in a strong and effective capital adequacy process for a BHC.

Risk Identification

BHCs should have a process in place to identify all risk exposures stemming from numerous sources, including stress conditions, changing economic and financial environments, on-and-off balance sheet items, and their impact on capital adequacy. In addition, BHCs should critically scrutinize underlying assumptions regarding risk reduction through risk mitigation or risk transfer techniques. Senior management should regularly update and review the risk identification plan with special consideration for how their risk profiles might change under stress scenarios. Risk identification techniques should be able to detect the changes in the overall risk profile as well as the signs of capital inadequacy in the early stages.

BHCs should integrate the identified risk exposures into their internal capital planning processes. Scenario-based stress testing may not capture all potential risks faced by BHCs, some risks are difficult to quantify or they do not fall into the integrated firm-wide scenarios. However, such risks must be included and accounted for in the capital planning processes. These risks are categorized as “other risks,” and their examples include compliance, reputational, and strategic risks. There are a variety of methods which BHCs can employ, including internal capital targets to incorporate such risks.

Internal Controls

An internal audit team should carefully scrutinize the internal control data for accuracy before submitting to senior management and the board. BHCs should have efficiently running management information systems (MIS) for collecting and analyzing pertinent information set quickly and accurately.

In addition, BHCs should put in place a detailed and organized documentation system fully encompassing all dimensions of capital planning processes, including risk

identification, loss estimation techniques, capital adequacy, and capital decision processes.

There must be a thorough, independent, and regular review and validation of all models used for internal capital planning purposes, including assessment of conceptual soundness of models and verification of processes. A validation team should have a required technical skill set as well as complete independence from all business areas of the BHC and model developers. Such independence is crucial for the validation team to offer an unbiased, independent, and valuable verdict.

BHCs should maintain and update a list of all inputs, assumptions, and adjustments for the models used to generate final projections and estimates, such as income, loss expenses, and capital. These models should be validated for their effective use, not only under normal conditions, but also under stress conditions. BHCs should make full disclosure of their validation process and outcome, and should restrict the use of models which are not validated.

Governance

BHCs should have boards with sufficient expertise and involvement to fully understand and evaluate the information provided to them by senior management regarding their capital planning processes. The board should be furnished with comprehensive information with respect to risk exposures, loss estimates, determinants of revenues and losses, underlying models and assumptions, and weaknesses and strengths of capital planning processes. Also, the boards should be informed about the stress scenarios and any corrective measures undertaken as a result of stress testing outcomes.

Under the Capital Plan Rule, the management of BHCs is required to furnish key information to the board for its approval of internal capital adequacy plans. Such information should include underlying assumptions and results of stress testing and the outcome of internal audits, as well as model review and validation checks.

Senior management should evaluate the internal capital plan on an ongoing basis, focusing on key weaknesses, strengths, assumptions, scenarios, estimates, and models. In addition, senior management should make appropriate adjustments and remediation to the capital plan if the review process reveals shortcomings in the plan.

BHCs should maintain detailed minutes of board meetings, describing the issues raised and discussed, as well as the information used and the recommendations made in these meetings.

Capital Policy

A capital policy should clearly define the principles and guidelines for capital goals, issuance, usage, and distributions. The policy should also fully spell out the details of the BHC's capital planning processes, including the decision rules of capital usage and distribution, financing, and other policies. The capital policy should focus on the unique needs and financial situation of BHCs while taking into consideration the supervisory expectations. Policies regarding common stock dividends and repurchase agreements should include the following:

- Key metrics influencing the size, timing, and form of capital distributions.
- Materials used in making capital distribution decisions.
- Specific scenarios that would cause a distribution to be reduced or suspended.
- Situations that would cause the BHC to consider replacing common equity with other forms of capital.
- Key roles and responsibilities of individuals or groups for producing reference materials, making distribution recommendations and decisions, and reviewing analysis.

Capital goals developed by BHCs should be compatible with their risk tolerance, risk profile, regulatory requirements, and expectations of various stakeholders (e.g., shareholders, creditors, supervisors, and rating agencies). BHCs should establish specific goals for both the level and composition of capital under normal as well as stress conditions. Capital targets, which need to be set above the capital goals for capital adequacy under stress conditions, should take into consideration future economic outlooks, stress scenarios, and market conditions.

While setting capital distribution levels, BHCs must take into consideration numerous factors, including future growth plans (including acquisitions) and associated risk, current and future general economic conditions, in particular the impact of macroeconomic and global events during stress conditions, on their capital adequacy. Capital distribution decisions must be connected to capital goals or capital adequacy requirements.

BHCs should develop strong contingency planning offering numerous options to deal with contingency situations as well as their effectiveness under stress conditions. Contingency plans should be based on realistic assumptions and contain futuristic outlooks, rather than overly relying on history. Contingency actions should be feasible and realistic in the sense that they should be easy to implement when or if the contingency warrants. Capital triggers flagging the early warning of capital deterioration should be based on the projected results, regulatory requirements, and the expectations of various stakeholders, including creditors, shareholders, regulators, investors, and counterparties.

Stress Testing and Stress Scenario Design

Scenario design and stress testing should focus on unique situations of BHCs, their asset and liability mix, portfolio composition, business lines, geographical territory, and revenue and loss factors, while taking into consideration the impact of macroeconomic and firm-specific vulnerabilities and risks. That is, the stress test designing should go above and beyond the general guidelines established by the supervisory authority. Also, a BHC's scenario designing and testing should not employ optimistic assumptions benefiting the BHC.

BHCs should employ both an internal model and expert judgment, an outside expert's opinion. If only a third-party model is used, it must be tailored to the unique risk profile and business model of a BHC. The designed scenarios should assume a strong strain on the revenue and income of BHCs.

Stress testing models should be based on multiple variables encompassing all the risk exposures faced by BHCs on a firm-wide basis. For example, BHCs concentrated in a region, business, or industry should include relevant region, business, or industry-related variables. In addition, the scenarios should clearly spell out how they address specific risks faced by BHCs. The description should also provide explanations of how a scenario stresses specific BHC weaknesses and how variables are related to each other.

Estimating Losses, Revenues, and Expenses

Quantitative and Qualitative Basis

BHCs should prefer using internal data to estimate losses, revenues, and expenses. However, in certain situations, it may be more appropriate to use external data. In these instances, it should be ensured that the external data reflects the underlying risk profile of their business lines, and necessary adjustments should be made to data input or output to make the analysis reflect a true picture of the BHC's unique characteristics.

A range of quantitative methods are available to BHCs for estimating losses, revenues, and expenses. Regardless of which method they use, the final outcome should be identification of key risk factors and impact of changing macro and financial conditions under normal and stress conditions on a firm-wide basis.

In addition, BHCs should segment their line of businesses and portfolios utilizing common risk characteristics showing marked differences in past performances. For example, a borrower's risk characteristics can be segmented by criteria such as credit score ranges. However, each risk segment should have sufficient data observations on losses, revenues, and expenses, (and underlying factors impacting losses, revenues, and expenses) in order to generate meaningful model estimates.

Past relationships between losses, revenues, expenses, and underlying driving factors, and their interrelationships may not hold in the future, thus, necessitating employment of sensitivity analysis (to answer "what if" questions) when using models based on historical underlying interactions.

BHCs sometimes use qualitative methodologies, like expert judgment or management overlay, as a substitute or a complement to quantitative methods. Qualitative techniques should be based on sound assumptions, and an external reviewer should find these approaches logical, reasonable, and clearly spelled out. A sensitivity analysis should be used for a qualitative approach as well. From a supervisory standpoint, BHCs are expected to use conservative assumptions, not favorable to BHCs, for estimating losses, revenues, and expenses under normal and stress conditions.

Loss Estimation Methods

BHCs should employ loss estimation methods, which offer theoretical soundness and empirical validity. In addition to using general macroeconomic explanatory variables, the loss estimation models should use specific variables exhibiting a direct link to particular exposures and portfolios.

BHCs should use uniform, reputable methods to aggregate losses across various lines of business and portfolios for firm-wide scenario analysis. They should also use automated processes, without manual intervention or managerial adjustments showing

clear linkage from data sources to loss estimation and aggregation. For estimating retail loan losses, BHCs often use internal data, but for wholesale loss estimation, internal data is supplemented with external data. In the case using external data, BHCs should demonstrate that the data reflects their risk exposures, encompassing geographic, industry, and other key dimensions. Risk segmentation should be supported by the data capturing the unique characteristics of each risk pool.

BHCs can use either an economic loss approach (i.e., expected losses) or an accounting-based loss approach (i.e., charge-off and recovery) to estimate credit losses. For the expected loss approach, BHCs should categorize losses into probability of default (PD), loss given default (LGD), or exposure at default (EAD) and then identify the determinants of each component. Long run averages for PDs, LGDs, and EADs should not be used, as these averages reflect economic downturn and upturn periods not necessarily suitable for scenario testing under stress conditions. LGD should be linked to underlying risk factors, such as a fall in the value of collateralized assets under stress conditions, and it should be estimated at some level of segmentation, such as lending product or type of collateral. EADs should be modeled to exhibit variation depending on changes in macroeconomic conditions.

If BHCs are using rating systems as a key input to estimate expected losses under stress (e.g., on their wholesale portfolios), they should recognize the limitations in rating systems and their data and make necessary adjustments.

BHCs should utilize a robust time series with sufficient granularity while employing role-rate models to estimate the rate at which delinquent and non-delinquent accounts in the current quarter are expected to roll over into default or delinquent status in the next quarter.

If using charge-off models (i.e., accounting models), BHCs should include variables which represent the risk characteristics of an underlying portfolio while estimating the statistical relationship between charge-off rates and macroeconomic variables at the portfolio level.



MODULE QUIZ 54.2

1. How many of the following statements are most likely correct? BHCs should have risk identification processes that evaluate:
 - I. On- and off-balance sheet positions.
 - II. Risk transfer and/or risk mitigation techniques.
 - III. Changes in institutions' risk profile due to portfolio quality.
 - IV. Reputational risk.
 - A. One statement.
 - B. Two statements.
 - C. Three statements.
 - D. Four statements.
2. Which of the following statements is most likely correct?
 - A. The internal controls policy of BHCs requires that senior management should furnish the board of directors with sufficient information to comprehend the BHC risk exposures.
 - B. A governance policy offers fundamental guidelines and principles to BHCs for the capital issuance, use, distribution, and planning purposes.

- C. Suspension or reduction in dividends or repurchase programs do not fall under the capital policy of BHCs.
 - D. Designing and testing a scenario-related default of a major counterparty is an example of BHC stress testing and a stress scenario design policy.
3. Which of the following statements is most likely correct?
- I. Under the expected losses methodologies, loss estimation involves three elements: probability of default, loss given default, and exposure at default.
 - II. Net interest income projections should incorporate changing conditions for balance sheet positions, including embedded options, prepayment rates, loan performance, and repricing rates.
- A. I only.
 - B. II only.
 - C. Both I and II.
 - D. Neither I nor II.

MODULE 54.3: ASSESSING THE IMPACT OF CAPITAL ADEQUACY

Operational Risk

In order to determine operational risk, many BHCs estimate correlation between operational risk and macroeconomic factors. If they do not discover a statistically significant relationship between the variables, they employ other methods, including scenario analysis utilizing historical data and management input. BHCs should employ a combination of techniques to develop strong loss estimates under stress conditions, including past loss records, future expected events, macro conditions, and firm-specific risks.

BHCs using regression models to estimate loss frequency and loss severity under stress scenarios should provide statistical support for the period chosen for estimation purposes instead of arbitrary and judgmental selection.

A modified loss distribution approach (LDA) is also used by BHCs to estimate value at risk (VaR) to estimate operational risk losses at a chosen confidence interval (e.g., 90% or 95%). To generate a strong and effective process, BHCs should offer a sound justification for their choice and perform a sensitivity analysis around the chosen interval.

Some BHCs use scenario analyses in case they encounter model or data limitations in order to incorporate a wide range of risks (which is not possible otherwise due to data or model limitations). In such events, BHCs should provide a rationale for the chosen scenario in their loss estimation process.

Market Risk and Counterparty Credit Risk

BHCs, which are involved in trading, are subject to counterparty credit risk from changes in the value of risk exposure and creditworthiness of the counterparty due to changing macroeconomic conditions.

In order to estimate the potential loss resulting from market credit interaction, BHCs use probabilistic approaches (which produce a probability distribution of expected

portfolio losses) and deterministic approaches (which yield point estimates of an expected portfolio loss).

BHCs using probabilistic approaches should clearly offer evidence that such methods can yield more severe risk scenarios compared to historical scenarios. BHCs should also explain how they utilize tail loss scenarios to detect and address firm-specific risks.

BHCs using deterministic approaches should demonstrate that they have employed a wide range of scenarios, adequately covering their key risk exposures, including mark-to-market positions in the event of firm-specific or market-wide stress conditions. In addition, BHCs should clearly spell out the underlying assumptions employed in stress testing scenarios for risk measurement purposes and corrective measures to fix the identified deficiencies.

Market shock scenarios do not directly incorporate the default of the counterparty. Some BHCs explicitly incorporate the scenario of default of key counterparties (including key customers) while using some sort of probabilistic approach involving some estimates of the PD, LGD, and EAD of counterparties. This method allows BHCs to focus exclusively on the defaults of counterparties to which BHCs have large risk exposure.

BHCs also use assumptions about risk mitigation in the future. Such assumptions, if used, should be conservative in nature. In stress scenarios, the ability of BHCs to take desired actions may be limited.

PPNR Projection Methodologies

PPNR is pre-provision net revenue (i.e., net revenue before adjusting for loss provisions). While estimating revenues and expenses over a planning horizon under stressed conditions (the Capital Plan Rule requires forecasts over the next nine quarters), BHCs should not only take into consideration their current situation, but also the possible future paths of business activities and operational environments related to their on- and off-balance sheet risk exposures, underlying assumptions, and assets and liabilities.

BHCs should also take into consideration the impact of regulatory changes on their performance and ability to achieve their stated targets and goals. Projections should be based on coherent and clearly defined relationships among numerous, relevant variables, such as revenues, expenses, and balance sheet items within a given scenario. For example, assumptions related to origination should be the same for projections related to loans, fees, costs, and losses.

Underlying assumptions for revenues, expenses, and loss estimates should be theoretically and empirically sound, and the central planning group as well as the corporate planning group should be engaged in aggregating projections on an enterprise-wide basis. In the case of limited data, BHCs should employ external data in conjunction with internal data.

Net interest income projections are not isolated projections; rather, they are entrenched with other items of a capital adequacy plan. Balance sheet assumptions should be consistent while projecting net interest income. For example, balance sheet

assumptions for projecting net interest income should be the same when estimating loss. Methods employed for projecting net interest income should incorporate ongoing changes in current and projected balance sheet positions.

BHC projections under various scenarios, based on product characteristics (e.g., a change in deposit mix due to increased demand for time deposits), underlying assumptions, and rationale by product should be carefully explained.

BHCs linking loss projections to net interest income projections should clearly establish this link while using modeling approaches, which incorporate the behavioral characteristics of the loan portfolio.

Net interest income projections should be based on methodologies that incorporate discount or premium amortization adjustments for assets not held at par value that would materialize under different scenarios.

New business pricing projections and underlying assumptions, such as constant additions to a designated index value, should be compatible with past data, scenario conditions, and BHCs' balance sheet projections.

BHCs should project noninterest income in light of stated scenarios and business strategies. Projection methods should fully encompass underlying major risk exposures and characteristics of a specific business line. For example, an asset management group should project noninterest income using various methods, including brokerage as well as money management revenues.

Additionally, BHCs with trading portfolios should establish a clear link between trading revenue projections to trading assets and liabilities and the compatibility of all the elements of stress scenario conditions.

BHCs with off-balance sheet business items should demonstrate the linkage between revenue projections and changes in on- and off-balance sheet items.

BHCs should not assume perfect correlation between revenues (generated from trading or private equity activity) and broad indices. BHCs should estimate the sensitivity coefficients for changes in revenue as a result of changes in broad index movements.

Furthermore, BHCs holding mortgage servicing rights assets (MSRAs) should carefully design assumptions regarding default, prepayment, and delinquency rates, ensuring that these assumptions are robust and scenario specific. In addition, BHCs that hedge MSRA risk exposure should generate scenario specific assumptions.

For BHCs, projecting volume increases in mortgage loans while ignoring market saturation or other key factors would be an ineffective and weak process, whereas consideration of individual business models, client profiles, and capacity constraint (while projecting mortgage loan volume) would be an effective and strong capital adequacy process.

Macroeconomic relationships should be based on sound theoretical construct and supported by empirical evidence. For example, BHCs may experience a steep decline in credit card fee revenues in a strong recessionary period because of a decline in consumer spending. An example of a weaker practice of a capital planning process is if a

BHC does not show a sufficient decline in revenue in stressed conditions despite obvious macro relationships.

In addition, BHCs should utilize a wide set of explanatory variables to develop statistical relationships. BHCs should take into consideration the impact of macroeconomic conditions, such as an economic downturn, on their noninterest expense projections. Non-interest expense projections, like all other projections, should be consistent with revenue and balance sheet estimates and should generate the same underlying strategic assumptions. If projections assume that a decline in revenue (e.g., due to an increase in credit collection costs in an economic downturn) can be offset by some mitigating strategies, BHCs should then clearly demonstrate the feasibility of such actions. Mitigation actions should not be supported by past relationships and actions only because future financial, macro, and global environments may not be as favorable to execute such strategies, as was the case in the past.

Estimation methods to project noninterest expense should focus on uncovering determinants (factors) of individual expense items and how sensitive those factors are to changing macro conditions and business strategies.

Generating Projections

BHCs should have a well-defined and well-documented process of generating projections with respect to size and composition of on- and off-balance sheet items and risk-weighted assets (RWA) over a stress horizon period.

Projecting balance sheet items, such as changes in assets and funding, directly without consideration of underlying drivers (of such changes), would be a weak practice. BHCs should identify the impact of changes in key factors on changes in asset and liabilities. Projections should take into consideration these vital relationships.

BHCs should incorporate relationships between revenues, expenses, and balance sheet items into their scenario analyses. Projections about losses, revenues, expenses, and on- and off-balance sheet items should not be based on favorable underlying assumptions. These assumptions may not stand the trial of uncertain market conditions under stress conditions.

Projections for RWA should be consistent with the projections for risk exposures of on- and off-balance sheet items. All underlying assumptions used for balance sheet and RWA projections should be clearly documented and critically reviewed and validated.

BHCs with a strong process of implementation should form a centralized group responsible for aggregating loss, revenue, expense, on- and off-balance sheets, and RWA projections for enterprise-wide scenario analysis. In addition, BHCs should establish a strong governance structure to critically scrutinize assumptions, methods, and estimates generated in an enterprise-wide scenario analysis and offer needed adjustments. BHCs should carefully evaluate the validity and relevance of underlying assumptions across business lines, portfolios, loss, expense, and revenue estimates if an enterprise-wide scenario analysis produces post-stress results that are more favorable than the baseline conditions. The outcomes of such analyses should also be reconciled for regulatory as well as management reporting purposes.



MODULE QUIZ 54.3

1. An analyst is discussing net interest income projections with a colleague. Which of the following items should not be incorporated into net interest income projections?
 - A. Prepayment rates.
 - B. Balance sheet positions.
 - C. Forward earnings guidance.
 - D. Embedded options.

KEY CONCEPTS

LO 54.a

The Federal Reserve's Capital Plan Rule mandates all top-tier, U.S. domiciled bank holding companies with consolidated assets equal to or greater than \$50 billion to develop and maintain an effective and robust internal capital plan for evaluating and assessing their capital adequacy.

There are seven principles on which the Federal Reserve assesses the effectiveness of a BHC's internal capital planning, also known as the capital adequacy process (CAP). These seven principles are related to risk management foundation, resource and loss estimation methods, capital adequacy, capital planning and internal controls policies, and governance oversight.

LO 54.b

BHCs should develop a process to effectively identify all of their risk exposures on a firm-wide basis. BHCs should establish a mechanism for a comprehensive, independent, and regular review and validation of all the models used for capital adequacy planning purposes. BHCs should have boards actively involved in evaluating and approving their internal capital adequacy plans. BHCs should develop a capital policy that clearly defines the principles and guidelines for capital goals, issuance, usage, and distributions.

Stress testing and stress scenario design should be based on a variety of factors encompassing all the risk exposures faced by BHCs on a firm-wide basis. With the option of utilizing various quantitative and qualitative methods, BHCs should carefully identify key risk exposures on a firm-wide scenario basis. BHCs should use loss estimation methodologies, which are based on sound theoretical and empirical foundations. BHCs should use a combination of inputs in order to develop loss estimates arising from operational risk. In order to estimate the counterparty credit risk, BHCs mostly use probabilistic or deterministic approaches. BHCs using a probabilistic approach should offer evidence of generating probable scenarios stronger than past observed events. BHCs using a deterministic approach should generate a wide range of stress scenarios.

While estimating pro-provision net revenue (PPNR) projection methodologies, BHCs should pay particular attention to interrelationships among numerous relevant variables such as revenues, expenses, and on- and off-balance sheet items within a given scenario. Methodologies used for projecting net interest income should incorporate ongoing, current, and projected balance sheet positions. BHCs should project noninterest income in light of stated risk scenarios and business strategies.

BHCs should have a well-defined process in place to develop projections of revenues, expenses, losses, on- and off-balance sheet items, and risk-weighted assets in an enterprise-wide scenario analysis. Projections should be based on sound underlying assumptions, interactions, and factors (main drivers of change), and the estimates should be scrutinized, documented, and reported.

ANSWER KEY FOR MODULE QUIZZES

Module Quiz 54.1

1. **D** Oversight from peer BHCs and annual reporting to the stock exchange are not included in the seven principles of an effective capital adequacy process. (LO 54.a)
2. **D** BHCs with total consolidated assets of \$50 billion or greater. The other answers are not part of the requirements under the Capital Plan Rule. (LO 54.a)

Module Quiz 54.2

1. **D** All of the statements are correct. BHCs should have risk identification processes effectively identifying all risk exposures for assessing capital needs. Reputational risk, like strategic risk and compliance risk, falls under the category of “other risks” and are more difficult to quantify. Nevertheless, there are a wide range of methods BHCs employ to evaluate other risks. (LO 54.b)
2. **D** The first statement is the requirement of the governance policy and not the internal control policy. The second statement falls under capital policy and not the governance policy. Regarding the third statement, capital contingency plans (e.g., suspension or reduction in dividends or repurchase programs) are a key part of capital policies of BHCs detailing the actions intended to be taken under deficiencies in capital position. The fourth statement is correct. Many different scenarios, including counterparty default, fall under the BHCs’ stress testing and scenario design policy. (LO 54.b)
3. **C** Both statements are correct. Loss estimation involves probability of default, loss given default, and exposure at default. Net interest income projections should incorporate changing conditions for balance sheet positions, including embedded options, prepayment rates, loan performance, and repricing rates. (LO 54.b)

Module Quiz 54.3

1. **C** Net interest income projections should incorporate changing conditions for balance sheet positions, including embedded options, prepayment rates, loan performance, and repricing rates. (LO 54.b)

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 assigned reading—Carey.

READING 55

CAPITAL REGULATION BEFORE THE GLOBAL FINANCIAL CRISIS

Study Session 9

EXAM FOCUS

This reading provides an overview of the international capital standards put in place by the Basel Committee on Banking Supervision. Basel I (1988) contained the first steps toward risk-weighting bank activities, on- and off-balance sheet, to relate required capital to risk. Basel I was the first to set a capital to risk-weighted assets requirement, but it only considered credit risk, not market or operational risk. Basel II took a more sophisticated approach to measuring bank credit risk, market risk, and operational risk. For the exam, understand the contribution Basel II makes to risk measurement, and know the differences between the methods used to calculate various risks. Also, know the difference between Basel II and Solvency II, a similar international standard for insurance companies and the likely repercussions a firm will face if it breaches the standards. In addition, be able to calculate a bank's required capital under the various regimes. One of the recurring themes in this reading is the difference between a standardized approach for measuring risk, used by less sophisticated banks (and insurance companies), and an internal approach that is firm specific and more complex but often lowers required capital because it allows banks to use their own model inputs and considers the correlations between assets.

MODULE 55.1: BASEL I REGULATIONS AND REVISIONS

LO 55.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.

Early banks had to signal financial soundness through large amounts of capital and impressive bank buildings. The first “regulations” resulted from private firms banding together to protect banks from bank runs. For example, the Bank of England was originally a private sector entity that helped other banks. Clearinghouses were also private and members shared financial statements, monitoring each other's solvency in

private. Private monitoring and protection of banks had limitations. Regulation, as we know it currently, arose from these limitations:

- A true panic would lead to runs and losses that could not be managed by private firms. The power to print money was required, thus central banks, which were backed by the government, gradually replaced private entities as “lenders of last resort.”
- Governments realized that financial crises had far reaching effects on the overall economy and were followed by recessions and depressions. As such, governments became more determined to ensure the solvency and liquidity of the financial system.
- The customers of failed banks were unhappy and complained about the difficulty of assessing the safety and soundness of banks, even when fraud was not to blame for bank failures.
- International trade flourished in the 1960s and 1970s. This made international coordination of regulations more important.
 - Large financial institutions became internationally linked, leading to global systemic risk (i.e., the economies of multiple countries could be affected by a failure).
 - As banks became increasingly global, banks operating in countries with more lax standards were perceived to have a competitive advantage over banks operating in countries with strict enforcement of capital regulations.
 - Globalization led to technical complexities. Settlements became important and differences in delivery times and delivery currencies resulted in transactions failing to clear. For example, Herstatt Bank failed in 1974 as a result of clearing issues due to time zone differences (called settlement risk).

As a result of these and other limitations, the Basel Committee on Banking Supervision (BCBS) was created in 1974. The accord is made up roughly of the Group of Ten (G10) nations.

Prior to 1988, bank capital regulations were inconsistent across countries and ignored the riskiness of individual banks. Requirements were stated as minimum ratios of capital to total assets or as maximum ratios of total assets to capital. Some countries and/or regulatory authorities were more diligent in their enforcement of capital regulations than others. Also, bank transactions were becoming more complex. Off-balance sheet transactions in over-the-counter (OTC) derivatives like interest rate swaps, currency swaps, and options were growing. These off-balance sheet deals did not affect total assets, and thus did not affect the amount of capital a bank was required to keep. The compositions of bank balance sheets also differ significantly in terms of risk. All of these factors provided fuel to the growing belief that total assets did not reflect a bank's total risk.

In 1988, the Basel Committee put forth its first guidance to set international risk-based capital adequacy standards, called the 1988 BIS Accord, now commonly known as **Basel I**. Basel I has no legal authority over the world's financial institutions. However, countries have adopted the standards through domestic laws and regulations.

Capital and Risk-Weighted Assets

LO 55.b: Explain the calculation of risk-weighted assets and the capital requirement per the original Basel I guidelines.

Although it seems simple by today's standards, the real innovation of Basel I was risk-weighting bank assets, rather than focusing on capital relative to total assets. Basel I put forth three capital requirements:

1. The bank's total assets-to-capital ratio had to be less than 20 (i.e., capital to total assets had to be greater than $1/20$ or 5%). This capital requirement was similar to the requirements in many countries prior to 1988.
2. Tier 1 capital to **risk-weighted assets (RWA)** must exceed 4%. On- and off-balance sheet items are used to calculate a RWA. RWA is intended to measure a bank's total credit exposure.
3. The ratio of total capital (Tier 1 + Tier 2) to RWA must exceed 8%. The ratios are sometimes referred to as the **Cooke ratios**, after Peter Cooke from the Bank of England. Basel I stipulated that Tier 2 capital must be no more than half of total capital. Excess Tier 1 capital (i.e., greater than 4% of RWA) may be used to satisfy the total capital to RWA ratio.

Basel I defined the two components of capital as follows:

Tier 1 capital (or core capital) consists of:

- Equity (subtract goodwill from equity).
- Noncumulative perpetual preferred stock.

Tier 2 capital (or supplementary capital) consists of:

- Cumulative perpetual preferred stock.
- Certain types of 99-year debentures.
- Subordinated debt with an original maturity greater than five years (where the subordination is to depositors).

Equity capital (i.e., Tier 1) absorbs losses. Supplementary capital (i.e., Tier 2) is subordinate to depositors and thus protects depositors in the event of a bank failure. At least 50% of capital must be Tier 1. Half of the Tier 1 requirement has to be met with common equity. Under Basel I, some countries required banks to have more capital than required by the Basel I Accord.



PROFESSOR'S NOTE

Though not made explicit by the BCBS, there were two underlying assumptions. First, Tier 1 capital was meant to preserve solvency and Tier 2 capital was meant to reduce the impact of bank failures on depositors. Second, loan loss reserves were not counted as loss absorbing nor solvency preserving.

The process for calculating risk-weighted assets includes assigning a risk weight that reflects the bank's credit risk exposure to each of the on- and off-balance sheet items. A

sample of some of the risk weights assigned to various asset categories is shown in Figure 55.1.

Figure 55.1: Risk Weights for On-Balance Sheet Items

Risk Weight (%)	Asset Category
0%	Cash, gold, claims on Organization of Economic Co-operation and Development (OECD) countries such as U.S. Treasury bonds and insured residential mortgages
20%	Claims on OECD banks and government agencies like U.S. agency securities such as Fannie Mae and Freddie Mac or municipal bonds
50%	Uninsured residential mortgages
100%	Loans to corporations, consumer loans, corporate bonds, claims on non-OECD banks

Risk-weighted assets are calculated by multiplying the on-balance sheet amount of the item by the percentage risk weight and summing the products.

EXAMPLE: Risk-weighted assets

The assets of Blue Star Bank consist of \$20 million in U.S. Treasury bills, \$20 million in insured mortgages, \$50 million in uninsured mortgages, and \$150 million in corporate loans. Using the risk weights from Figure 55.1, **calculate** the bank's risk-weighted assets.

Answer:

$$(0.0 \times \$20) + (0.0 \times \$20) + (0.5 \times \$50) + (1.0 \times \$150) = \$175 \text{ million}$$

Off-balance sheet items are expressed as **credit equivalent amounts (CEA)**. The CEA is a measure, prescribed by the regulator, to quantify credit risk for off-balance sheet instruments such as derivatives. This means the bank "converts" off-balance sheet items into on-balance sheet equivalents for the purpose of calculating risk-based capital. The weight is then multiplied by the principal amount (i.e., the credit equivalent amount) of the item to arrive at a risk-weighted value. A **conversion factor** is applied to the principal amount of the instrument for nonderivatives. Off-balance sheet items that are similar, from a credit perspective, to loans (e.g., banker's acceptances) have a conversion factor of 100%. Other off-balance sheet items, such as note issuance facilities, have lower conversion factors.

Figure 55.2: Credit Conversion Factors

Conversion Factor	Off-balance Sheet Category
100%	Guarantees on loans and bonds, bankers acceptances, and equivalents
50%	Standby letters of credit and warranties related to transactions
20%	Loan commitments with original maturities equal to or greater than one year
0%	Loan commitments with original maturity less than one year

For example, a \$200 million standby letter of credit to a government agency would first be converted to a \$100 million credit equivalent ($\$200 \text{ million} \times 0.50$) then would be assigned a 20% risk weight. It would thus contribute \$20 million to RWA.

For interest rate swaps and other OTC derivatives, regulators may choose between the **current exposure method** and the **original exposure method**.

For the current exposure method, the **credit equivalent amount** is calculated as:

$$\max(V, 0) + D \times L$$

where:

V = current value of the derivative to the bank

D = add-on factor (to account for changes in the contract's future market value)

L = principal amount

The first term in the equation [$\max(V, 0)$] reflects the bank's current exposure. If the counterparty defaults and V, the current value of the derivative, is positive, the bank will lose V. If the counterparty defaults and V is negative, the exposure is 0 (i.e., no gain or loss to the bank). The **add-on amount** ($D \times L$) allows for the possibility that the bank's exposure may increase in the future. Add-on factors are higher for higher risk derivatives (e.g., longer maturities, riskier underlying assets). A sample of add-on factors is shown in Figure 55.3.

Figure 55.3: Current Exposure Method: Add-On Factors as a Percentage of Principal for Derivatives

Remaining Maturity in Years	Interest Rate Swaps	Exchange Rate Swaps and Gold	Equity	Other Commodities
< 1 year	0.0	1.0	6.0	10.0
1 to 5 years	0.5	5.0	8.0	12.0
> 5 years	1.5	7.5	10.0	15.0



PROFESSOR'S NOTE

Basel I was the first attempt at handling derivatives exposure and, as such, was somewhat simple. Interest rate and exchange rate derivatives were included, equity and commodity derivatives were not. Later amendments included equity and commodity contracts.

EXAMPLE: Credit equivalent amounts for off-balance sheet items

Blue Star Bank has entered a \$175 million interest rate swap with a remaining maturity of three years. The current value of the swap is \$2.5 million. Using the add-on factors in Figure 55.3, **calculate** the swap's credit equivalent amount.

Answer:

The add-on factor is 0.5% of the interest rate swap principal.

$$\text{credit equivalent amount} = \$2.5 + (0.005 \times \$175) = \$3.375 \text{ million}$$

The nature of the counterparty determines risk weights. The credit equivalent amount is multiplied by the counterparty risk weight to calculate risk-weighted assets. Risk weights are shown in Figure 55.1.

EXAMPLE: Calculating risk-weighted assets for an off-balance sheet item

In the previous example, Blue Star Bank entered an interest rate swap that had a credit equivalent amount of \$3,375,000. **Calculate** the risk-weighted assets assuming (1) the counterparty is an OECD bank and (2) the counterparty is a corporation.

Answer:

RWA assuming counterparty is an OECD bank:

$$\$3,375,000 \times 0.2 = \$675,000$$

RWA assuming counterparty is a corporation:

$$\$3,375,000 \times 1.0 = \$3,375,000$$

The total RWAs of the bank are calculated by summing the on- and off-balance sheet risk-weighted items as follows:

$$\sum_{i=1}^N w_i L_i + \sum_{j=1}^M w_j C_j$$

where:

w_i = the risk weight of the counterparty of the i th on-balance sheet item

L_i = principal of the i th on-balance sheet item

w_j = the risk weight of the counterparty of the j th off-balance sheet item

C_j = credit equivalent amount of the j th off-balance sheet item

The bank must maintain at least 8% capital to RWA.

EXAMPLE: Calculating risk-based capital

Using the information from the previous three examples, **calculate** Blue Star Bank's required capital, assuming the swap counterparty is a corporation.

Answer:

$$(\$175 \text{ million} + \$3.375 \text{ million}) \times 0.08 = \$14.27 \text{ million}$$

The **original exposure method** is only allowed for interest rate and foreign exchange contracts. For the original exposure method, nations may ignore current market values and choose to use either the original or remaining maturity of the derivative.

For banks choosing the original exposure method, a sample of add-on factors is shown in Figure 55.4.

Figure 55.4: Original Exposure Method: Add-On Factors (D) as a Percentage of Principal for Interest Rate and Foreign Exchange Contracts

Remaining Maturity in Years	Interest Rate	Foreign Exchange
< 1 year	0.5	2.0
1 to 2 years	1.0	5.0
> 2 years	$1.0 + 1.0 \times \text{INT}(M - 1)$	$5.0 + 3.0 \times \text{INT}(M - 1)$

Note: M = maturity of the exposure; INT(X) = the closest integer to X

The 1995 Amendment: Netting

LO 55.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.

By 1995, quantitative market risk management was popular, value at risk (VaR) was in widespread use, and the stock market had crashed in 1987. At that point, the “Market Risk Amendment” was put in place allowing for bilateral netting of exposures. Before netting was permitted, Basel I disincentivized hedging. For example, Bank A could buy protection from Bank B against falling rates and later enter a contract with the same counterparty and same notional value to sell protection. Changes in interest rates in this case would have offsetting effects, but Basel I applied an add-on to each swap. The International Swaps and Derivatives Association master agreement allowed positive and negative values to offset one another, called netting.

Netting is frequently employed in transactions that generate credit exposure to both sides. When each side has credit risk, we value and net the two to determine which side has the greater obligation. For example, assume Counterparty A has swap transactions with Counterparty B valued at +\$20 million, −\$7 million, and +\$5 million. If Counterparty B defaults without a netting agreement, Counterparty A would lose the \$25 million (20 + 5) that is owed (assuming no recovery). With netting, Counterparty A would only lose the net amount of the transactions, which is \$18 million (20 − 7 + 5).

The impact of netting was not taken into consideration under the Basel I Accord in 1988. However, by 1995, the accord was modified to allow for a reduction in the CEA, given that a legal netting agreement was in place. To measure the impact of netting, the **net replacement ratio (NRR)** was developed. This ratio is equal to the current exposure with netting divided by the current exposure without netting. For example, the NRR from the previous example between Counterparty A and Counterparty B is equal to 0.72 (\$18 million / \$25 million). The NRR value is incorporated into a modified version of the credit equivalent amount by multiplying it by the product of the add-on factor (D) and the principal amount (L). This modification can then be used to reduce a bank’s RWA. Credit equivalent amounts are calculated as:

$$\text{CEA} = \max\left(\sum_{i=1}^N V_i, 0\right) + \sum_j \left[0.4 \times D_j + 0.6 \times D_j \times \text{NRR}\right]$$

In calculating CEAs, the complete netting of market positions is allowed and add-ons are reduced for each category.

EXAMPLE: Credit equivalent amount for derivatives with netting

Using the information in the following table regarding a portfolio of five derivatives from two counterparties, (1) **determine** which values may be netted against each other, (2) **calculate** the NRR, and (3) **calculate** the CEA.

Counter-party	Type	Maturity	Notional Principal	Market Value	Add-on Factor	D_j (i.e., the add-on amount)
1	Interest rate	2	100	-5	0.5%	$100 \times 0.005 = 0.5$
1	Interest rate	3	100	0	0.5%	$100 \times 0.005 = 0.5$
1	Foreign exchange	2	100	15	5%	$100 \times 0.05 = 5.0$
2	Equity option	6	200	0	10%	$200 \times 0.10 = 20$
2	Soybean option	0.5	200	-10	10%	$200 \times 0.10 = 20$

Answer:

(1) With netting, the current exposure portion of the credit equivalent amount is 10 for the first counterparty (i.e., the -5 exposure on the interest rate derivative is netted against the 15 exposure on the foreign exchange derivative). It is 0 for the second counterparty for a total of 10. The current exposure cannot be less than zero and the -10 soybean market value cannot be netted against the 10 from counterparty 1; it may only be netted against positive exposures from the second counterparty.

(2) The NRR = 0.667. The numerator is the current exposure with netting (i.e., 10) and the denominator is the total positive exposure (i.e., 15).

(3) The add-on must be calculated separately for each type of derivative, multiplying the add-on factor by the notional amount to obtain D_j (see column 7 for calculations).

$$\begin{aligned}\text{CEA} &= 10 + (0.4 \times 0.5 + 0.6 \times 0.5 \times 0.667) \\ &+ (0.4 \times 0.5 + 0.6 \times 0.5 \times 0.667) \\ &+ (0.4 \times 5.0 + 0.6 \times 5.0 \times 0.667) \\ &+ (0.4 \times 20.0 + 0.6 \times 20.0 \times 0.667) \\ &+ (0.4 \times 20.0 + 0.6 \times 20.0 \times 0.667) \\ &= 10 + 0.4 + 0.4 + 4.0 + 16.0 + 16.0 = 46.8\end{aligned}$$

The 1996 Amendment: Market Risk and Trading Activities

Market risk is the risk associated with changes in the market values of trading book assets. The 1995 amendment requirements did not capture market risk. The goal of the **1996 Amendment** to the 1988 Basel Accord was to require banks to measure market risks associated with trading activities and maintain capital to back those risks. Banks

must **mark-to-market** (i.e., *fair value accounting*) bonds, marketable equity securities, commodities, foreign currencies, and most derivatives that are held by the bank for the purpose of trading (referred to as the *trading book*). Banks do not have to use fair value accounting on assets they intend to hold for investment purposes (referred to as the *banking book*). This includes loans and some debt securities. The 1996 Amendment proposed two methods for calculating market risk:

1. Standardized Measurement Method
2. Internal Model-Based Approach

Standardized Measurement Method

This method assigns a capital charge separately to each of the items in the trading book. It ignores correlations between the instruments. Banks with less sophisticated risk management processes are more likely to use this approach.

Internal Model-Based Approach

The internal model-based approach allowed banks to internally develop risk measures to then use in regulator-specified formulas. This is in contrast to the standardized approach, where most details were based on observable characteristics such as the remaining maturity of a position. This method involves using a formula specified in the amendment to calculate a value at risk (VaR) measure and then convert the VaR into a capital requirement. Capital charges are generally lower using this method because it better reflects the benefits of diversification (i.e., correlations between the instruments). As such, banks with more advanced risk management functions prefer the internal model-based approach.

Risks covered by the VaR model include movements in broad market variables such as interest rates, exchange rates, stock market indices, and commodity prices.

Under both approaches, for each of the five categories, capital charges were calculated separately for specific risk (SR) and general market risk (MR). The VaR model does not incorporate company-specific risks such as changes in a firm's credit spread or changes in a company's stock price. The SR charge instead captures these company-specific risks. For example, a corporate bond has interest rate risk, captured by VaR, and credit risk, captured by the SR.

The 1996 Amendment created a new class of capital, Tier 3 capital. **Tier 3 capital** consisted of short-term subordinated, unsecured debt with an original maturity of at least two years. It could be used to meet the market risk capital requirement at the time of the amendment. Tier 3 capital has subsequently been eliminated under Basel III.

According to the 1996 Amendment, the market risk VaR is calculated with a 10-trading-day time horizon and a 99% confidence level.

$$\max(V_a R_{t-1}, m \times VaR_{avg})$$

where:

VaR_{t-1} = previous day's VaR

VaR_{avg} = the average VaR over the past 60 trading days

m = multiplicative factor

The multiplicative factor must be at least three but may be set higher by bank supervisors if they believe a bank's VaR model has deficiencies. This means the capital charge will be the higher of either the previous day's VaR or three times the average of the daily VaR plus a charge for company-specific risks.

Banks calculate a 10-day 99% VaR for SR. Regulators then apply a multiplicative factor (which must be at least four) similar to m_c to determine the capital requirement. The total capital requirement for banks using the internal model-based approach must be at least 50% of the capital required using the standardized approach.

The bank's total capital charge, according to the 1996 Amendment, is the sum of the capital required according to Basel I, described in LO 55.b, and the capital required based on the 1996 Amendment, described in this LO. For simplicity, the RWAs for market risk capital was defined as 12.5 times the value given in the previous equation. The total capital a bank has to keep under the 1996 Amendment is:

$$\text{total capital} = 0.08 \times (\text{credit risk RWA} + \text{market risk RWA})$$

where:

$$\text{market RWA} = 12.5 \times [\max(V_a R_{t-1}, m \times V_a R_{\text{avg}})]$$

$$\text{credit RWA} = \Sigma(\text{RWA on-balance sheet}) + \Sigma(\text{RWA off-balance sheet})$$

EXAMPLE: Market risk capital charge

A bank calculates the previous day's market risk VaR as \$10 million. The average VaR over the preceding 60 trading days is \$8 million. Assuming a multiplicative factor of three, **calculate** the market risk capital charge.

Answer:

$$\text{market risk capital charge} = 0.08 \times [12.5 \times (3 \times \$8 \text{ million})] = \$24 \text{ million}$$

Backtesting

The 1996 Amendment also requires banks to backtest the one-day 99% VaR over the previous 250 days. A bank calculates the VaR using its current method for each of the 250 trading days and then compares the calculated VaR to the actual loss. If the actual loss is greater than the estimated loss, an **exception** is recorded. The multiplicative factor (m) is set based on the number of exceptions. If, over the previous 250 days, the number of exceptions is:

- less than 5, m is usually set equal to 3.
- 5, 6, 7, 8, or 9, m is set equal to 3.4, 3.5, 3.65, 3.75, and 3.85, respectively.
- greater than 10, m is set equal to 4.

The bank supervisor has discretion regarding the multiplier. If the exception is due to changes in the bank's positions during that day, the higher multiplier may or may not be used. If the exception is due to deficiencies in the bank's VaR model, higher multipliers are likely to be applied. There is no guidance to supervisors in terms of higher multipliers if an exception is simply the result of bad luck.

PROFESSOR'S NOTE



Basel I had a number of shortcomings that were remedied over the coming years with new capital accords. For example, Basel I treats all corporate loans the same in terms of capital requirements. The creditworthiness of the borrower is ignored. Also, Basel I did not include a model for default correlations.



MODULE QUIZ 55.1

1. Michigan One Bank and Trust has entered a \$200 million interest rate swap with a corporation. The remaining maturity of the swap is six years. The current value of the swap is \$3.5 million. Using the table below to find the add-on factor for the interest rate swap, the equivalent risk-weighted asset (RWA) under Basel I is closest to:

Add-On Factors as a Percentage of Principal for Derivatives

Remaining Maturity in Years	Interest Rate	Equity
< 1 year	0.0	6.0
1 to 5 years	0.5	8.0
> 5 years	1.5	10.0

- A. \$3,000,000.
 - B. \$3,250,000.
 - C. \$3,500,000.
 - D. \$6,500,000.
2. Saugatuck National Bank uses the internal model-based approach to set market risk capital as prescribed by the 1996 Amendment to the 1988 Basel Accord. The bank has backtested its 99% one-day VaRs against the actual losses over the last 250 trading days. Based on the results of the backtesting, the bank recorded 11 exceptions. Based on these results, the multiplicative factor (m) in the model should be set:
 - A. less than 3.
 - B. equal to 3.
 - C. between 3.1 and 3.9.
 - D. equal to 4.

MODULE 55.2: BASEL II REGULATIONS

Pillars of Sound Bank Management

LO 55.d: Describe changes to the Basel regulations made as part of Basel II, including the three pillars.

While Basel I improved the way capital requirements were determined for banks worldwide, it had some major limitations. First, all corporate loans were treated the same (i.e., a risk weight of 100%) regardless of the creditworthiness of the borrower. A firm with an AAA credit rating was treated the same as a borrower with a C rating. Basel I also ignored the benefits of diversification (i.e., there was no model of default correlation). Basel II, proposed in June 1999 and, after multiple revisions, published in 2004 and implemented in 2007, corrected a number of the deficiencies in Basel I. The rules applied to “internationally active” banks and thus many small regional banks in the United States were not subject to the requirements but fell under Basel IA, similar to Basel I, instead. All European banks are regulated under Basel II.

There are three pillars under Basel II: (1) minimum capital requirements, (2) supervisory review, and (3) market discipline.

Pillar 1: Minimum Capital Requirements

The key element of Basel II regarding capital requirements is to consider the credit ratings of counterparties. Capital charges for market risk remained unchanged from the 1996 Amendment. Basel II added capital charges for operational risk. Banks must hold total capital equal to 8% of RWA under Basel II, as under Basel I. Total capital under Basel II is calculated as:

$$\text{total capital} = 0.08 \times (\text{credit risk RWA} + \text{market risk RWA} + \text{operational risk RWA})$$

Pillar 2: Supervisory Review

Basel II is an international standard governing internationally active banks across the world. A primary goal of Basel II is to achieve overall consistency in the application of capital requirements. However, Pillar 2 allows regulators from different countries some discretion in how they apply the rules. This allows regulatory authorities to consider local conditions when implementing rules. Supervisors must also encourage banks to develop better risk management functions and must evaluate bank risks that are outside the scope of Pillar 1, working with banks to identify and manage all types of risk. Banks were also required to have internal capital adequacy and assessment processes (ICAAP) that take their risk profiles into account.

Pillar 3: Market Discipline

The goal of Pillar 3 is to increase transparency. Banks are required to disclose more information about the risks they take and the capital allocated to these risks. Qualitative disclosures such as the bank's corporate structure and quantitative disclosures, such as the bank's capital, risk exposures, and risk measures, were required. The key idea behind Pillar 3 is that if banks must share more information with shareholders (and potential shareholders), they will make better risk management decisions. Banks have discretion in determining what is relevant and material and thus what should be disclosed. Also, using data provided by banks, supervisors fine-tuned the design of the Accord, repeatedly conducting quantitative impact studies (QIS). According to Basel II, banks should disclose:

- The entities (banks and other businesses such as securities firms in Europe) to which Basel II rules are applied.
- A description of the characteristics, terms, and conditions of all the capital instruments held by the bank.
- A list of the instruments comprising the bank's Tier 1 capital. The amount of capital provided by each instrument should also be disclosed.
- A list of the instruments comprising the bank's Tier 2 capital.
- The capital requirements for each type of risk covered under Basel II: credit, market, and operational risks.
- Information about other bank risks.
- Information about the bank's risk management function, how it is structured, and how it operates.

- In sum, Basel II contained four important innovations:
 1. More sophisticated risk weight formulas based on the internal risk measures of banks and modern concepts of credit risk management.
 2. Required capital for operational risk, in addition to credit and market risks.
 3. Specific requirements for supervision related to capital (Pillar 2) and improved transparency as a result of greater bank disclosures (Pillar 3).
 4. Use of QIS to improve the Basel II Accord.

Credit Risk Capital Requirements

LO 55.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.

LO 55.f: Calculate credit risk capital under Basel II utilizing the IRB approach.

Basel II specifies three approaches that banks can use to measure credit risk:

1. Standardized approach.
2. Foundation internal ratings-based (IRB) approach.
3. Advanced IRB approach.

The Standardized Approach

The **standardized approach** is used by banks with less sophisticated risk management functions. The risk-weighting approach is similar to Basel I, although some risk weights were changed. Significant changes include:

- OECD status is no longer considered important under Basel II.
- The credit ratings of countries, banks, and corporations are relevant under Basel II. For example, sovereign (country) risk weights range from 0% to 150%, and bank and corporate risk weights range from 20% to 150%.
- Bank supervisors may apply lower risk weights when the exposure is to the country in which the bank is incorporated.
- Bank supervisors may choose to base risk weights on the credit ratings of the countries in which a bank is incorporated rather than on the bank's credit rating. For example, if a sovereign rating is AAA to AA–, the risk weight assigned to a bank is 20%. The risk weight increases to 150% if the country is rated below B–, and is 100% if the country's bonds are unrated.
- Risk weights are lower for unrated countries, banks, and companies than for poorly-rated countries, banks, and companies.
- Bank supervisors who elect to use the risk weights in Figure 55.5 are allowed to lower the risk weights for claims with maturities less than three months. For example, the risk weights for short-maturity assets may range from 20% if the rating is between AAA to BBB– or unrated, to 150% if the rating is below B–.

A sample of risk weights under the standardized approach is presented in Figure 55.5.

Figure 55.5: Risk Weights (As a Percentage) Under Basel II's Standardized Approach

	AAA to AA-	A+ to A-	BBB+ to BBB-	BB+ to BB-	B+ to B-	Below B-	Unrated
Country	0	20	50	100	100	150	100
Bank	20	50	50	100	100	150	50
Corporation	20	50	100	100	150	150	100

Additionally, a risk weight of 75% is applied to unrated retail, 35% to unrated mortgage, 0% to cash, and 100% to other.

Collateral Adjustments

Banks adjust risk weights for collateral using the **simple approach**, similar to Basel I, or the **comprehensive approach**, used by most banks. Under the simple approach, the risk weight of the collateral replaces the risk weight of the counterparty. The counterparty's risk weight is used for exposure not covered by collateral. Collateral must be revalued at least every six months. A minimum risk weight of 20% is applied to collateral. Using the comprehensive approach, banks adjust the size of the exposure upward and the value of the collateral downward, depending on the volatility of the exposure and of the collateral value.

EXAMPLE: Adjusting for collateral using the simple approach

Blue Star Bank has a \$100 million exposure to Monarch, Inc. The exposure is secured by \$80 million of collateral consisting of AAA-rated bonds. Monarch has a credit rating of B. The collateral risk weight is 20% and the counterparty risk weight is 150%. Using the simple approach, **calculate** the risk-weighted assets.

Answer:

$$(0.2 \times 80) + (1.5 \times 20) = \$46 \text{ million risk-weighted assets}$$

EXAMPLE: Adjusting exposure and collateral using the comprehensive approach

Blue Star Bank assumes an adjustment to the exposure in the previous example of +15% to allow for possible increases in the exposures. The bank also allows for a -20% change in the value of the collateral. **Calculate** the new exposure using the comprehensive approach.

Answer:

$$(1.15 \times 100) - (0.8 \times 80) = \$51 \text{ million exposure}$$

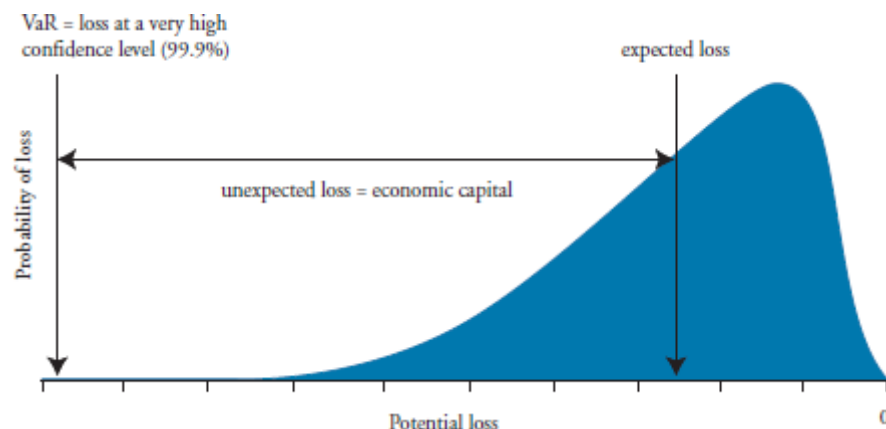
Applying a risk weight of 150% to the exposure:

$$1.5 \times 51 = \$76.5 \text{ million risk-weighted assets}$$

The Internal Ratings-Based (IRB) Approach

United States regulators applied Basel II to large banks only. As such, regulatory authorities decided that the **IRB approach** must be used by U.S. banks. Under the IRB approach, the capital requirement is based on a VaR calculated over a one-year time horizon and a 99.9% confidence level. The model underlying this approach is shown in Figure 55.6. Note that any losses beyond the VaR threshold amount are considered *stress losses*. These losses would not be covered by economic capital.

Figure 55.6: Capital Requirement



The goal of the IRB approach is to capture unexpected losses (UL). Expected losses (EL) should be covered by the bank's pricing (e.g., charging higher interest rates on riskier loans to cover EL). The capital required by the bank is thus VaR minus the bank's EL. The VaR can be calculated using a Gaussian copula model of time to default. That is:

$$DR_{99.9_i} = WCDR_i = N \left[\frac{N^{-1}(PD_i) + \sqrt{\rho} N^{-1}(0.999)}{\sqrt{1-\rho}} \right]$$

In this equation, $WCDR_i$ is the **worst case probability of default** or the default rate at the 99.9 percentile ($DR_{99.9}$). The bank can be 99.9% certain that the loss from the i th counterparty will not exceed this amount in the coming year. PD is the one-year **probability of default** of the i th obligor given a large number of obligors, and ρ is the **copula correlation** between each pair of obligors.



PROFESSOR'S NOTE

The WCDR or worst case probability of default can be referred to as the $DR_{99.9}$ (default rate at the 99.9 percentile). The original research by Gordy (2003)¹ developed the “asymptotic single risk factor” model of credit losses, commonly referred to as a one-factor Gaussian copula model. This research led to the IRB approach.

Assuming the bank has a large portfolio of instruments such as loans and derivatives with the same correlation, the one-year 99.9% VaR is approximately:

$$VaR_{99.9\%, 1\text{-year}} \approx \sum_i EAD_i \times LGD_i \times DR_{99.9_i}$$

EAD_i is the **exposure at default** of the i th counterparty or the dollar amount the i th counterparty is expected to owe if it defaults. For example, if the counterparty has a loan outstanding, EAD would likely be the principal amount outstanding on the loan at

the time of default. LGD_i is the **loss given default** for the i th counterparty or the proportion of the EAD_i that is expected to be lost in the event of default. For example, if the bank expected to collect (i.e., recover) 40% in the event of default, the LGD_i would be 60% (i.e., $1 - 0.4 = 0.6$).

Recall from Book 2 that the expected loss (EL) from default is computed as:

 Numberfigure

The capital the bank is required to maintain is the excess of the worst-case loss over the bank's expected loss defined as follows:

$$\text{capital} = \sum_i [EAD_i \times LGD_i \times DR_{99.9}] - \sum_i [EAD_i \times LGD_i \times PD_i]$$

$$\text{capital} = \text{VaR}_{99.9\%, 1\text{-year}} - \text{EL}$$

Note that $DR_{99.9}$, PD , and LGD are expressed as decimals while EAD is expressed in dollars.

Figure 55.7 shows the dependence of the one-year $DR_{99.9}$ on PD and correlation, ρ .

Figure 55.7: Dependence of One-Year, 99.9% $DR_{99.9}$ on PD and ρ

	$PD = 0.1\%$	$PD = 0.5\%$	$PD = 1\%$	$PD = 1.5\%$	$PD = 2.0\%$
$\rho = 0.0$	0.1%	0.5%	1.0%	1.5%	2.0%
$\rho = 0.2$	2.8%	9.1%	14.6%	18.9%	22.6%
$\rho = 0.4$	7.1%	21.1%	31.6%	39.0%	44.9%
$\rho = 0.6$	13.5%	38.7%	54.2%	63.8%	70.5%
$\rho = 0.8$	23.3%	66.3%	83.6%	90.8%	94.4%

It is clear from Figure 55.7 that $DR_{99.9}$ increases as the correlation between each pair of obligors increases and as the probability of default increases. If the correlation is 0, then $DR_{99.9}$ is equal to PD .

Basel II assumes a relationship between the PD and the correlation based on empirical research. The formula for correlation is:

$$\rho = 0.12 \times (1 + e^{-50 \times PD})$$

Note that there is an inverse relationship between the correlation parameter and the PD . As creditworthiness declines, the PD increases. At the same time, the PD becomes more idiosyncratic and less affected by the overall market, thus the inverse relationship.

From a counterparty's perspective, the capital required for the counterparty incorporates a maturity adjustment as follows:

$$\text{capital} = EAD \times LGD \times (DR_{99.9} - PD) \times MA$$

where:

$$MA = \text{maturity adjustment} = [1 + (M - 2.5) \times b] / (1 - 1.5 \times b)$$

M = maturity of the exposure

$$b = [0.11852 - 0.05478 \times \ln(PD)]^2$$

The **maturity adjustment**, MA, allows for the possibility of declining creditworthiness and/or the possible default of the counterparty for longer term exposures (i.e., longer than one year). If $M = 1.0$, then $MA = 1.0$ and the maturity adjustment has no impact. The risk-weighted assets are calculated as 12.5 times capital required:

$$RWA = 12.5 \times [EAD \times LGD \times (DR99.9 - PD) \times MA]$$

The capital required is 8% of RWA. The capital required should be sufficient to cover unexpected losses over a one-year period with 99.9% certainty (i.e., the bank is 99.9% certain the unexpected loss will not be exceeded). Expected losses should be covered by the bank's product pricing. Theoretically, the DR99.9 is the probability of default that happens once every 1,000 years. If the Basel Committee finds the capital requirements too high or too low, it reserves the right to apply a scaling factor (e.g., 1.06 or 0.98) to increase or decrease the required capital.



PROFESSOR'S NOTE

On the exam, if you begin with RWA, multiply by 0.08 to get the capital requirement. If instead you begin with the capital requirement, multiply by 12.5 (or divide by 0.08) to get RWA. In other words, these percentages are simply reciprocals (i.e., $1/0.08 = 12.5$).

The **foundation IRB approach** and the **advanced IRB approach** are similar with the exception of who provides the estimates of LGD, EAD, and M. The key differences between the two approaches are outlined by the following.

Foundation IRB Approach

- The bank supplies the PD estimate. For bank and corporate exposures, there is a 0.03% floor set for PD.
- The LGD, EAD, and M are supervisory values set by the Basel Committee. The Basel Committee set LGD at 45% for senior claims and 75% for subordinated claims. If there is collateral, the LGD is reduced using the comprehensive approach described earlier.
- The EAD is calculated similar to the credit equivalent amount (CEA) required under Basel I. It includes the impact of netting.
- M is usually set to 2.5.

Advanced IRB Approach

- Banks supply their own estimates of PD, LGD, EAD, and M.
- PD can be reduced by credit mitigants such as credit triggers subject to a floor of 0.03% for bank and corporate exposures.
- LGD is primarily influenced by the collateral and the seniority of the debt.
- With supervisory approval, banks can use their own estimates of credit conversion factors when calculating EAD.

Foundations IRB Approach and Advanced IRB Approach for Retail Exposures

- The two methods are merged for retail exposures. Banks provide their own estimates of PD, EAD, and LGD.
- There is no maturity adjustment (MA) for retail exposures.
- The capital requirement is $EAD \times LGD \times (DR99.9 - PD)$.
- Risk-weighted assets are $12.5 \times EAD \times LGD \times (DR99.9 - PD)$.
- Correlations are assumed to be much lower for retail exposures than for corporate exposures.

EXAMPLE: RWA under the IRB approach

Assume Blue Star Bank has a \$150 million loan to an A-rated corporation. The PD is 0.1% and the LGD is 50%. The DR99.9 is 3.4%. The average maturity of the loan is 2.5 years. **Calculate** the RWA using the IRB approach and **compare** it to the RWA under Basel I.

Answer:

$$b = [0.11852 - 0.05478 \times \ln(0.001)]^2 = 0.247$$

$$MA = 1 / [1 - (1.5 \times 0.247)] = 1.59$$

risk-weighted assets

$$= 12.5 \times 150 \times 0.5 \times (0.034 - 0.001) \times 1.59$$

$$= \$49.19 \text{ million}$$

Under Basel I, the RWA for corporate loans was 100% or \$150 million in this case. Thus, the IRB approach lowers the RWA for higher-rated corporate loans, in this case from \$150 million to \$49.19 million.

Operational Risk Capital Requirements

LO 55.g: Compare the basic indicator approach, the standardized approach, and the advanced measurement approach for the calculation of operational risk capital under Basel II.

Basel II requires banks to maintain capital for operational risks. Operational risks include failures of the bank's procedures that result in loss (e.g., fraud, losses due to improper trading activities such as experienced at Barings Bank in the mid-1990s). External events that result in loss, such as a fire, are also considered operational risks.

Under Basel II, there are three approaches banks may use to calculate capital for operational risk:

1. Basic indicator approach.
2. Standardized approach.
3. Advanced measurement approach.

Basic Indicator Approach (BIA)

This is the simplest approach and is used by banks with less sophisticated risk management functions. The required capital for operational risk is equal to the bank's average annual gross income (i.e., net interest income plus noninterest income) over the last three years multiplied by 0.15. In other words, capital for operational risk must equal 15% of three-year average annual gross income, ignoring years with negative gross income. Also, positive capital may be offset by negative capital within a year. However, if the total year's capital is expected to be negative, the year is ignored in the average. For example, a bank with gross income of \$20 billion in year one, -\$2 billion in year two, and \$12 billion in year three would have a capital requirement of $(\$20 + \$12)/2 \times 0.15$ or \$2.4 billion because the year with negative gross income is ignored from the calculation.

Standardized Approach

This method is similar to the basic indicator approach. The primary difference between the two approaches is that a different multiplier is applied to the bank's gross income for different lines of business. For example, gross earnings generated from retail banking might have a 12% multiplier, from commercial banking a 15% multiplier, and from payments and settlement activities an 18% multiplier.

Advanced Measurement Approach (AMA)

Like the IRB approach discussed for credit risk, the capital requirement for operational risk under the advanced measurement approach is based on an operational risk loss (i.e., VaR) calculated over a one-year time horizon with a 99.9% confidence level. The approach has an advantage in that it allows banks to consider risk mitigating factors such as insurance contracts (e.g., fire insurance).



PROFESSOR'S NOTE

While Basel II generally lowered credit risk capital requirements for most banks, requiring banks to hold capital for operational risks had the effect of raising overall capital requirements back to (approximately) Basel I levels.

Solvency II Framework

LO 55.h: Summarize elements of the Solvency II capital framework for insurance companies.

In the United States and the European Union, Solvency II establishes capital requirements for operational, investment, and underwriting risks of insurance companies. Solvency II requires capital buffers above the minimum capital requirement (MCR), called the **solvency capital requirement (SCR)**. The two approaches an insurance firm can use to calculate the solvency capital requirement (SCR) under Solvency II are:

1. Standardized approach.
2. Internal models approach.

Standardized Approach

Analogous to Basel II, the standardized approach to calculating SCR under Solvency II is intended for less sophisticated insurance firms that cannot or do not want to develop their own firm-specific risk measurement model. It is intended to capture the risk profile of the average firm and is more cost efficient for smaller firms with less fully developed risk management functions.

Internal Models Approach

This approach is similar to the IRB approach under Pillar 1 of Basel II. A VaR is calculated with a one-year time horizon and a 99.5% confidence level. There is a capital charge for the following three types of risk:

1. *Underwriting risk*: divided into risks arising from life insurance, nonlife insurance (such as property and casualty insurance), and health insurance.
2. *Investment risk*: divided into market risk and credit risk.
3. *Operational risk*.

As with Basel II, regulators have implemented quantitative impact studies (QISs) to examine if capital is sufficient to weather significant market events. Also, similar to Basel II, insurance companies can use a combination of Tier 1 capital (equity, retained earnings, and equivalents), Tier 2 capital (liabilities available for write-off in a liquidation and subordinated to policyholders), and Tier 3 capital (subordinated to policyholders but not satisfying other criteria for Tier 2 capital).

Internal models developed by insurance companies must satisfy the following three tests:

1. **Statistical quality test**: This tests the quality of the data and the methodology the firm uses to calculate VaR.
2. **Calibration test**: This tests whether risks are measured in agreement with an industry-wide SCR standard and target criteria set by regulators.
3. **Use test**: This test determines if the model is relevant and used by risk managers in business decision-making.



MODULE QUIZ 55.2

1. Bank Macatawa has a \$150 million exposure to Holland Metals Co. The exposure is secured by \$125 million of collateral consisting of AA+-rated bonds. Holland Metals Co. is unrated. The collateral risk weight is 20%. Bank Macatawa assumes an adjustment to the exposure of +15% to allow for possible increases in the exposure and allows for a -25% change in the value of the collateral. Risk-weighted assets for the exposure are closest to:
 - A. \$78.75 million.
 - B. \$93.75 million.
 - C. \$118.13 million.
 - D. \$172.50 million.
2. Which of the following accords first required banks to hold capital for operational risk?
 - A. Basel I.
 - B. The 1996 Amendment to Basel I.
 - C. Basel II.
 - D. Solvency II.
3. Which of the following statements is correct regarding capital requirements for insurance companies?

- A. Basel II includes the regulation of banks and insurance companies in the three pillars.
- B. The minimum capital requirement is likely to be higher than the solvency capital requirement for insurance companies.
- C. The repercussion for violating the solvency capital requirement is likely liquidation and the transfer of company insurance policies to another firm.
- D. The internal models approach to calculating the solvency capital requirement is similar to internal ratings-based approach under Basel II in that the firm must calculate a VaR with a one-year time horizon.

KEY CONCEPTS

LO 55.a

Prior to 1988, bank capital regulations were inconsistent across countries and ignored the riskiness of individual banks. In 1988, the Basel Committee put forth its first guidance to set international risk-based capital adequacy standards known as Basel I.

Basel I was originally developed to cover credit risk capital requirements. It was amended in 1996 to also include market risk capital requirements. Basel II was introduced in 2004 and addressed not only credit and market risk capital but also operational risk capital.

LO 55.b

Under Basel I, banks calculated risk-weighted assets for on- and off-balance sheet items. Capital was required as a percentage of risk-weighted assets. For example, cash and Treasury securities received a 0% risk weight while commercial loans received a 100% risk weight. Off-balance sheet items were expressed as credit equivalent amounts and were “converted” into risk-weighted assets. Capital could be Tier 1 or Tier 2 but at least half of the capital requirement (4%) had to be met with Tier 1 capital (equity and noncumulative perpetual preferred). Capital requirements are:

- $(\text{Tier 1 capital} / \text{risk-weighted assets}) > 4\%$
- $(\text{Total capital} / \text{risk-weighted assets}) > 8\%$

LO 55.c

Netting is used to reduce credit risk by determining which side of the transaction has a greater obligation. The net replacement ratio (NRR) is equal to the current exposure with netting divided by the current exposure without netting. This ratio is used to modify the credit equivalent amount and reduce a bank’s risk-weighted assets.

Banks were required to measure market risk in addition to credit risk under the 1996 Amendment to the 1988 Basel Accord. The 1996 Amendment proposed two methods for calculating market risk including the standardized measurement method and the internal model-based approach. The standardized method assigns a capital charge separately to each of the items in the trading book. This method ignores correlations between the instruments. The internal model-based approach uses a formula specified in the amendment to calculate a value at risk (VaR) measure used to determine the capital requirement. Capital charges are generally lower using this method because it considers correlations between the instruments.

According to the 1996 Amendment, the market risk VaR is calculated with a 10-trading-day time horizon and a 99% confidence level. The capital requirement for market risk is:

$$\max(\text{VaR}_{t-1}, m \times \text{VaR}_{\text{avg}})$$

where:

VaR_{t-1} = previous day's VaR

VaR_{avg} = the average VaR over the past 60 days

m = multiplicative factor, minimum value of three

The 1996 Amendment requires banks to backtest the one-day 99% VaR over the previous 250 days. If the actual loss is greater than the estimated loss, an exception is recorded. The multiplicative factor (m) is set based on the number of exceptions. If, over the previous 250 days, the number of exceptions is:

- less than 5, m is usually set equal to three.
- 5, 6, 7, 8, or 9, m is set equal to 3.4, 3.5, 3.65, 3.75, and 3.85, respectively.
- greater than 10, m is set equal to four.

The bank supervisor has discretion regarding the multiplier.

LO 55.d

Basel II is an international standard, governing “internationally active banks.” There are three pillars under Basel II as follows:

1. *Pillar 1 – minimum capital requirements.* This pillar involves calculating capital based on the riskiness of the bank, taking into consideration credit risk, market risk, and operational risk.
2. *Pillar 2 – supervisory review.* A primary goal of Basel II is to achieve overall consistency in the application of the capital requirements across countries while, at the same time, giving supervisors discretion to consider market conditions in their own countries.
3. *Pillar 3 – market discipline.* Banks are required to disclose more information about the risks they take and the capital allocated to those risks. According to Basel II, if banks must share more information with shareholders (and potential shareholders), they will make better risk management decisions.

LO 55.e

Basel II specifies three approaches banks can use to measure credit risk, including the standardized approach, the foundation internal ratings-based (IRB) approach, and the advanced IRB approach. The standardized approach is the least complicated and the risk-weighting approach is similar to Basel I, although some risk weights were changed. The foundation IRB approach and the advanced IRB approach are similar. The key difference is who supplies the input variables. Banks supply their own estimates of probability of default (PD), loss given default (LGD), exposure at default (EAD), and the maturity adjustment (M) if using the advanced approach. Under the foundation approach, banks supply PD estimates, while the Basel Committee supplies the estimates of LGD, EAD, and M.

LO 55.f

Under the IRB approach, the credit risk capital requirement is based on a VaR calculated over a one-year time horizon and a 99.9% confidence level. Capital is computed as VaR minus the bank's expected loss, which is equivalent to the bank's unexpected loss.

LO 55.g

Basel II requires banks to maintain capital for operational risks. Operational risks include failures of the bank's procedures that result in loss (e.g., fraud, losses due to improper trading activities) or external events such as fires or floods that result in loss. Under Basel II, there are three approaches banks may use to calculate capital for operational risk including the basic indicator approach (the simplest), the standardized approach (similar to the basic indicator approach but with different multipliers applied to different lines of business), and the advanced measurement approach (the most complex). The capital requirement for operational risk under the advanced measurement approach is based on an operational risk loss calculated over a one-year time horizon and a 99.9% confidence level (i.e., VaR). The approach has an advantage in that it allows banks to consider risk mitigating factors such as insurance contracts.

In the context of Basel II, the default rate at the 99.9% percentile (DR99.9), often called the worst case probability of default, is the amount the bank can be 99.9% certain the loss will not exceed (from a specific counterparty) in the coming year. The one-year probability of default (PD) is the probability that an obligor, given a large number of obligors, will default. The exposure at default (EAD) is the dollar amount a counterparty is expected to owe if it defaults. The loss given default (LGD) is the proportion of the EAD that is expected to be lost in the event the counterparty defaults. For example, if the bank expected to collect 40% in the event of default by a counterparty, the LGD is 60%.

LO 55.h

Solvency II establishes capital requirements for operational, investment, and underwriting risks of insurance companies. There are two approaches an insurance firm can use to calculate the solvency capital requirement under Solvency II. They are the standardized approach and the internal models approach. The standardized approach is least complicated and is meant to capture the risk of the average firm. The internal models approach is similar to the IRB approach under Basel II. It involves calculating a VaR with a one-year time horizon and a 99.5% confidence level.

ANSWER KEY FOR MODULE QUIZZES

Module Quiz 55.1

1. **B** The add-on factor is 1.5% of the interest rate swap principal for swaps with a maturity greater than five years.

$$\text{credit equivalent amount} = \max(V, 0) + D \times L$$

where:

V = current value of the derivative to the bank

D = add-on factor

L = principal amount

credit equivalent amount = $\$3.5 + (0.015 \times \$200) = \$6,500,000$

The risk-weight factor for a corporate counterparty under Basel I is 100% for corporate loans.

(LO 55.b)

2. **D** Saugatuck National Bank must compare the VaR calculated using its current method for each of the 250 trading days to the actual loss over the same period to determine the multiplicative factor. If the actual loss is greater than the estimated loss, an exception is recorded. If, over the previous 250 days, the number of exceptions is:

- less than 5, m_c is usually set equal to three.
- 5, 6, 7, 8, or 9, m_c is set equal to 3.4, 3.5, 3.65, 3.75, and 3.85, respectively.
- greater than 10, m_c is set equal to four.

Therefore, with 11 exceptions recorded, m_c should be set equal to four. (LO 55.c)

Module Quiz 55.2

1. **A** Exposure = $(1.15 \times 150) - (0.75 \times 125) = 172.5 - 93.75 = \78.75

The risk weight for an unrated corporate counterparty based on Figure 55.5 in the reading is 100%. Applying the 100% risk weight, risk-weighted assets are:

risk-weighted assets = $1.0 \times 78.75 = \$78.75$ million

(LO 55.e)

2. **C** Basel II requires banks to maintain capital for operational risks. Banks can use three methods to measure operational risk. They are the basic indicator approach, the standardized approach, and the advanced measurement approach. (LO 55.g)
3. **D** Solvency II, not Basel II, establishes capital requirements for insurance companies. The minimum capital requirement (MCR) is just that, a true floor and is thus likely to be lower than the solvency capital requirement (SCR). The repercussion for violating the MCR is likely the prohibition of taking new business and possible liquidation. The repercussion for violating the SCR is the requirement of a plan to remedy the situation and bring the capital back to the required level. The internal models approach is similar to the internal ratings-based approach under Basel II in that the insurance company must calculate a one-year VaR with a 99.5% confidence level (versus 99.9% confidence for banks under Basel II). (LO 55.h)

¹ Gordy, M. B., 2003. "A risk-factor model foundation for ratings-based capital ratios." *Journal of Financial Intermediation* 12, 199–232.

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 assigned reading—Carey.

READING 56

SOLVENCY, LIQUIDITY, AND OTHER REGULATION AFTER THE GLOBAL FINANCIAL CRISIS

Study Session 9

EXAM FOCUS

Following the 2007–2009 financial crisis, the Basel Committee on Banking Supervision implemented reforms to shore up bank capital. This reading describes the measures taken in Basel 2.5 and Basel III to increase capital and tighten the definition of what constitutes capital in normal periods, create buffers to protect banks against loss in stress periods, and encourage banks to better manage liquidity risks by requiring banks to maintain liquidity coverage and net stable funding ratios. It also describes the major reforms that have been implemented since the 2007–2009 financial crisis that impact banks and bank regulation. For the exam, know the major changes to capital regulation, including the incremental risk capital charge, the comprehensive risk capital charge, the stressed value at risk (VaR), the capital conservation buffer, and the countercyclical buffer. Understand why banks may use less mainstream funding sources, such as contingent convertible bonds (CoCos), as a result of higher capital requirements. In addition, be able to calculate the leverage ratio, liquidity coverage ratio, and net stable funding ratio given a bank's balance sheet. Finally, be able to recognize and describe major reforms following the financial crisis including the creation of the Financial Stability Oversight Council and the Consumer Financial Protection Bureau.

MODULE 56.1: STRESSED VaR, INCREMENTAL RISK CAPITAL CHARGE, AND COMPREHENSIVE RISK CHARGE

Stressed VaR

LO 56.a: Describe and calculate the stressed VaR introduced in Basel 2.5 and calculate the market risk capital charge.

The implementation of Basel II coincided with the financial crisis of 2007–2009. Some people blamed Basel II because banks using the advanced internal ratings-based (IRB) approach to calculate credit risk were allowed to use their own estimates of probability of default (PD), loss given default (LGD), and exposure at default (EAD). Some believed Basel II was a move toward self-regulation and allowed banks to underestimate risks. As a result, the Basel Committee on Banking Supervision implemented a series of changes to the calculation of market risk capital. These changes were part of Basel 2.5, implemented December 31, 2011. There were three primary changes, including:

1. The calculation of a stressed value at risk (SVaR) measure.
2. The implementation of a new incremental risk change (IRC).
3. A comprehensive risk measure (CRM) for instruments sensitive to correlations between default risks of various instruments (e.g., securitizations and related instruments).

In the past, banks used the historical simulation method to calculate VaR in order to find the market risk capital charge. The assumption in the historical simulation method is that percentage changes in market variables the next day are random samples of the percentage changes over the previous one to four years. Volatilities of most market variables were low in the precrisis period (i.e., 2003–2006). As such, market risk VaRs were also low during this period and continuing for a time following the start of the financial crisis because models were still using historical data with low volatilities. To remedy the problem of low VaRs, Basel 2.5 required banks to calculate two VaRs, the usual VaR, using the historical simulation method, and a **stressed VaR**, using a 250-day period of stressed market conditions. Initially, regulators thought the year 2008 would be ideal for stressed market conditions. However, banks are now required to identify a one-year period in the most recent seven years when their actual portfolios performed poorly (i.e., were most stressed). This means the stressed period may be different across banks.

The total market risk capital charge is the sum of the usual bank VaR and the stressed VaR. The formula for the total capital charge is:

$$\max(\text{VaR}_{t-1}, m_r \times \text{VaR}_{\text{avg}}) + \max(\text{SVaR}_{t-1}, m_s \times \text{SVaR}_{\text{avg}})$$

where:

VaR_{t-1} = previous day's VaR, 10-day time horizon, 99% confidence level

VaR_{avg} = the average VaR over the past 60 days, 10-day time horizon, 99% confidence level

m_r = multiplicative factor, determined by supervisor, minimum value of three

SVaR_{t-1} = previous day's stressed VaR, 10-day time horizon, 99% confidence level

SVaR_{avg} = the average stressed VaR over the past 60 days, 10-day time horizon, 99% confidence level

m_s = stressed VaR multiplicative factor, determined by supervisor, minimum of three

EXAMPLE: Total market risk capital charge

Spartan State Bank has calculated a market risk VaR for the previous day equal to \$15.6 million. The average VaR over the last 60 days is \$4.8 million. The bank has calculated a stressed VaR for the previous day equal to \$17.7 million and an average stressed VaR equal to \$18.4 million. Spartan State Bank has an accurate risk measurement model and recorded only two exceptions while backtesting actual

losses against the calculated VaR. As such, the multiplicative factors, both m_r and m_s , are set to 3. **Calculate** the total market risk capital charge.

Answer:

$$\text{total capital charge} = \$15.6 \text{ million} + (\$18.4 \times 3) = \$70.8 \text{ million}$$



PROFESSOR'S NOTE

Because the stressed VaR will be equal to or, more likely, greater than VaR (because the stressed period should be more stressed than the more recent period, by definition), the capital charge for market risk under Basel 2.5, will be at least double the capital charge under Basel II.

Incremental Risk Charge

LO 56.b: Explain the process of calculating the incremental risk capital charge for positions held in a bank's trading book.

Prior to the financial crisis, the capital charge for exposures in the bank's trading book (i.e., bonds, marketable equity securities, commodities, foreign currencies, and most derivatives that are held by the bank for the purpose of trading) was generally lower than the capital charge for exposures in the banking book (i.e., instruments the bank intends to hold for investment purposes including loans and some debt securities). A one-year 99.9% confidence level VaR was required for calculating capital for the banking book while a multiplier was applied to a 10-day 99% VaR for capital to back the trading book. As a result, some banks would shift illiquid instruments that could potentially default to the trading book.

The Basel Committee proposed an **incremental default risk charge (IDRC)** in 2005 to correct the problem. The proposal required a 99.9% confidence level, one-year time horizon VaR for instruments in the trading book that are sensitive to default risk. This change had the effect of requiring roughly the same capital for trading book instruments as banking book instruments (trading book capital was the greater of market risk capital and banking book capital). However, because much of the 2007–2009 losses in the financial sector were due not to defaults but instead to downgrades, widening credit spreads, and losses of liquidity, the Basel Committee revised the IDRC to become an **incremental risk charge (IRC)**. Instead of instruments sensitive to default, it is now credit-sensitive instruments. Banks must consider ratings change sensitivities in addition to default sensitivity. Banks are expected to rebalance the portfolio through the year to lessen default risk.

As part of the IRC calculation, banks are required to estimate a liquidity horizon for each instrument in the portfolio. For example, assume an AA-rated bond in the portfolio has a liquidity horizon of six months. If at the end of six months the bond has defaulted or has been downgraded, it is assumed that the bank will replace the bond with an AA-rated bond comparable to the one held at the start of the period, and a loss would be recorded on the sale of the downgraded or defaulted position. This rebalancing is assumed at the end of each six-month period (or three months, nine months, etc.,

depending on the estimated liquidity horizon). The Basel Committee set the minimum liquidity horizon at three months.

This assumption of rebalancing to the beginning of the period position is known as the **constant level of risk** assumption. Small losses occur as bonds are downgraded and the portfolio is rebalanced, but the likelihood of default is lessened. Generally, this assumption reduces the one-year 99.9% VaR. As discussed in the previous reading, the specific risk charge (SRC) captures changing credit spreads.

Comprehensive Risk Charge

LO 56.c: Describe the comprehensive risk (CR) capital charge for portfolios of positions that are sensitive to correlations between default risks.

The **comprehensive risk (CR) charge** is a single capital charge for correlation-dependent instruments that replaces the **specific risk charge (SRC)** and the IRC. The measure accounts for risks in the “correlation book.” Instruments that are sensitive to the correlation between the default risks of different assets include asset-backed securities (ABS) and collateralized debt obligations (CDOs). In normal periods, there is little risk of loss for highly rated tranches of these instruments. However, in times of stress, as in the 2007–2009 financial crisis, correlations with other instruments increase and even the highest-rated tranches can be vulnerable to loss.

The committee has specified a standardized approach for rated instruments. Due to the experience of the financial crisis, *res securitizations*, such as CDOs of ABSs, have higher capital requirements than normal securitizations such as mortgage-backed securities.

Figure 56.1: Standardized Capital Charge for Correlation-Dependent Instruments

Type of Instrument	AAA to AA–	A+ to A–	BBB+ to BBB–	BB+ to BB–	Below BB– or Unrated
Securitization	1.6%	4%	8%	28%	100%
Resecuritization	3.2%	8%	18%	52%	100%

For instruments most exposed to losses (i.e., unrated instruments or instruments rated below BB–), the bank must hold dollar-for-dollar capital against the tranche, equivalent to a 100% capital charge. With supervisory approval, banks may use an internal model to calculate the CR charge. If a bank is allowed to use an internal model, it must routinely perform rigorous stress tests. Internal models must be sophisticated and capture the cumulative effects of several factors including:

- Credit spread risk.
- Multiple defaults.
- The volatility of implied correlations.
- The relationship between implied correlations and credit spreads.
- The costs of rebalancing hedges.
- The volatility of recovery rates.



PROFESSOR'S NOTE

The Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank) does not allow ratings to be used in setting capital requirements. As such, the United States is trying to devise its own CR rules that do not use ratings.



MODULE QUIZ 56.1

1. Which of the following statements about a stressed value at risk (VaR), required under Basel 2.5, is correct?
 - A. Basel 2.5 has established the year 2008 as the “stress” period. All banks use data from 2008 to calculate the stressed VaR.
 - B. The stressed VaR replaces the “normal” VaR for the purpose of calculating capital for credit risks.
 - C. Market risk capital under Basel 2.5 should be at least double that of market risk capital under Basel II due to the addition of the stressed VaR.
 - D. The stressed VaR must be calculated using a 99.9% confidence interval.
2. Banks are required to rebalance their portfolios as the creditworthiness of bonds decline, leading to losses over time but generally not to outright default. This requirement to specify a liquidity horizon for each instrument in the portfolio and rebalance at the end of the liquidity horizon is part of:
 - A. the incremental risk charge calculation.
 - B. the net stable funding charge formula.
 - C. the countercyclical buffer estimation.
 - D. the comprehensive risk charge calculation.

MODULE 56.2: BASEL III CAPITAL REQUIREMENTS, BUFFERS, AND LIQUIDITY RISK MANAGEMENT

Basel III Capital Requirements

LO 56.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**
-

Basel III increased capital for credit risk and tightened the definition of capital in response to the 2007–2009 financial crisis. Proposals were published in 2010 and 2011 and amended in later years. Basel III eliminated Tier 3 capital.

The 2007–2009 financial crisis revealed weaknesses in the Basel II framework, including:

- Market participants, at the depths of the financial crisis, cared only about tangible Tier 1 common equity capital (i.e., capital that could maintain a bank as a going concern).
- Regulators and other officials realized that distress at some banks posed greater threats to society than distress at other banks (i.e., systemic risk). As such, categories of systemically important financial institutions were created.

- It appeared that banks were able to “game” risk-based capital requirements. Leverage ratios were needed as a backup. This was reinforced by market participants who focused on both common equity capital and leverage ratios.
- Banks needed substantial capital after absorbing losses, to remain a going concern (not simply solvent).
- Some solvent banks suffered bank runs and, in some cases, failed. Wholesale funding was unstable and liquid reserves were inadequate to cover withdrawn funding. These problems led to the creation of liquidity requirements.
- Lehman (and other banks) did not honor its commitments as a counterparty in derivatives contracts. It became clear that capital was needed to cover counterparty credit risk.
- A large exposures framework (LEF) was created to set a common global standard to limit exposure concentrations to a single counterparty, especially between systemically important banks. Limits were set at 15% of capital for global systemically important institutions and 25% for other institutions.

Each category of capital is described as follows.

Tier 1 capital (or core capital) includes:

- Common equity including retained earnings (called Tier 1 equity capital or Tier 1 common capital).
- A limited amount of unrealized gains and losses and minority interest.

Tier 1 core capital does not include:

- Goodwill and other intangibles.
- Deferred tax assets.
- Changes in retained earnings arising from securitized transactions.
- Changes in retained earnings arising from the bank’s credit risk, called debit (debt) value adjustment (DVA).

Additional Tier 1 capital includes:

- Noncumulative perpetual preferred stock (additional Tier 1 capital is part of total Tier 1 capital).
- Debt with triggers that cause conversion to equity or write-downs.
- Approved minority interest not included in Core Tier 1.

Tier 2 capital (or supplementary capital) is designed to absorb losses after failure. It is meant to protect depositors and other creditors. It includes:

- Debt subordinated to depositors with an original maturity of five years or more.
- Some preferred stock, such as cumulative perpetual preferred.
- General loan loss reserves, not allocated to absorb losses on specific positions. Reserves may not exceed 1.25% of standardized approach risk-weighted assets (RWAs), or 0.6% of IRB RWAs.

Capital is adjusted downward to reflect:

- defined benefit pension plan deficits (but is not adjusted upward for surpluses).

- certain cross-holdings within a group.
- mortgage servicing rights greater than 10% of common equity.

In addition, there are rules governing capital issued by consolidated subsidiaries and also for the inclusion of minority interests.

Common equity is known as going-concern capital. It absorbs losses when the bank has positive equity (i.e., is a going concern). Tier 2 capital is known as gone-concern capital. When the bank has negative capital and is no longer a going concern, Tier 2 capital absorbs losses. Depositors are ranked above Tier 2 capital in liquidation so theoretically, as long as Tier 2 capital is positive, depositors should be paid in full.

Capital requirements for each tier and for total capital are:

- Tier 1 equity capital must be 4.5% of RWAs at all times.
- Total Tier 1 capital (i.e., equity capital plus additional Tier 1 capital such as perpetual preferred stock) must be 6% of RWAs at all times.
- Total capital (total Tier 1 capital plus Tier 2 capital) must be at least 8% of RWAs at all times. This requirement was left unchanged.

By comparison, under Basel I, the equity capital requirement was 2% of RWAs and the total Tier 1 capital requirement was 4% of RWAs. The new requirements are significantly more rigorous both because the percentages are higher and because the definition of what qualifies as equity capital has been tightened. The 8% total capital requirement is the same as under Basel I and Basel II, but again, the stricter definition of equity capital applies under Basel III.

Capital Conservation Buffer and Countercyclical Buffer

LO 56.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).

The **capital conservation buffer (CCB)** is meant to protect banks in times of financial distress. It is in keeping with the rationale behind the Prompt Corrective Action (PCA) system that was part of U.S. capital regulation beginning in 1991. The idea behind it is that when bank capital ratios approach minimums, increasingly stringent regulatory intervention is in order to move banks back to a well-capitalized position.

The CCB requires banks to build up a buffer of Tier 1 equity capital equal to 2.5% of RWAs in normal times, which will then be used to cover losses in stress periods. This means that in normal times a bank should have a minimum 7% Tier 1 equity capital ratio (i.e., $4.5\% + 2.5\% = 7.0\%$). Total Tier 1 capital must be 8.5% of RWAs and Tier 1 plus Tier 2 capital must be 10.5% of RWAs in normal periods. Banks need an extra cushion against loss during stress periods. The idea behind the buffer is that it is easier for banks to raise equity capital in normal periods than in periods of financial stress.

Dividend payments are constrained when the buffer is wholly or partially used up. For example, if a bank's Tier 1 equity capital ratio is 6%, the bank must retain a minimum of 60% earnings, thus dividends cannot exceed 40% of earnings.

In an effort to avoid repeating the government bailouts during the 2007–2009 financial crisis, regulations were established to ensure that **global systemically important banks (G-SIBs)** have sufficient capital to avoid financial difficulties. G-SIBs are a subset of systemically important financial institutions (SIFI), which also includes nonbanks deemed “too big to fail.” The failure of an SIFI could potentially create significant issues for the global financial system.

An additional capital requirement was implemented for G-SIBs. The rationale, similar to the rationale for the CCB, is that there is great costs to society if G-SIBs are in distress or fail. Larger buffers (relative to non-G-SIBs) reduces the likelihood of failure of these systemically important banks.

G-SIB buffer requirements range from 1% to 3.5% (1%, 1.5%, 2%, 2.5% and 3.5%). The G-SIB list was first published in 2011. There were 29 institutions on the G-SIB list in 2018. Since 2011, no bank has been in the 3.5% category and only HSBC and JPMorgan Chase have been in the 2.5% category. A leverage ratio buffer was introduced for G-SIBs in 2017 (equal to one-half of the bank's risk-based G-SIB buffer, not including the CCB or countercyclical buffer [CCyB]). In 2018, the United States proposed the G-SIB leverage buffer be half the sum of the CCB and G-SIB risk-based buffer requirements.

The Basel Committee and Financial Stability Board also established proposals for G-SIBs regarding the total loss-absorbing capacity (TLAC). In default, TLAC instruments (e.g., equity, subordinated debt) can be used to absorb loss and, in turn, protect depositors and enable the bank to recapitalize itself. Recapitalization might partially be accomplished by converting certain debt into equity. These contingent convertible bonds, known as CoCos, are discussed in LO 56.g.

While left to the discretion of individual country supervisors, Basel III also recommends that banks have a capital buffer to protect against the cyclicity of bank earnings, called the **countercyclical buffer (CCyB)**. The countercyclical buffer can range from 0% to 2.5% of RWAs. Like the capital conservation buffer, it must be met with Tier 1 equity capital. The buffer will be phased in between January 1, 2016, and January 1, 2019.

For countries that require the countercyclical buffer, dividend restrictions may apply. The CCyB is complicated for international banks because the requirement may differ across countries. The CCyB is a weighted average of the requirements of each nation in which the bank operates.

Rationales for imposing the CCyB include:

- **Overheating.** Higher capital requirements restrict the credit supply to banks and thus restrict the potential for overheated credit markets. If the credit cycle is dampened, the frequency and severity of financial crises may also be reduced.
- **Cost-of-capital rationale.** This rationale assumes that it is easier and less costly to raise capital in good times than in bad. This implies that financial stability can be achieved at a lower cost by increasing (decreasing) the CCyB in good (bad) times.



PROFESSOR'S NOTE

While the buffer requires the ratios to be 7% (Tier 1 equity), 8.5% (total Tier 1 capital), and 10.5% (total capital) of risk-weighted assets, the ratios are expected to decline in times of market stress due to losses. At that point, the ratio requirements described in LO 56.d are applied (i.e., 4.5%, 6.0%, and 8.0%, respectively). However, once financial markets stabilize, banks will face pressure to increase the ratios again. Given the higher equity requirements under Basel III, it will likely be difficult for banks to achieve the high returns on equity (ROE) that they enjoyed in the 15 years leading up to the financial crisis (i.e., 1990–2006).

Liquidity Risk Management

LO 56.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.

During the 2007–2009 financial crisis, solvent banks failed because depositors and counterparties withdrew funds faster than banks could sell assets. A financial crisis failure that resulted from a bank run was Northern Rock. The bank relied on securitizations to fund its mortgage lending business. When securitizations became difficult, wholesale funding dried up. The Bank of England announced it would provide liquidity support to banks. The news of government intervention caused depositors to withdraw substantial funds from Northern Rock, and, simultaneously, wholesale funding fell further and the bank ultimately failed. The crisis made clear that it was not just default that could cause bank failures, but liquidity risk as well. As such, one of the primary goals of Basel III was to improve liquidity risk management in financial institutions.

Basel III specifies a minimum **leverage ratio** (capital / total exposure) of 3%. Total exposure includes all items on the balance sheet, in their entirety (i.e., not risk-weighted). It also includes some off-balance sheet items such as loan commitments.

Banks often finance long-term obligations with short-term funds such as commercial paper or repurchase agreements. This is fine during normal economic periods. However, in times of financial stress, this mismatched financing gives rise to liquidity risk. Banks find it difficult to roll over the short-term financing when they have, or are perceived to have, financial problems. During the 2007–2009 financial crisis, liquidity risk, not a lack of capital, was the real problem for many banks (e.g., Lehman Brothers). Basel III requires banks to meet the following two liquidity ratios: (1) liquidity coverage ratio and (2) net stable funding ratio.

Liquidity coverage ratio (LCR): The LCR focuses on the bank's ability to weather a 30-day period of reduced/disrupted liquidity. The severe stress considered could be a three-notch downgrade (e.g., AA to A), a loss of deposits, a complete loss of wholesale funding, a devaluation of the value of collateral for funding agreements like repurchase agreements (i.e., increased "haircuts"), and potential drawdowns on lines of credit. The point is that banks and authorities should be able to sell liquid assets to meet liquidity

demands during the month of disrupted liquidity, while simultaneously attempting to restore confidence in itself.

The LCR ratio is computed as:

$$\text{high-quality liquid assets} / \text{net cash outflows in a 30-day period} \geq 100\%$$

Liquid assets need to be at least as great as potential net cash outflows such that the bank can withstand one or more of the pressures described earlier. Examples of high-quality liquid assets (HQLA) include deposits at central banks and securities issued by central governments with a zero percent risk weight under the standardized approach. These assets are HQLA without haircuts. Corporate debt and equity have a 50% haircut. For example, a bank with \$100 million of corporate debt could count \$50 million in its HQLA calculation. Individual mortgage loans are excluded entirely.

As different liabilities will likely be withdrawn at different speeds, banks must make assumptions as it categorizes liabilities. For example, a bank may assume a 3% run-off rate for insured retail deposits. In contrast, the likely withdrawal rate of nonoperational wholesale funding will be much higher, such as a 100% run-off rate. And this is but a fraction of what must be categorized and modeled. This means that while the LCR definition is simple, its implementation is not.

Net stable funding ratio (NSFR): The NSFR focuses on the bank's ability to manage liquidity over a period of one year. The ratio is computed as:

$$\text{amount of available stable funding} / \text{amount of required stable funding} \geq 100\%$$

To calculate the numerator, each source of funding (such as retail deposits, repurchase agreements, capital, and so on) is multiplied by a factor that reflects the relative stability of the funding source. See Figure 56.2 for the **available stable funding (ASF)** factors and types of funding available. These ASF factors are similar to haircuts, as described above. The higher the factor, the more illiquid, meaning it is funding that is less likely to leave the bank (e.g., equity is considered a permanent source of funding which cannot be withdrawn in a crisis while wholesale funding is more likely to be withdrawn).

Figure 56.2: ASF Factors in NSFR

ASF Factor	Category
100%	Tier 1 and Tier 2 capital, preferred stock, debt with remaining maturity greater than one year.
95%	"Stable" demand and term deposits from individuals and small businesses with maturities less than one year.
90%	"Less stable" demand and term deposits from individuals and small businesses with maturities less than one year.
50%	Wholesale funding (demand and term deposits) from nonfinancial corporations, sovereigns, central banks, multilateral development banks, and public sector entities with maturities less than one year.
0%	All other liability and equity categories.

To calculate the denominator, each required amount of stable funding is multiplied by a factor that reflects the relative permanence of the funding required. See Figure 56.3 for

the **required stable funding (RSF)** factors and the types of assets requiring the funding.

Figure 56.3: RSF Factors in NSFR

RSF Factor	Category
0%	Cash and short-term instruments, securities, and loans to financial entities with residual maturities of less than one year.
5%	Marketable securities with maturities of greater than one year, if claim is on a sovereign with 0% risk weight (e.g., U.S. Treasury securities).
15%	Corporate bonds with rating of AA- or higher and residual maturity greater than one year. Claims on sovereigns or similar bodies with risk weight of 20%.
50%	Loans to financial institutions with remaining maturities less than one year, bonds rated A+ to BBB-.
65%	Residential mortgages.
85%	Loans to small businesses or retail customers with remaining maturities less than one year and risk weights over 35%, gold, and equities.
100%	All other assets.

EXAMPLE: Calculating the NSFR

Bank of the Bluegrass has the following balance sheet:

Cash (coins and banknotes)	10	Retail deposits (less stable)	100
Central bank reserves	10	Wholesale deposits (20% mature in one month)	75
Treasury bonds (> 1 yr)	10	Tier 2 capital	2
Mortgages	30	Tier 1 capital	18
Retail loans (< 1 yr)	30		
Small business loans (< 1 yr)	90		
Fixed assets	15		
Total assets	195	Total liabilities and equity	195

1. Use the balance sheet to **calculate** the liquidity coverage ratio. Assume HQLA factors (i.e., haircuts) are 100% for cash, central bank reserves and Treasury bonds (meaning no haircut), and 0% for all loans and fixed assets (meaning they do not count at all in HQLA, there is a 100% haircut and a 0% factor). Assume also a 5% run-off rate for less stable retail deposits and a 100% run-off rate of wholesale deposits that mature in the next 30 days. Assume a 0% run-off of Tier 2 and Tier 1 capital.
2. Using the information in Figure 56.2 and Figure 56.3 to find the corresponding ASF and RSF factors, **calculate** the bank's net stable funding ratio.

Answer:

1. $HQLA = 1.0 \times (30) + (0.0 \times 165) = 30$ Net cash outflow in a 30-day period = $(100 \times 0.05) + (75 \times 0.2) + (20 \times 0.0) = 20$ $LCR = 30 / 20 = 1.50 = 150\%$
2. $ASF = (100 \times 0.9) + (75 \times 0.5) + (2 \times 1.0) + (18 \times 1.0) = \147.50 $RSF = (10 \times 0) + (10 \times 0) + (10 \times 0.05) + (30 \times 0.65) + (30 \times 0.85) + (90 \times 0.85) + (15 \times 1.0) = \137.00 $NSFR = 147.50 / 137.00 = 1.0766 = 107.66\%$

With both the LCR and NSFR greater than 100%, Bank of the Bluegrass satisfies the new liquidity requirements.

These new rules represent a significant change for banks and will impact bank balance sheets.



PROFESSOR'S NOTE

Because banks are large and complex organizations, the number of factors, and categories and haircuts associated with liquidity measures is vast. We have included a few examples in Figure 56.2 and Figure 56.3. However, you will likely be given that information in a problem asking you to calculate the LCR or NSFR on the exam. Focus on what you are trying to understand about the bank from these ratios (i.e., can the bank weather 30-day liquidity stresses and manage liquidity over a one-year horizon). Know how to apply data given to you (e.g., ASF and RSF factors, haircut percentages, and the balance sheet) rather than trying to memorize the factors themselves.



MODULE QUIZ 56.2

1. Under Basel III, capital must be adjusted downward to reflect which of the following?
 - A. Planned bonuses for managers.
 - B. Deficits in defined benefit pension plans.
 - C. Corporate convertible debt.
 - D. There is no requirement under Basel III to adjust capital downward for anything.
2. The capital conservation buffer:
 - A. is intended to protect banks from the countercyclical nature of bank earnings.
 - B. can be set between 0.0% and 2.5% of risk-weighted assets, and is at the discretion of the regulators in individual countries.
 - C. causes the Tier 1 equity capital ratio requirement to increase to 7% of risk-weighted assets in normal economic periods.
 - D. requires that total capital to risk-weighted assets must be 10.5% at all times.
3. Highlands Bank has estimated stable funding in the bank to be \$100 million. The bank estimates that net cash outflows over the coming 30 days will be \$137 million. The bank has capital of \$5 million and a total exposure of \$140 million. The bank estimates that it has high-quality liquid assets of \$125 million. What is the bank's liquidity coverage ratio (LCR)?
 - A. 89.3%.
 - B. 91.2%.
 - C. 73.0%.
 - D. 3.6%.

MODULE 56.3: CONTINGENT CONVERTIBLE BONDS AND DODD-FRANK REFORM

Contingent Convertible Bonds

LO 56.g: Describe the mechanics of contingent convertible bonds (CoCos) and explain the motivations for banks to issue them.

Traditional convertible bonds converted to equity at the option of the bondholder. The bondholder would convert when the firm's stock price exceeded thresholds specified in the indenture. **Contingent convertible bonds (CoCos)**, unlike traditional convertible bonds, convert to equity automatically when certain conditions are met. These bonds typically convert to equity when the company or bank is experiencing financial strains.

The motivation for banks to issue CoCos is that during normal financial periods, the bonds are debt and thus do not drag down return on equity (ROE). However, in periods of financial stress, the bonds convert to equity, providing a cushion against loss, which helps prevent insolvency. The needed capital is provided by private sector bondholders rather than the government, allowing the bank to avoid a bailout.

Potential triggers that activate conversion are:

- The ratio of Tier 1 equity capital to risk-weighted assets. For example, Credit Suisse issued CoCos in 2011. Conversion is triggered if Tier 1 equity capital to risk-weighted assets falls below a threshold.
- Supervisors' judgment about the issuing bank's solvency prospects. For example, the Credit Suisse CoCos automatically convert if bank supervisors determine that the bank needs public sector aid (i.e., equity capital) to avoid insolvency.
- A minimum ratio of a bank's market capitalization to its assets. Market value triggers may reduce balance sheet manipulations (as one might see if the ratio of capital to risk-weighted assets is used as a trigger) but might instead introduce stock price manipulation.

Reforms After the Global Financial Crisis

LO 56.h: Provide examples of legislative and regulatory reforms that were introduced after the 2007–2009 financial crisis.

Many legislative and regulatory reforms have been introduced since the 2007–2009 financial crisis. They include:

- The establishment of the **Financial Stability Oversight Council (FSOC)**. The job of the FSOC is to look out for risks that affect the entire financial system. The body monitors systemic risks.
- The FSOC and the Office of Financial Research (OFR) are charged with identifying systemically important financial institutions (SIFIs). G-SIBs are one type of SIFIs. SIFIs must establish living wills that map out how the firm can be safely wound down in the event of failure. SIFIs may also be required to hold additional capital.
- Changes in compensation. Precrisis, executive pay at large banks was effectively independent of risk taking. Compensation was one factor blamed for imprudent risk taking. Postcrisis, compensation packages that encourage short-term performance

goals that may lead to increased risk taking are discouraged. Shareholders were given a nonbinding vote on executive compensation packages. Board compensation committees must be made up of independent directors.

- Increased regulation and improved transparency of over-the-counter (OTC) derivatives including requiring standardized OTC derivatives between financial institutions be cleared by exchanges or **central counterparties (CCPs)**. To facilitate OTC trading, **swap execution facilities (SEFs)** were mandated (electronic platforms that promote price transparency).
- The requirement that rating agencies be more transparent in their assumptions and methods used to rate firms. An **Office of Credit Ratings** was created to monitor rating agencies. The potential legal liabilities of rating agencies were also increased under Dodd-Frank.
- Individual protections were increased, both for investors and consumers. The **Consumer Financial Protection Bureau** was created within the Federal Reserve to ensure that consumers understand loan applications and terms for things like mortgages and credit cards. The goal is that consumers receive clear and accurate information when they shop for financial products and services. It is also meant to curb abuses by financial firms.
- Banks are required to assess a mortgage borrower's ability to repay. Foreclosures may be disallowed if a bank does not make a good faith effort to determine that the borrower can repay the loan.
- At least one board member should have risk management experience at large, complex organizations.
- Firms are required, with some exceptions, to keep a minimum of 5% of the assets they securitize.
- The establishment of the **Volcker Rule**, part of the **Dodd-Frank Act**, intended to curtail proprietary trading by institutions (like banks) that accept insured deposits as a source of funding. One of the problems with this rule is that it can be difficult to distinguish between a bank's speculative trading and hedging activities.



PROFESSOR'S NOTE

These and other changes, such as the establishment of the *Office of Financial Research (OFR)* and the expansion of the FDIC's power to liquidate banks, were part of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank). It was signed into law in July 2010. The act is intended to protect consumers from abuses and prevent future bailouts and/or collapses of banks and other financial firms. Starting in mid-2018, some Dodd-Frank provisions have been rolled back.



MODULE QUIZ 56.3

1. Which of the following statements is correct regarding the mechanics and motivations of contingent convertible bonds (CoCos)?
 - I. During normal financial periods, CoCos are debt and do not drag down return on equity.
 - II. During periods of financial stress, CoCos convert to equity, providing a cushion against loss, which helps prevent insolvency.
- A. Statement I only.

- B. Statement II only.
- C. Both statements I and II.
- D. Neither statement I nor II.

KEY CONCEPTS

LO 56.a

Basel 2.5 requires banks to calculate two market risk VaRs. The first is the usual VaR required in Basel II, using the historical simulation method. The second is a stressed VaR, using a 250-day period of stressed market conditions. To calculate the stressed VaR, banks must identify a one-year period out of the previous seven years when their portfolios performed poorly. The total market risk capital charge is the sum of the usual bank VaR and the stressed VaR.

LO 56.b

The Basel Committee proposed an incremental default risk charge (IDRC) in 2005 to correct for the fact that the banking book was attracting more capital than the trading book in most banks. For instruments in the trading book that are sensitive to default risk, the IDRC requires the bank to calculate a 99.9% confidence level, one-year time horizon VaR. This was altered to account for ratings change sensitivities in addition to default sensitivities following the 2007–2009 financial crisis and became known as the incremental risk capital charge. Banks must estimate a liquidity horizon for each instrument and rebalance the portfolio if credit quality declines.

LO 56.c

The comprehensive risk (CR) capital charge accounts for risks in the correlation book. Asset-backed securities (ABS) and collateralized debt obligations (CDOs) are sensitive to the default risk of other assets. For example, they are sensitive to the default risk of the securitized assets that collateralize the instruments. The committee has specified a standardized approach to assign capital charges for rated instruments.

Resecuritizations, such as CDOs of ABSs, have higher risk weights than normal securitizations, such as mortgage-backed securities. For unrated instruments or instruments rated below BB–, the bank must carry dollar-for-dollar capital to back the position, equivalent to a 100% capital charge.

LO 56.d

Basel III increased capital requirements for credit risk and tightened the definition of what qualifies as Tier 1 and Tier 2 capital. Basel III eliminated Tier 3 capital. Under Basel III, a bank's total capital consists of Tier 1 equity capital (primarily common stock plus retained earnings), additional Tier 1 capital (primarily noncumulative perpetual preferred), and Tier 2 capital (primarily debt subordinated to depositors with an original maturity of at least five years). Core Tier 1 equity capital must be at least 4.5% of risk-weighted assets, total Tier 1 capital must be 6% of risk-weighted assets, and total capital (Tier 1 plus Tier 2) must be at least 8% of risk-weighted assets (left unchanged from Basel II).

LO 56.e

The capital conservation buffer protects banks in times of financial distress. Banks are required to build up a buffer of Tier 1 equity capital equal to 2.5% of risk-weighted

assets in normal times, which will then be used to cover losses in stress periods. This means that in normal times, a bank should have a minimum 7% Tier 1 equity capital ratio. Total Tier 1 capital must be 8.5% of risk-weighted assets and Tier 1 plus Tier 2 capital must be 10.5% of risk-weighted assets in normal periods. Dividend restrictions apply when capital ratios fall below required levels.

Basel III also recommends that banks have a capital buffer to protect against the cyclical nature of bank earnings, called the countercyclical buffer. This requirement is left to the discretion of individual country supervisors and can range from 0% to 2.5% of risk-weighted assets.

LO 56.f

One of the primary goals of Basel III is to improve liquidity risk management in financial institutions. Basel III requires banks to meet the following three liquidity ratios:

1. A minimum leverage ratio (capital / total exposure) of 3%. Total exposure includes all items on the balance sheet in their entirety (i.e., not risk-weighted) and some off-balance sheet items, such as loan commitments.
2. A minimum liquidity coverage ratio (high-quality liquid assets / net cash outflows in a 30-day period) of 100%. The LCR focuses on the bank's ability to weather a 30-day period of reduced/disrupted liquidity.
3. A minimum net stable funding ratio (amount of stable funding / required amount of stable funding) of 100%. The NSFR focuses on the bank's ability to manage liquidity over a period of one year.

LO 56.g

Contingent convertible bonds (CoCos) convert to equity automatically when certain conditions are met, usually when the company or bank is experiencing financial stresses. The motivation for banks to issue CoCos is that during normal financial periods, the bonds are debt and thus do not weigh down return on equity (ROE). However, in periods of financial stress, the bonds convert to equity, providing a cushion against loss and preventing insolvency and potentially allowing the bank to avoid a bailout.

LO 56.h

A vast array of regulatory and legislative changes occurred across the globe in the decade following the 2007–2009 financial crisis. The Dodd-Frank Act was signed into law in July 2010 in the United States. The act is intended to protect consumers from abuses and prevent future bailouts and/or collapses of banks and other financial firms. Some of the more important changes that have been implemented include:

- The establishment of the Financial Stability Oversight Council (FSOC). The job of the FSOC is to look out for risks that affect the entire financial system.
- The FSOC and the Office of Financial Research (OFR) are charged with identifying systemically important financial institutions (SIFIs). SIFIs must establish living wills that map out how the firm can be safely wound down in the event of failure. SIFIs may also be required to hold additional capital.
- The establishment of the Volcker Rule, intended to curtail proprietary trading by banks.

- The Consumer Financial Protection Bureau (CFPB) was created to ensure that consumers understand loan applications and terms for things like mortgages and credit cards. With the CFPB, consumers receive clear and accurate information when they shop for financial products and services in order to curb financial abuses by financial firms.
- Increased regulation and improved transparency for over-the-counter (OTC) derivatives including requiring standardized OTC derivatives be cleared by exchanges or by central counterparties (CCPs).
- Compensation packages have changed since the financial crisis. Before the financial crisis, executive pay at large banks was effectively independent of risk taking. Compensation was one factor blamed for imprudent risk taking. Compensation packages that encourage short-term performance goals that may lead to increased risk taking are now discouraged.

ANSWER KEY FOR MODULE QUIZZES

Module Quiz 56.1

1. **C** Basel 2.5 required banks to calculate two VaRs, the usual VaR, using the historical simulation method, and a stressed VaR, using a 99% confidence level, 250-day period of stressed market conditions. The total market risk capital charge is the sum of the usual bank VaR and the stressed VaR. Initially, regulators thought the year 2008 would be ideal for stressed market conditions. However, banks are now required to identify a one-year period when their portfolios performed poorly. This means the stressed period may be different across banks. (LO 56.a)
2. **A** As part of the incremental risk charge (IRC) calculation, banks are required to estimate a liquidity horizon for each instrument in the portfolio. For example, assume an AA+-rated bond in the portfolio has a liquidity horizon of three months. If, at the end of three months, the bond has defaulted or has been downgraded, it is assumed that the bank will replace the bond with an AA+-rated bond comparable to the one held at the start of the period. This rebalancing is assumed at the end of each three-month period (or six months, nine months, etc., depending on the estimated liquidity horizon). Rebalancing allows banks to take losses as instruments are downgraded but generally allows the bank to avoid defaults. (LO 56.b)

Module Quiz 56.2

1. **B** Capital is adjusted downward to reflect:
 - defined benefit pension plan deficits (but is not adjusted upward for surpluses).
 - certain cross-holdings within a group.
 - mortgage servicing rights greater than 10% of common equity. (LO 56.d)
2. **C** The capital conservation buffer is meant to protect banks in times of financial distress. Banks are required to build up a buffer of Tier 1 equity capital equal to 2.5% of risk-weighted assets in normal times, which will then be used to cover losses in stress periods. This means that in normal times, a bank should have a

minimum 7% Tier 1 equity capital to risk-weighted assets ratio, an 8.5% total Tier 1 capital to risk-weighted assets ratio, and a 10.5% Tier 1 plus Tier 2 capital to risk-weighted assets ratio. The capital conservation buffer is a requirement and is not left to the discretion of individual country regulators. It is not a requirement at all times but is built up to that level in normal economic periods and declines in stress periods. (LO 56.e)

3. **B** Basel III requires a minimum liquidity coverage ratio of 100%. The LCR focuses on the bank's ability to weather a 30-day period of reduced/disrupted liquidity. The formula is computed as follows:

high-quality liquid assets / net cash outflows in a 30-day period

$$\text{LCR} = \$125 \text{ million} / \$137 \text{ million} = 0.912 \text{ or } 91.2\%$$

In this case, Highlands Bank does not meet the minimum 100% requirement and is in violation of the rule. (LO 56.f)

Module Quiz 56.3

1. **C** Contingent convertible bonds (CoCos), unlike traditional convertible bonds, convert to equity when the company or bank is experiencing financial strains. During normal financial periods, the bonds are debt and thus do not drag down return on equity (ROE). (LO 56.g)

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 assigned reading—Basel Committee on Banking Supervision.

READING 57

HIGH-LEVEL SUMMARY OF BASEL III REFORMS

Study Session 9

EXAM FOCUS

This is a brief summary of reforms to the revised Basel III framework that were announced in December 2017. The reforms deal primarily with credit risk and, to a lesser extent, operational risk. For the exam, do not get bogged down in the details of the regulatory rules. Instead, focus on the big picture: a summary view of the reforms, the motivation for those reforms, and the intended result of implementing those reforms.

MODULE 57.1: HIGH-LEVEL SUMMARY OF BASEL III REFORMS

LO 57.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.

The financial crisis of 2007–2009 led to Basel III revisions that will be implemented beginning in 2022. The regulatory framework in place during the crisis failed to prevent the systemic shocks that severely weakened the global banking system and the global economy. The Basel III revisions and the December 2017 reforms (which are summarized in this reading) are designed to address those shortcomings.

The goals and impacts of the December 2017 Basel III reforms include the following:

- Expanding the robustness and sensitivity of the standardized approaches (SA) for measuring credit risk, credit valuation adjustment (CVA) risk, and operational risk. These are discussed in LO 57.b.
- Restricting the use of internal model approaches for credit risk, CVA risk, and operational risk. This is discussed in LO 57.b.
- Introducing a leverage ratio buffer for global systemically important banks (G-SIBs). This is discussed in LO 57.b.

- Creating an output floor that is more robust and risk-sensitive than the current Basel II floor. This is discussed in LO 57.c.
-

LO 57.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**
-

Standardized Approach (SA) for Credit Risk

Basel III reforms enhanced the standardized approach (SA) by doing the following:

- Increasing the granularity of risk-weight definitions, and hence, improving the risk sensitivity of the measures. For example, under all Basel II, the same risk weight was applied to all residential mortgages; under Basel III reforms, the risk weight of a residential mortgage depends on the loan-to-value ratio. More granular treatments were also developed for rated and unrated exposures to banks and corporates, as well as residential and commercial real estate, retail exposures, subordinated debt and equity, and off-balance sheet items.
- Reducing the reliance on external credit ratings as an assessment of credit risk.
- Providing the foundation for the revised output floor discussed in LO 57.c.

Internal Ratings-Based (IRB) Approaches for Credit Risk

The internal ratings-based (IRB) approaches for credit risk proved problematic in application during the financial crisis as a result of their complexity, lack of comparability across banks, and lack of robust modeling of some asset classes.

The advanced IRB (A-IRB) approach allowed banks in certain cases to estimate the probability of default (PD), loss given default (LGD), exposure at default (EAD), and exposure maturity. The foundation IRB (F-IRB) approach requires fixed values for LGD and EAD—the two parameters that contributed the most to risk-weighted asset variability.

As a result, Basel III reforms:

- took away the A-IRB approach for exposures to large and mid-size corporates, as well as banks and other financial institutions, and required the use of the F-IRB approach in those cases;
- required input floors for PD, LGD, and EAD to force more conservative estimates of credit risk; and
- provided more specific requirements for how banks estimate model parameters.

Credit Valuation Adjustment (CVA) Risk Framework

CVA risk results from the counterparty risk inherent in derivatives contracts. It was a significant contributor to bank losses during the financial crisis. The Basel III reforms:

- enhance the risk sensitivity by incorporating the market-risk exposure component of CVA and its associated hedge instruments;
- remove the option to use the IRB approach to CVA risk, and require the use of a standardized approach (SA) or a basic approach; and
- improve consistency with the revised market-risk framework by basing the CVA framework on fair value sensitivities to market-risk factors.

Operational Risk Framework

The operational risk framework in place during the financial crisis included an advanced measurement approach (AMA) and three SAs. Despite this complexity, the framework was insufficient in two important ways: capital requirements were insufficient to cover bank losses from operational risk factors, and the type of risk factors that led to these losses (e.g., misconduct and inadequate systems and controls) were not captured adequately in the internal models.

As a result, the operational risk framework has been simplified by allowing only one SA for all banks. Operational risk capital requirements are determined by measures of the bank's:

- income, which is assumed to be positively correlated to future operational risk; and
- historical operational risk losses, which are also assumed to be positively correlated to future operational risk.

Leverage Ratio Framework

The Basel III reforms revise the leverage ratio framework by:

- adding a leverage ratio buffer for G-SIBs that must be met with Tier 1 capital; and
- refining the leverage ratio exposure measure to better reflect the exposure from derivatives and off-balance sheet items.

LO 57.c: Describe the revised output floor introduced as part of the Basel III reforms and approaches to be used when calculating the output floor.

The idea of an *output floor* is to restrict the ability of large banks to gain an advantage by significantly reducing their capital requirements by using internal approaches instead of SA. In effect, it sets a minimum capital requirement for internal approaches relative to SA.

Specifically, risk-weighted assets are calculated as the higher of (1) total risk-weighted assets calculated from the approach the bank has regulatory approval to use (including both standardized and internal approaches), and (2) 72.5% of total risk-weighted assets using the SA.

Standardized approaches to be used when calculating the floor are based on the type of risk exposure:

- The SA for **credit risk**, as discussed in LO 57.b.
- The SA for measuring **counterparty credit risk (SA-CCR)** is used for derivatives. The SA for credit risk is then applied to the counterparty.
- For **credit valuation adjustment (CVA) risk**, the standardized approach (SA-CVA) or the basic approach (BA-CVA), both of which are discussed in LO 57.b, or 100% of the bank's counterparty credit risk capital requirement.
- For **securitization risk**, the choices are the external ratings-based approach (SEC-ERBA), the standardized approach (SEC-SA), or a 1,250% risk weight.
- For **market risk**, the SA is permitted.
- For **operational risk**, the SA is permitted.



MODULE QUIZ 57.1

1. The Basel III reforms restricted the use of internal model approaches for all of the following risk categories except:
 - A. credit risk.
 - B. systemic risk.
 - C. operational risk.
 - D. credit valuation risk.
2. The Basel III reforms introduced a leverage buffer ratio for all:
 - A. global banks.
 - B. unregulated global banks.
 - C. global systemically important banks.
 - D. banks regulated by the U.S. Federal Reserve and the European Banking Authority.
3. The advanced internal ratings-based (A-IRB) approach for credit risk will no longer be permissible to use under the Basel III reforms for each of the following except:
 - A. large corporate exposures.
 - B. mid-size corporate exposures.
 - C. banks and other financial institutions.
 - D. residential and commercial real estate.
4. The new operational risk capital requirements under the Basel III reforms are determined by measures of the bank's:
 - A. leverage and income.
 - B. income and historical operational risk losses.
 - C. income and expected operational risk losses.
 - D. leverage and expected operational risk losses.
5. The output floor sets the minimum level of:
 - A. leverage.
 - B. functional capital.
 - C. credit valuation adjustment (CVA) risk exposure.
 - D. risk-weighted assets.
6. Under Basel III reforms, the approaches that can be used when calculating the output floor for CVA risk include all of the following except:
 - A. the basic (BA-CVA) approach.
 - B. the standardized (SA-CVA) approach.
 - C. the internal ratings-based (IRB-CVA) approach.

D. 100% of the bank's counterparty credit risk capital requirement.

KEY CONCEPTS

LO 57.a

The goals and impacts of the December 2017 Basel III reforms include:

- expanding the robustness and sensitivity of the standardized approaches (SA) for measuring credit risk, credit valuation adjustment (CVA) risk, and operational risk;
- restricting the use of internal model approaches for credit risk, CVA risk, and operational risk;
- introducing a leverage ratio buffer for global systemically important banks (G-SIBs); and
- creating an output floor that is more robust and risk-sensitive than the current Basel II floor.

LO 57.b

Basel III reforms:

- enhance the SA for credit risk by increasing the granularity of risk-weight definitions, reducing the reliance on external credit ratings, and providing a foundation for a revised output floor;
- restrict use of the A-IRB approach for credit risk;
- remove the option to use the IRB approach for CVA risk;
- allow only one SA for operational risk; and
- add a leverage ratio buffer for G-SIBs.

LO 57.c

Basel III reforms revise the output floor, which restricts the ability of large banks to gain an advantage by significantly reducing their capital requirements by using internal approaches instead of standardized approaches (SA).

Risk-weighted assets are calculated as the higher of (1) total risk-weighted assets calculated from the approach the bank has regulatory approval to use (including both standardized and internal approaches), and (2) 72.5% of total risk-weighted assets using the SA.

ANSWER KEY FOR MODULE QUIZ

Module Quiz 57.1

1. **B** The use of internal model approaches are restricted for credit risk, operational risk, and credit valuation risk. (LO 57.b)
2. **C** The Basel III reforms revise the leverage ratio framework by adding a leverage ratio buffer for G-SIBs that must be met with Tier 1 capital. (LO 57.b)
3. **D** The Basel III reform took away the A-IRB approach for exposures to large and mid-size corporates, as well as banks and other financial institutions, and required

the use of the foundation IRB (F-IRB) approach in those cases. (LO 57.b)

4. **B** Operational risk capital requirements are determined by measures of the bank's income and historical operational risk losses, both of which are assumed to be positively correlated to future operational risk. (LO 57.b)
5. **D** The output floor sets a minimum level of risk-weighted assets. (LO 57.c)
6. **C** IRB approaches cannot be used for calculating the output floor for CVA risk. (LO 57.c)

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 assigned reading—Basel Committee on Banking Supervision.

READING 58

BASEL III: FINALIZING POST-CRISIS REFORMS

Study Session 9

EXAM FOCUS

The focus of this reading is on the calculation of the standardized approach for measuring operational risk capital requirements. In particular, candidates should understand how the business indicator (BI) is derived, and how buckets are used to group banks by size such that the BI will have a different impact on the standardized approach given a bank's bucket. Candidates should also know how to calculate the internal loss multiplier and the loss component, and understand how this component impacts the standardized approach given a bank's bucket classification. The standardized approach has evolved over time from earlier approaches that were more model-based and allowed for too much flexibility. Finally, candidates should also be familiar with the Basel Committee's outline of general and specific criteria applicable to operational loss data.

MODULE 58.1: BASEL III: FINALIZING POST-CRISIS REFORMS

The Standardized Approach

LO 58.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.

The **standardized approach** for measuring operational risk represents a combination of (1) a financial statement operational risk exposure proxy (termed the business indicator, or BI), (2) the business indicator component (BIC), which is the product of a regulatory marginal coefficient and BI, and (3) operational loss data specific to an individual bank, reflected in the internal loss multiplier (ILM).

The Business Indicator

The **business indicator (BI)** is calculated as the most recent three-year average for each of the following three components:

$$BI = ILDC_{avg} + SC_{avg} + FC_{avg}$$

where:

ILDC = interest, lease, dividend component

SC = services component

FC = financial component

The three individual components are calculated as follows, using three years of average data:

interest, lease, dividend component (ILDC) =

$$\min[\text{abs}(II_{avg} - IE_{avg}); 0.0225 \times IEA_{avg}] + DI_{avg}$$

where:

abs = absolute value

II = interest income

IE = interest expenses

IEA = interest earning assets

DI = dividend income

Services component (SC) =

$$\max(OOI_{avg}; OOE_{avg}) + \max(FI_{avg}; FE_{avg})$$

where:

OOI = other operating income

OOE = other operating expenses

FI = fee income

FE = fee expenses

Financial component (FC) =

$$\text{abs}(\text{net P\<B}_{avg}) + \text{abs}(\text{net P\&LBB}_{avg})$$

where:

P&L = profit & loss statement line item

TB = trading book

BB = banking book

For the purposes of calculating the standardized approach, banks (based on their size for the BI component) are divided into three buckets as shown in Figure 58.1.

Figure 58.1: BI Buckets

Bucket	BI Range	BIC
1	€0 billion – €1 billion	$0.12 \times BI$
2	€1 billion – €30 billion	$0.15 \times BI$
3	€30 billion – $+\infty$	$0.18 \times BI$

For example, if BI is equal to €40 billion, the BIC would be computed as:

$$(0.12 \times 1) + [0.15 \times (30 - 1)] + [0.18 \times (40 - 30)] = 0.12 + 4.35 + 1.8 \\ = \text{€6.27 billion}$$

Internal Loss Multiplier

Through the addition of a loss component, the standardized approach becomes more sensitive to risk than it would be with just the BI component alone. Internal losses are factored into the standardized approach calculation via the **internal loss multiplier (ILM)**, which is calculated as follows:

$$\text{internal loss multiplier} = \ln \left[e^1 - 1 + \left(\frac{\text{loss component}}{\text{BIC}} \right)^{0.8} \right]$$

where:

loss component = 15 × average annual operational risk loss over the last 10 years

The **loss component** serves to reflect the operational loss exposure based on a bank's internal loss experiences. A bank whose exposure is considered average relative to its industry will have a loss component equivalent to its BI component; this implies an internal loss multiplier equal to 1 and the standardized approach capital is equal to its BI component. If a bank's loss experience is greater (less) than the industry average, its loss component will be above (below) the BI component and its standardized approach capital will be above (below) the BI component.

Ideally, a bank will have 10 years of quality data to calculate the averages that go into the loss component calculation. If 10 years are not available, then during the transition to the standardized approach calculation, banks may use 5 years and add more years as time progresses until they reach the 10-year requirement. If a bank does not have 5 years of data, then the BI component becomes the only component of the standardized approach calculation.

Standardized Approach Capital Requirement

The standardized approach is used to determine the operational risk capital requirement and is calculated as follows:

For BI bucket 1 banks:

operational risk capital = BIC

For BI bucket 2 and 3 banks:

operational risk capital = BIC × ILM

The amounts used in the BIC, which are bucket-dependent, will follow the equations shown in the BIC column of Figure 58.1. The internal loss multiplier is calculated per the previous section.

For banks that are part of a consolidated entity, the standardized approach calculations will incorporate fully consolidated BI amounts (netting all intragroup income and expenses). At a subconsolidated level, the standardized approach uses BI amounts for the banks that are consolidated at that particular level. At the subsidiary level, the standardized approach calculations will use the BI amounts from the specific subsidiary. If the BI amounts for a subsidiary or subconsolidated level reach the bucket 2 level, the banks must incorporate their own loss experiences (not those of other members of the group). If a subsidiary of a bank in buckets 2 and 3 does not meet the qualitative standards associated with using the loss component, the standardized approach capital requirement is calculated using 100% of the BI component.

EXAMPLE: Computing the standardized approach capital requirement

PS Bank, Inc., has a BI of €18.48 million for the current fiscal year. **Calculate** PS Bank's operational risk capital requirement with the standardized approach.

Answer:

PS Bank is a bucket 1 bank because its BI falls within a range of €0 billion to €1 billion. For bucket 1 banks, the only component of the standardized approach calculation is the BI component and the calculation is $0.12 \times €18.48 \text{ million}$, or €2.22 million.

The Standardized Approach vs. Earlier Approaches

LO 58.b: Compare the Standardized Measurement Approach (SMA) to earlier methods of calculating operational risk capital, including the Advanced Measurement Approaches (AMA).

Before the development of the standardized approach, some banks were using the advanced measurement approach (AMA) to assess operational risk. The AMA, which was introduced as part of the Basel II framework in 2006, allowed for the estimation of regulatory capital based on a range of internal modeling practices. This approach was a principles-based framework allowing for significant flexibility. Although the hope of the Basel II Committee was for best practices to emerge as flexibility declined, this never happened and challenges associated with comparability among banks (due to a wide range of modeling practices) and overly complex calculations remained.

Given the challenges previously noted, the Basel Committee set a goal of creating a new measure to allow for greater comparability and less complexity relative to prior methods. The standardized approach was created as this measure, with the intent of providing a means of assessing operational risk that would include both a standardized measure of operational risk and bank-specific loss data. Unlike AMA, the standardized approach is a single, non-model-based method used to estimate operational risk capital that combines financial statement information with the internal loss experience of the specific bank.

Identification, Collection, and Treatment of Operational Loss Data

LO 58.c: Describe general and specific criteria recommended by the Basel Committee for the identification, collection and treatment of operational loss data.

Banks that incorporate the loss component into the standardized approach calculation must follow the following general criteria:

- Documented processes and procedures must be in place for the identification, collection, and treatment of internal loss data.
- A bank must maintain information on each operational risk event, including gross loss amounts, the date of occurrence (when the event first began or happened), the date of discovery (when the bank became aware of the event), the date of accounting (when the reserve, loss, or loss provision was first recognized in the bank's income statement, any gross loss amount recoveries, and what the drivers were of the loss event itself).
- Loss data accuracy must be comprehensive and reviewed independently.
- For the purposes of calculating minimum regulatory capital per the standardized approach framework, operational risk losses tied to credit risk-weighted assets will be excluded from the calculation. Operational risk losses tied to market risk will be included in the standardized approach calculation.
- A bank has to be able to document any criteria used to allocate losses to specific event types. In addition, a bank must be able to categorize historical internal loss data into the appropriate Level 1 supervisory categories per the Basel II Accord (Annex 9) and be prepared to provide this to supervisors when requested.
- An observation period of 10 years must be used as a basis for internally generated loss data calculations. On an exception basis and as long as good-quality data is not available for more than a five-year period, a bank first moving to the standardized approach can use a five-year observation period.
- Internal loss data must be comprehensive in nature and capture all material exposures and activities across all geographic locations and subsystems. When a bank first moves to the standardized approach, a €20,000 gross loss threshold is acceptable. Afterward, this threshold may be increased to €100,000 for banks in buckets 2 and 3.

In addition to the general criteria noted earlier, specific criteria must also be followed as described as follows:

- A policy must exist for each bank that sets the criteria for when an operational risk event or loss (which is recorded in the internal loss event database) is included in the loss data set for calculating the standardized approach regulatory capital amount (i.e., the standardized approach loss data set).
- For all operational loss events, banks must be able to specifically identify gross loss amounts, insurance recoveries, and noninsurance recoveries. A gross loss is a loss before any recoveries, while a net loss takes into account the impact of recoveries. The standardized approach loss data should include losses net of insurance recoveries.
- In calculating the gross loss for the standardized approach loss data set, the following components must be *included*:
 - External expenses (legal fees, advisor fees, vendor costs, etc.) directly tied to the operational risk event itself and any repair/replacement costs needed to restore the bank to the position it was in before the event occurring.
 - Settlements, impairments, write-downs, and any other direct charges to the bank's income statement as a result of the operational risk event.

- Any reserves or provisions tied to the potential operational loss impact and booked to the income statement.
- Losses (tied to operational risk events) that are definitive in terms of financial impact but remain as pending losses because they are in transition or suspense accounts not reflected on the income statement. Materiality will dictate whether the loss is included in the data set.
- Timing losses booked in the current financial accounting period that are material in nature and are due to events that give rise to legal risk and cross more than one financial accounting period.
- In calculating the gross loss for the standardized approach loss data set, the following components must be *excluded*:
 - The total costs of improvements, upgrades, and risk assessment enhancements and initiatives that are incurred after the risk event occurs.
 - Insurance premiums.
 - The costs associated with general maintenance contracts on property, plant, and equipment (PP&E).
- The only date a bank can use to build its standardized approach loss data set is the date of accounting. For any legal loss events, the date of accounting (which is when the legal reserve representing the probable estimated loss) is the latest date that can be used for the loss data set.
- Any losses related to a common operational risk event or are related by operational risk events over time, but posted to accounts over many years, should be allocated to the given year of the loss.



MODULE QUIZ 58.1

1. The business indicator (BI) component in the standardized approach calculation for a bank with a BI of €13 billion will be closest to:
 - A. €1.43 billion.
 - B. €1.92 billion.
 - C. €2.43 billion.
 - D. €13.00 billion.
2. Which of the following items from the profit & loss (P&L) statement should be included in the BI component calculation?
 - A. Administrative expenses.
 - B. Insurance premiums paid.
 - C. Depreciation related to capitalized equipment.
 - D. Provision reversals related to operational loss events.
3. Which of the following components within the BI calculation takes into account a bank's trading and banking book P&L results?
 - A. Loss component.
 - B. Services component.
 - C. Financial component.
 - D. Interest, lease, dividend component.
4. Which of the following statements best describe a difference between the standardized approach and older operational risk capital approaches?

- A. The advanced measurement approach (AMA) was introduced as part of the Basel III revisions.
 - B. The AMA was more flexible in its application than the standardized approach.
 - C. The standardized approach accounts for internal loss experiences that were not factored into the AMA.
 - D. The standardized approach uses a model-based methodology, while the AMA was more flexible and principle-based.
5. In deriving the standardized approach loss data set for an individual bank, each of the following items will most likely be included in the gross loss calculation except:
- A. legal fees of €900,000 associated with an unusual risk event.
 - B. a €2 million settlement tied to a recent operational risk event.
 - C. a €1.4 million reserve booked to the income statement to cover a potential operational loss.
 - D. €1.75 million spent on maintenance contracts tied to the bank's property, plant, and equipment.

KEY CONCEPTS

LO 58.a

The standardized approach includes both a business indicator (BI) component accounting for operational risk exposure and an internal loss multiplier accounting for operational losses unique to an individual bank. While the BI component is factored into the standardized approach for banks of all sizes, the impact it has on the standardized approach operational risk capital calculation will vary depending on where the bank is classified from buckets 1–3.

LO 58.b

The older advanced measurement approach (AMA) allowed banks to use a vast range of models that were inherently more flexible for individual banks, but prevented valuable comparisons among banks. For this reason, the standardized approach was created as a non-model-based approach used to assess operational risk using both financial statement measures and loss data unique to individual banks.

LO 58.c

For identifying, collecting, and accounting for operational loss data, the Basel Committee has outlined several general and specific criteria that should be used. Key general criteria include processes and procedures, documentation needed, thresholds for capturing losses, and appropriate periods. Specific criteria include how to calculate gross losses (what is included versus what is excluded) and key dates used to capture the losses.

ANSWER KEY FOR MODULE QUIZ

Module Quiz 58.1

1. **B** A bank with a BI of €13 million will fall into bucket 2, which covers a BI range of €1 billion to €30 billion. With the BI component formula of $0.15 \times \text{BI}$ for bucket 2

banks, the BI component for this bank will be equal to $0.12 \times 1 + 0.15 \times (13 - 1) = \text{€}1.92 \text{ billion}$. (LO 58.a)

2. **D** A provision reversal would normally be excluded except when it relates to operational loss events. Each of the other three choices represents a P&L item that should be excluded from the BI component calculation. (LO 58.c)
3. **C** The formula for the financial component of the BI calculation is equal to $\text{abs}(\text{net P\<B}_{\text{avg}}) + \text{abs}(\text{net P\&LBB}_{\text{avg}})$, with TB representing the trading book and BB representing the banking book. (LO 58.a)
4. **B** Because banks were able to use a wide range of models for calculating the AMA, there was more flexibility to these approaches than under the newer standardized approach. The AMA was introduced as part of the Basel II framework in 2006. AMA did account for internal losses. The standardized approach is nonmodel based, whereas the AMA did incorporate bank-specific models. (LO 58.b)
5. **D** The costs associated with maintenance contracts for PP&E are outlined in the specific criteria for collecting operational loss data as *excluded* for the purposes of calculating the gross loss for the SMA loss data set. (LO 58.c)

FORMULAS

Reading 52

economic capital = risk capital + strategic risk capital

risk-adjusted return on capital (RAROC):

$$\text{RAROC} = \frac{\text{after-tax expected risk-adjusted net income}}{\text{economic capital}}$$

$$\text{RAROC} = \frac{\left(\begin{array}{l} \text{expected revenues} - \text{costs} - \text{expected losses} \\ - \text{taxes} + \text{return on economic capital} \pm \text{transfers} \end{array} \right)}{\text{economic capital}}$$

hurdle rate:

$$h_{AT} = \frac{[(CE \times R_{CE}) + (PE \times R_{PE})]}{(CE + PE)}$$

where:

CE = market value of common equity

PE = market value of preferred equity

R_{CE} = cost of common equity (could be derived from the capital asset pricing model [CAPM])

R_{PE} = cost of preferred equity (yield on preferred shares)

$$\text{Adjusted RAROC} = \text{RAROC} - \beta_E (R_M - R_F)$$

where:

R_F = risk-free rate = hurdle rate

R_M = expected return on market portfolio

β_E = firm's equity beta

$(R_M - R_F)$ = excess return over risk-free rate to account for the nondiversifiable systematic risk of the project

Reading 55

market risk capital requirement:

$$\max(\text{VaR}_{t-1}, m \times \text{VaR}_{\text{avg}})$$

where:

VaR_{t-1} = previous day's VaR

VaR_{avg} = the average VaR over the past 60 trading days

m = multiplicative factor

$$\text{total capital} = 0.08 \times (\text{credit risk RWA} + \text{market risk RWA} + \text{operational risk RWA})$$

expected loss:

$$EL = \sum_i \text{EAD}_i \times \text{LGD}_i \times \text{PD}_i$$

$$\text{capital} = \text{EAD} \times \text{LGD} \times (\text{DR99.9} - \text{PD}) \times \text{MA}$$

where:

$$\text{MA} = \text{maturity adjustment} = [1 + (M - 2.5) \times b] / (1 - 1.5 \times b)$$

M = maturity of the exposure

$$b = [0.11852 - 0.05478 \times \ln(\text{PD})]^2$$

Reading 56

stressed VaR:

$$\max(\text{VaR}_{t-1}, m_r \times \text{VaR}_{\text{avg}}) + \max(\text{SVaR}_{t-1}, m_s \times \text{SVaR}_{\text{avg}})$$

where:

VaR_{t-1} = previous day's VaR, 10-day time horizon, 99% confidence level

VaR_{avg} = the average VaR over the past 60 days, 10-day time horizon, 99% confidence level

m_r = multiplicative factor, determined by supervisor, minimum value of three

SVaR_{t-1} = previous day's stressed VaR, 10-day time horizon, 99% confidence level

SVaR_{avg} = the average stressed VaR over the past 60 days, 10-day time horizon, 99% confidence level

m_s = stressed VaR multiplicative factor, determined by supervisor, minimum of three

liquidity coverage ratio:

high-quality liquid assets / net cash outflows in a 30-day period $\geq 100\%$

net stable funding ratio:

amount of available stable funding / amount of required stable funding $\geq 100\%$

Reading 58

business indicator:

$$\text{BI} = \text{ILDC}_{\text{avg}} + \text{SC}_{\text{avg}} + \text{FC}_{\text{avg}}$$

where:

ILDC = interest, lease, dividend component

SC = services component

FC = financial component

internal loss multiplier:

$$\text{internal loss multiplier} = \ln \left[e^1 - 1 + \left(\frac{\text{loss component}}{\text{BIC}} \right)^{0.8} \right]$$

where:

loss component = $15 \times$ average annual operational risk loss over the last 10 years

INDEX

5-whys analysis, 61

A

action plan, 96

add-on amount, 281

adjusted RAROC, 232

advanced IRB approach, 294

advanced measurement approach, 296

anti-money laundering (AML), 162

Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT), 149

audit committee, 92

available stable funding (ASF), 315

B

backtesting, 200, 287

bank holding companies, 263

Basel I, 278

Basel II, 288

Basel III, 310

Basel taxonomy, 39

basic indicator approach, 296

behavioral controls, 142

benchmarking, 199

boundary events, 54

bow tie diagram, 61

Bureau of Financial Protection, 319

burned-out capital, 227

business continuity management (BCM), 81

business disruption and system failures (BDSF), 3, 41

business impact analysis, 81

business indicator (BI), 336

business indicator component (BIC), 15

business line managers, 92

C

- calibration test, 297
- capital adequacy process, 264
- capital assessment risk aggregation, 111
- capital conservation buffer, 312
- Capital One, 184
- Capital Plan Rule, 263
- causal analysis, 59
- central counterparties (CCPs), 319
- challenger banks, 164
- clients, products, and business practices (CPBP), 3, 41
- coherence, 213
- coherent risk measure, 243
- collective controls, 76
- combined assurance, 99
- compliance risk, 171
- compliance risk management, 190
- comprehensive approach, 291
- Comprehensive Capital Analysis and Review (CCAR), 114, 214
- comprehensive risk (CR) charge, 308
- concentration risk, 171
- Consumer Financial Protection Bureau (CFPB), 190, 319
- contingent convertible bonds (CoCos), 318
- contract provisions, 173
- conversion factor, 280
- Cooke ratio, 110, 279
- copula correlation, 292
- core capital, 279, 311
- corporate operational risk function (CORF), 20, 92
- corrective controls, 47, 75
- countercyclical buffer, 313
- counterparty credit risk, 251
- country risk, 172
- credit equivalent amount, 280, 281
- current exposure method, 281
- customer due diligence (CDD), 150
- customer identification, 152
- customer verification, 152
- cyber-governance, 122
- cyber-resilience, 122
- cyber risk, 140

cybersecurity, 122

D

damage to physical assets (DPA), 3, 42
detective controls, 47, 75, 142
directive controls, 47, 75
disaster recovery plan (DRP), 81
distributed denial of service (DDOS), 126
Dodd-Frank Act, 190, 320
due diligence, 172

E

economic capital, 110, 223, 226
employment practices and workplace safety (EPWS), 3, 42
enterprise risk management (ERM) framework, 107
Equifax, 142
examination, 77
exception, 287
execution, delivery, and process management (EDPM), 3, 40
executive committee (ExCo), 92
expected losses, 226
expected revenues, 226
expected shortfall, 244
exposure at default, 293
exposures, 33
external audits, 151
external fraud (EF), 3, 42, 162
external loss, 34
external operational risk, 73
extreme value theory (EVT), 64

F

factor analysis of information risk (FAIR), 60
fault tree analysis (FTA), 59
financial crime, 161
Financial Stability Oversight Council (FSOC), 319

financing of terrorism, 149
first line of defense, 21, 108
foundation IRB approach, 294
frequency distribution, 63

G

Gaussian copula function, 207
global systemically important banks (G-SIBs), 312
goodwill, 227
governance, risk, and compliance (GRC) systems, 97

H

heatmap, 57, 94
horizon scanning, 96
hurdle rate, 231

I

immeasurable risks, 113
impact scales, 56
incident dates, 53
incident response and recovery, 126
incremental default risk charge (IDRC), 308
incremental risk charge (IRC), 308
information controls, 142
information security risk, 139
intentional actions, 139
internal audits, 151
inter-risk diversification, 111
internal fraud (IF), 2, 42, 162
internal loss, 34
internal loss multiplier (ILM), 15, 337
internal model-based approach (market risk), 285
internal models approach (Solvency II), 297
internal operational risk, 74
internal ratings-based approach (IRB), 292
intra-risk diversification, 111

K

key control indicators (KCI), 58
key performance indicators (KPI), 58
key risk indicators (KRI), 58, 95
knowledge-based mistakes, 78
know your customer (KYC), 164

L

Lean techniques, 78
legal risk, 3, 172
leverage ratio, 314
likelihood assessment scales, 56
liquidity coverage ratio, 314
lookbacks, 165
loss component, 337
loss distribution approach (LDA), 62, 115
loss given default, 293

M

macroeconomic (macro) stress testing, 113
marginal capital, 234
market risk, 285
Market Risk Amendment, 283
Markets in Financial Instruments Directive (MiFID), 190
Markets in Financial Instruments Regulation (MiFIR), 190
mark-to-market, 285
maturity adjustment, 294
measurable risks, 113
mergers and acquisitions (M&A), 80
MiFID II, 190
mistakes, 78
mitigating controls, 142
model risk, 195, 206
model risk management (MRM), 206

models, 205
money laundering (ML), 149, 162
monotonicity, 243
Morgan Stanley, 184

N

NASA Mars Orbiter, 208
near misses, 34, 96
net present value, 226
net replacement ratio (NRR), 284
net stable funding ratio, 315
netting, 283
New Initiative Risk Assessment Process (NIRAP), 79
New Product Approval Process (NPAP), 79
NIST CSF, 140

O

observation, 77
Office of Credit Ratings, 319
operational resilience, 6, 66
operational risk, 1, 39, 172
operational risk capital requirements, 295
Operational Riskdata eXchange (ORX) taxonomy, 42
operational risk events, 40
operational risk management (ORM) report, 94
optimistic controls, 76
original exposure method, 281, 283
outcomes analysis, 200

P

parameter (model) stress testing, 113
Pillar 1, 13, 110, 288
Pillar 2, 14, 110, 288
Pillar 3, 14, 100, 110, 289
point-in-time, 230
politically exposed persons (PEPs), 164

positive homogeneity, 244
predictable risk, 33
prevention through design (PtD), 77
preventive controls, 47, 75, 142
probability of default, 292
process mapping, 35

Q

qualitative risk data, 99
quality improvement, 78

R

regulation technology (RegTech), 164
regulatory capital, 109, 224
reperformance, 77
reporting cake, 93
reputational risk, 3, 171
required stable funding (RSF), 315
resecuritizations, 308
residual risk self-assessment (RRSA), 55
reverse stress testing, 113
risk-adjusted return on capital (RAROC), 110, 225
risk aggregation, 245
risk and control assessment (RCA), 55
risk and control self-assessment (RCSA), 34, 55, 94
risk appetite, 23, 109
risk appetite metrics, 95
risk assessments, 2, 172
risk capital, 223
risk committee, 17, 92
risk culture, 24, 108
risk event reports, 96
risk governance, 108
risk identification, 2
risk mitigation, 2, 73
risk monitoring, 2
risk specialists, 21
risk-weighted assets, 215, 279

risk wheel, 33
root-cause analysis, 60
rule-based mistakes, 78

S

sanctions lists, 164
second line of defense, 21, 108
self-assessment, 77
sensitivity analysis, 198
severity distribution, 63
Sharpe ratio, 226
simple approach, 291
Six Sigma, 78
slips, 78
smurfing, 163
solvency capital requirement (SCR), 297
Solvency II, 297
specific risk charge (SRC), 286, 308
spoofing, 191
stand-alone capital, 234
standard deviation, 244
standardized approach (credit risk), 290
standardized approach (operational risk), 296, 335
standardized approach (SA), 15
standardized approach (Solvency II), 297
standardized measurement method (market risk), 285
statistical quality test, 297
strategic risk, 3
strategic risk capital, 227
stressed value at risk (VaR), 306
stress testing, 112, 211
subadditivity, 243
Supervisory Capital Assessment Program, 212
supplementary capital, 279, 311
suspicious transaction reports, 151
swap execution facilities, 319
Swiss cheese model, 60
systems security, 162

T

- terrorism financing (TF), 162
- technical controls, 142
- theft and fraud, 162
- three lines of defense model, 20
- third line of defense, 22, 108
- third-party risk management (TPRM), 181
- through-the-cycle, 230
- Tier 1 capital, 279, 311
- Tier 2 capital, 279, 311
- Tier 3 capital, 286
- translation invariance, 244

U

- unauthorized activities, 162
- underwriting risk, 297
- unexpected losses, 227
- unintentional actions, 139
- unpredictable risk, 33
- USAA Federal Savings Bank (USAA FSB), 164
- use test, 297

V

- value at risk (VaR), 244
- Volcker Rule, 190, 320
- vulnerabilities, 33

W

- worst case probability of default, 292

Required Disclaimers:

CFA Institute does not endorse, promote, or warrant the accuracy or quality of the products or services offered by Kaplan. CFA Institute, CFA[®], and Chartered Financial Analyst[®] are trademarks owned by CFA Institute.

Certified Financial Planner Board of Standards Inc. owns the certification marks CFP[®], CERTIFIED FINANCIAL PLANNER[™], and federally registered CFP (with flame design) in the U.S., which it awards to individuals who successfully complete initial and ongoing certification requirements. The College for Financial Planning[®], a Kaplan company, does not certify individuals to use the CFP[®], CERTIFIED FINANCIAL PLANNER[™], and CFP (with flame design) certification marks. CFP[®] certification is granted only by Certified Financial Planner Board of Standards Inc. to those persons who, in addition to completing an educational requirement such as this CFP[®] Board-Registered Program, have met its ethics, experience, and examination requirements.

The College for Financial Planning[®], a Kaplan company, is a review course provider for the CFP[®] Certification Examination administered by Certified Financial Planner Board of Standards Inc. CFP Board does not endorse any review course or receive financial remuneration from review course providers.

GARP[®] does not endorse, promote, review, or warrant the accuracy of the products or services offered by Kaplan 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, nor is GARP[®] responsible for any fees or costs of any person or entity providing any services to Kaplan. FRM[®], GARP[®], and Global Association of Risk Professionals[™] are trademarks owned by the Global Association of Risk Professionals, Inc.

CAIAA does not endorse, promote, review or warrant the accuracy of the products or services offered by Kaplan, nor does it endorse any pass rates claimed by the provider. CAIAA is not responsible for any fees or costs paid by the user to Kaplan nor is CAIAA responsible for any fees or costs of any person or entity providing any services to Kaplan. CAIA[®], CAIA Association[®], Chartered Alternative Investment AnalystSM, and Chartered Alternative Investment Analyst Association[®] are service marks and trademarks owned by CHARTERED ALTERNATIVE INVESTMENT ANALYST ASSOCIATION, INC., a Massachusetts non-profit corporation with its principal place of business at Amherst, Massachusetts, and are used by permission.