2017 SchweserNotes™ Part II

FRM®

Exam Prep

Operational and Integrated Risk Management

eBook 3

KAPLAN UNIVERSITY SCHOOL OF PROFESSIONAL AND CONTINUING EDUCATION | SCHWESER

Getting Started

Part II FRM® Exam

Welcome

As the Vice President of Product Management at Kaplan Schweser, I am pleased to have the opportunity to help you prepare for the 2017 FRM® Exam. Getting an early start on your study program is important for you to sufficiently **Prepare ▸ Practice ▸ Perform®** on exam day. Proper planning will allow you to set aside enough time to master the learning objectives in the Part II curriculum.

Now that you've received your SchweserNotes™, here's how to get started:

Step 1: Access Your Online Tools

Visit **www.schweser.com/frm** and log in to your online account using the button located in the top navigation bar. After logging in, select the appropriate part and proceed to the dashboard where you can access your online products.

Step 2: Create a Study Plan

Create a study plan with the **Schweser Study Calendar** (located on the Schweser dashboard). Then view the **Candidate Resource Library** on-demand videos for an introduction to core concepts.

Step 3: Prepare and Practice

Read your SchweserNotes™

Our clear, concise study notes will help you **prepare** for the exam. At the end of each reading, you can answer the Concept Checker questions for better understanding of the curriculum.

Attend a Weekly Class

Attend our **Live Online Weekly Class** or review the on-demand archives as often as you like. Our expert faculty will guide you through the FRM curriculum with a structured approach to help you **prepare** for the exam. (See our instruction packages to the right. Visit **www.schweser.com/frm** to order.)

Practice with SchweserPro™ QBank

Maximize your retention of important concepts and **practice** answering exam-style questions in the **SchweserPro™ QBank** and taking several **Practice Exams**. Use **Schweser's QuickSheet** for continuous review on the go. (Visit **www.schweser.com/frm** to order.)

Step 4: Final Review

A few weeks before the exam, make use of our **Online Review Workshop Package**. Review key curriculum concepts in every topic, **perform** by working through demonstration problems, and **practice** your exam techniques with our 8-hour live **Online Review Workshop**. Use **Schweser's Secret Sauce®** for convenient study on the go.

Step 5: Perform

As part of our **Online Review Workshop Package**, take a **Schweser Mock Exam** to ensure you are ready to **perform** on the actual FRM Exam. Put your skills and knowledge to the test and gain confidence before the exam.

Again, thank you for trusting Kaplan Schweser with your FRM Exam preparation!

Sincerely,

Derek Burkett

Derek Burkett, CFA, FRM, CAIA
VP, Product Management, Kaplan Schweser

The Kaplan Way for Learning

FRM® Instruction Packages:

- **PremiumPlus™ Package**
- **Premium Instruction Package**

Live Instruction*:

Remember to join our Live Online Weekly Class. Register online today at **www.schweser.com/frm.**

May Exam Instructor
Dr. John Broussard
CFA, FRM

November Exam Instructor
Dr. Greg Filbeck
CFA, FRM, CAIA

*Dates, times, and instructors subject to change

Contact us for questions about your study package, upgrading your package, purchasing additional study materials, or for additional information:

www.schweser.com/frm | Toll-Free: 888.325.5072 | International: +1 608.779.8397

FRM Part II Book 3: Operational and Integrated Risk Management

FRM 2017 PART II BOOK 3: OPERATIONAL AND INTEGRATED RISK MANAGEMENT

Printed in the United States of America.

ISBN: 978-1-4754-5355-3

Reading Assignments and Learning Objectives

The following material is a review of the Operational and Integrated Risk Management principles designed to address the learning objectives set forth by the Global Association of Risk Professionals.

Reading Assignments

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

48. "Model Risk," Chapter 15 (page 116)

49. "Risk Capital Attribution and Risk-Adjusted Performance Measurement," Chapter 17 (page 128)

50. "Range of Practices and Issues in Economic Capital Frameworks," (Basel Committee on Banking Supervision Publication, March 2009). (page 146)

51. "Capital Planning at Large Bank Holding Companies: Supervisory Expectations and Range of Current Practice," Board of Governors of the Federal Reserve System, August 2013. (page 162)

Bruce Tuckman, Angel Serrat, *Fixed Income Securities: Tools for Today's Markets, 3rd Edition* (Hoboken, NJ: John Wiley & Sons, 2011)

52. "Repurchase Agreements and Financing," Chapter 12 (page 176)

Kevin Dowd, *Measuring Market Risk, 2nd Edition* (West Sussex, England: John Wiley & Sons, 2005).

53. "Estimating Liquidity Risks," Chapter 14 (page 190)

Allan Malz, *Financial Risk Management: Models, History, and Institutions* (Hoboken, NJ: John Wiley & Sons, 2011).

54. "Assessing the Quality of Risk Measures," Chapter 11 (page 204)

55. "Liquidity and Leverage," Chapter 12 (page 215)

56. Darrell Duffie, 2010. "The Failure Mechanics of Dealer Banks," *Journal of Economic Perspectives* 24:1, 51–72. (page 236)

57. Til Schuermann, "Stress Testing Banks," prepared for the Committee on Capital Market Regulation, Wharton Financial Institutions Center (April 2012). (page 247)

58: "Guidance on Managing Outsourcing Risk," Board of Governors of the Federal Reserve System, December 2013. (page 258)

John Hull, *Risk Management and Financial Institutions, 4th Edition* (Hoboken, NJ: John Wiley & Sons, 2015).

59. "Basel I, Basel II, and Solvency II," Chapter 15 (page 266)

60. "Basel II.5, Basel III, and Other Post-Crisis Changes," Chapter 16 (page 289)

61. "Fundamental Review of the Trading Book," Chapter 17 (page 306)

Learning Objectives

38. Principles for the Sound Management of Operational Risk

After completing this reading, you should be able to:

1. Describe the three "lines of defense" in the Basel model for operational risk governance. (page 1)
2. Summarize the fundamental principles of operational risk management as suggested by the Basel committee. (page 2)
3. Explain guidelines for strong governance of operational risk, and evaluate the role of the board of directors and senior management in implementing an effective operational risk framework. (page 3)
4. Describe tools and processes that can be used to identify and assess operational risk. (page 7)
5. Describe features of an effective control environment and identify specific controls that should be in place to address operational risk. (page 7)
6. Explain the Basel Committee's suggestions for managing technology risk and outsourcing risk. (page 8)

39. Enterprise Risk Management: Theory and Practice

After completing this reading, you should be able to:

1. Define enterprise risk management (ERM) and explain how implementing ERM practices and policies can create shareholder value, both at the macro and the micro level. (page 15)
2. Explain how a company can determine its optimal amount of risk through the use of credit rating targets. (page 17)
3. Describe the development and implementation of an ERM system, as well as challenges to the implementation of an ERM system. (page 17)
4. Describe the role of and issues with correlation in risk aggregation, and describe typical properties of a firm's market risk, credit risk, and operational risk distributions. (page 18)
5. Distinguish between regulatory and economic capital, and explain the use of economic capital in the corporate decision making process. (page 19)

40. Observations on Developments in Risk Appetite Frameworks and IT Infrastructure

After completing this reading, you should be able to:

1. Describe the concept of a risk appetite framework (RAF), identify the elements of an RAF, and explain the benefits to a firm of having a well-developed RAF. (page 25)
2. Describe best practices for a firm's Chief Risk Officer (CRO), Chief Executive Officer (CEO), and Board of Directors in the development and implementation of an effective RAF. (page 26)
3. Explain the role of an RAF in managing the risk of individual business lines within a firm. (page 27)
4. Describe the classes of risk metrics to be communicated to managers within the firm. (page 28)
5. Explain the benefits to a firm from having a robust risk data infrastructure, and describe key elements of an effective IT risk management policy at a firm. (page 28)
6. Describe factors that could lead to poor or fragmented IT infrastructure at an organization. (page 29)
7. Explain the challenges and best practices related to data aggregation at an organization. (page 30)

41. Information Risk and Data Quality Management

After completing this reading, you should be able to:

1. Identify the most common issues that result in data errors. (page 36)
2. Explain how a firm can set expectations for its data quality and describe some key dimensions of data quality used in this process. (page 36)
3. Describe the operational data governance process, including the use of scorecards in managing information risk. (page 38)

42. OpRisk Data and Governance

After completing this reading, you should be able to:

1. Describe the seven Basel II event risk categories and identify examples of operational risk events in each category. (page 43)
2. Summarize the process of collecting and reporting internal operational loss data, including the selection of thresholds, the timeframe for recoveries, and reporting expected operational losses. (page 46)
3. Explain the use of a Risk Control Self-Assessment (RCSA) and key risk indicators (KRIs) in identifying, controlling, and assessing operational risk exposures. (page 48)
4. Describe and assess the use of scenario analysis in managing operational risk, and identify biases and challenges that can arise when using scenario analysis. (page 51)
5. Compare the typical operational risk profiles of firms in different financial sectors. (page 53)
6. Explain the role of operational risk governance and explain how a firm's organizational structure can impact risk governance. (page 56)

43. External Loss Data

After completing this reading, you should be able to:

1. Explain the motivations for using external operational loss data and common sources of external data. (page 61)
2. Explain ways in which data from different external sources may differ. (page 64)
3. Describe the challenges that can arise through the use of external data. (page 65)
4. Describe the Société Générale operational loss event and explain the lessons learned from the event. (page 66)

44. Capital Modeling

After completing this reading, you should be able to:

1. Compare the basic indicator approach, the standardized approach, and the alternative standardized approach for calculating the operational risk capital charge, and calculate the Basel operational risk charge using each approach. (page 73)
2. Describe the modeling requirements for a bank to use the Advanced Measurement Approach (AMA). (page 78)
3. Describe the loss distribution approach to modeling operational risk capital. (page 79)
4. Explain how frequency and severity distributions of operational losses are obtained, including commonly used distributions and suitability guidelines for probability distributions. (page 79)
5. Explain how Monte Carlo simulation can be used to generate additional data points to estimate the 99.9^{th} percentile of an operational loss distribution. (page 81)
6. Explain the use of scenario analysis and the hybrid approach in modeling operational risk capital. (page 81)

45. Standardized Measurement Approach for Operational Risk

After completing this reading, you should be able to:

1. Explain the elements of the proposed Standardized Measurement Approach (SMA), including the business indicator, internal loss multiplier and loss component, and calculate the operational risk capital requirement for a bank using the SMA. (page 86)
2. Compare the SMA to earlier methods of calculating operational risk capital, including the Alternative Measurement Approaches (AMA), and explain the rationale for the proposal to replace them. (page 90)
3. Describe general and specific criteria recommended by the Basel Committee for the identification, collection, and treatment of operational loss data. (page 91)

46. Parametric Approaches (II): Extreme Value

After completing this reading, you should be able to:

1. Explain the importance and challenges of extreme values in risk management. (page 96)
2. Describe extreme value theory (EVT) and its use in risk management. (page 96)
3. Describe the peaks-over-threshold (POT) approach. (page 98)
4. Compare and contrast generalized extreme value and POT. (page 100)
5. Evaluate the tradeoffs involved in setting the threshold level when applying the GP distribution. (page 98)
6. Explain the importance of multivariate EVT for risk management. (page 100)

47. Validating Rating Models

After completing this reading, you should be able to:

1. Explain the process of model validation and describe best practices for the roles of internal organizational units in the validation process. (page 104)
2. Compare qualitative and quantitative processes to validate internal ratings, and describe elements of each process. (page 107)
3. Describe challenges related to data quality and explain steps that can be taken to validate a model's data quality. (page 109)
4. Explain how to validate the calibration and the discriminatory power of a rating model. (page 111)

48. Model Risk

After completing this reading, you should be able to:

1. Identify and explain errors in modeling assumptions that can introduce model risk. (page 116)
2. Explain how model risk can arise in the implementation of a model. (page 118)
3. Explain methods and procedures risk managers can use to mitigate model risk. (page 119)
4. Explain the impact of model risk and poor risk governance in the 2012 London Whale trading loss and the 1998 collapse of Long Term Capital Management. (page 120)

49. Risk Capital Attribution and Risk-Adjusted Performance Measurement

After completing this reading, you should be able to:

1. 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. (page 128)

2. Describe the RAROC (risk-adjusted return on capital) methodology and its use in capital budgeting. (page 130)
3. Compute and interpret the RAROC for a project, loan, or loan portfolio, and use RAROC to compare business unit performance. (page 130)
4. Explain challenges that arise when using RAROC for performance measurement, including choosing a time horizon, measuring default probability, and choosing a confidence level. (page 133)
5. Calculate the hurdle rate and apply this rate in making business decisions using RAROC. (page 135)
6. Compute the adjusted RAROC for a project to determine its viability. (page 136)
7. Explain challenges in modeling diversification benefits, including aggregating a firm's risk capital and allocating economic capital to different business lines. (page 136)
8. Explain best practices in implementing an approach that uses RAROC to allocate economic capital. (page 138)

50. Range of Practices and Issues in Economic Capital Frameworks

After completing this reading, you should be able to:

1. Within the economic capital implementation framework describe the challenges that appear in:
   - Defining risk measures
   - Risk aggregation
   - Validation of models
   - Dependency modeling in credit risk
   - Evaluating counterparty credit risk
   - Assessing interest rate risk in the banking book (page 146)
2. Describe the BIS recommendations that supervisors should consider to make effective use of risk measures not designed for regulatory purposes. (page 156)
3. Describe the constraints imposed and the opportunities offered by economic capital within the following areas:
   - Credit portfolio management
   - Risk based pricing
   - Customer profitability analysis
   - Management incentives (page 157)

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

After completing this reading, you should be able to:

1. 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. (page 162)
2. 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 RWA and balance sheet projections (page 164)

52. Repurchase Agreements and Financing

After completing this reading, you should be able to:

1. Describe the mechanics of repurchase agreements (repos) and calculate the settlement for a repo transaction. (page 176)
2. Explain common motivations for entering into repos, including their use in cash management and liquidity management. (page 177)
3. Explain how counterparty risk and liquidity risk can arise through the use of repo transactions. (page 179)
4. Assess the role of repo transactions in the collapses of Lehman Brothers and Bear Stearns during the (2007–2009) credit crisis. (page 180)
5. Compare the use of general and special collateral in repo transactions. (page 181)
6. Describe the characteristics of special spreads and explain the typical behavior of US Treasury special spreads over an auction cycle. (page 183)
7. Calculate the financing advantage of a bond trading special when used in a repo transaction. (page 184)

53. Estimating Liquidity Risks

After completing this reading, you should be able to:

1. Define liquidity risk and describe factors that influence liquidity, including the bid-ask spread. (page 190)
2. Differentiate between exogenous and endogenous liquidity. (page 191)
3. Describe the challenges of estimating liquidity-adjusted VaR (LVaR). (page 191)
4. Describe and calculate LVaR using the constant spread approach and the exogenous spread approach. (page 192)
5. Describe endogenous price approaches to LVaR, their motivation and limitations, and calculate the elasticity-based liquidity adjustment to VaR. (page 195)
6. Describe liquidity at risk (LaR) and compare it to LVaR and VaR, describe the factors that affect future cash flows, and explain challenges in estimating and modeling LaR. (page 197)
7. Explain the role of liquidity in crisis situations and describe approaches to estimating crisis liquidity risk. (page 198)

54. Assessing the Quality of Risk Measures

After completing this reading, you should be able to:

1. Describe ways that errors can be introduced into models. (page 204)
2. Describe how horizon, computational and modeling decisions can impact VaR estimates. (page 205)
3. Explain how model risk and variability can arise through the implementation of VaR models and the mapping of risk factors to portfolio positions. (page 205)
4. Identify reasons for the failure of the long-equity tranche, short-mezzanine credit trade in 2005 and describe how such modeling errors could have been avoided. (page 207)
5. Explain major defects in model assumptions that led to the underestimation of systematic risk for residential mortgage backed securities (RMBS) during the 2007–2009 financial downturn. (page 209)

55. Liquidity and Leverage

After completing this reading, you should be able to:

1. Differentiate between sources of liquidity risk, including balance sheet/funding liquidity risk, systematic funding liquidity risk, and transactions liquidity risk, and explain how each of these risks can arise for financial institutions. (page 215)

2. Summarize the asset-liability management process at a fractional reserve bank, including the process of liquidity transformation. (page 216)
3. Describe specific liquidity challenges faced by money market mutual funds and by hedge funds, particularly in stress situations. (page 218)
4. Compare transactions used in the collateral market and explain risks that can arise through collateral market transactions. (page 219)
5. Describe the relationship between leverage and a firm's return profile, calculate the leverage ratio, and explain the leverage effect. (page 221)
6. Explain the impact on a firm's leverage and its balance sheet of the following transactions: purchasing long equity positions on margin, entering into short sales, and trading in derivatives (page 223)
7. Explain methods to measure and manage funding liquidity risk and transactions liquidity risk. (page 227)
8. Calculate the expected transactions cost and the spread risk factor for a transaction, and calculate the liquidity adjustment to VaR for a position to be liquidated over a number of trading days. (page 228)
9. Explain interactions between different types of liquidity risk and explain how liquidity risk events can increase systemic risk. (page 215)

56. The Failure Mechanics of Dealer Banks

After completing this reading, you should be able to:

1. Describe the major lines of business in which dealer banks operate and the risk factors they face in each line of business. (page 236)
2. Identify situations that can cause a liquidity crisis at a dealer bank and explain responses that can mitigate these risks. (page 240)
3. Describe policy measures that can alleviate firm-specific and systemic risks related to large dealer banks. (page 243)

57. Stress Testing Banks

After completing this reading, you should be able to:

1. Compare and contrast the features and scope of supervisory stress tests before and after the Supervisory Capital Assessment Program (SCAP). (page 248)
2. Explain challenges in designing stress test scenarios, including the problem of coherence in modeling risk factors. (page 249)
3. Identify and explain challenges in modeling a bank's losses and revenues over a stress test horizon period. (page 250)
4. Explain the challenges in modeling a bank's balance sheet over a stress test horizon period. (page 251)
5. Compare and contrast the 2009 SCAP stress test, the 2011 and 2012 CCAR, and the 2011 EBA Irish and EBA European stress tests in their methodologies and key findings. (page 251)

58. Guidance on Managing Outsourcing Risk

After completing this reading, you should be able to:

1. Explain how risks can arise through outsourcing activities to third-party service providers, and describe elements of an effective program to manage outsourcing risk. (page 258)
2. Explain how financial institutions should perform due diligence on third-party service providers. (page 259)
3. Describe topics and provisions that should be addressed in a contract with a third-party service provider. (page 260)

59. Basel I, Basel II, and Solvency II

After completing this reading, you should be able to:

1. Explain the motivations for introducing the Basel regulations, including key risk exposures addressed, and explain the reasons for revisions to Basel regulations over time. (page 266)
2. Explain the calculation of risk-weighted assets and the capital requirement per the original Basel I guidelines. (page 267)
3. Describe and contrast the major elements—including a description of the risks covered—of the two options available for the calculation of market risk:
   - Standardized Measurement Method
   - Internal Models Approach (page 270)
4. Calculate VaR and the capital charge using the internal models approach, and explain the guidelines for backtesting VaR. (page 271)
5. Describe and contrast the major elements of the three options available for the calculation of credit risk:
   - Standardized Approach
   - Foundation IRB Approach
   - Advanced IRB Approach (page 273)
6. Describe and contrast the major elements of the three options available for the calculation of operational risk: basic indicator approach, standardized approach, and the Advanced Measurement Approach. (page 279)
7. Describe the key elements of the three pillars of Basel II: minimum capital requirements, supervisory review, and market discipline. (page 279)
8. Define in the context of Basel II and calculate where appropriate:
   - Probability of default (PD)
   - Loss given default (LGD)
   - Exposure at default (EAD)
   - Worst-case probability of default (page 273)
9. Differentiate between solvency capital requirements (SCR) and minimum capital requirements (MCR) in the Solvency II framework, and describe the repercussions to an insurance company for breaching the SCR and MCR. (page 281)
10. Compare the standardized approach and the internal models approach for calculating the SCR in Solvency II. (page 281)

60. Basel II.5, Basel III, and Other Post-Crisis Changes

After completing this reading, you should be able to:

1. Describe and calculate the stressed value-at-risk measure introduced in Basel 2.5, and calculate the market risk capital charge. (page 289)
2. Explain the process of calculating the incremental risk capital charge for positions held in a bank's trading book. (page 291)
3. Describe the comprehensive risk measure (CRM) for positions that are sensitive to correlations between default risks. (page 291)
4. Define in the context of Basel III and calculate where appropriate:
   - Tier 1 capital and its components
   - Tier 2 capital and its components (page 293)
   - Required Tier 1 equity capital, total Tier 1 capital, and total capital
5. Describe the motivations for and calculate the capital conservation buffer and the countercyclical buffer introduced in Basel III. (page 294)

6. 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. (page 295)
7. Describe the mechanics of contingent convertible bonds (CoCos) and explain the motivations for banks to issue them. (page 298)
8. Explain the major changes to the U.S. financial market regulations as a result of Dodd-Frank. (page 299)

61. Fundamental Review of the Trading Book

After completing this reading, you should be able to:

1. Describe the proposed changes to the Basel market risk capital calculation and the motivations for these changes, and calculate the market risk capital under this method. (page 306)
2. Compare the various liquidity horizons proposed by the Fundamental Review of the Trading Book (FRTB) for different asset classes and explain how a bank can calculate its expected shortfall using the various horizons. (page 308)
3. Explain proposed modifications to Basel regulations in the following areas:
   - Classification of positions in the trading book compared to the banking book
   - Treatment of credit spread and jump-to-default risk, including the incremental default risk charge (page 310)

The following is a review of the Operational and Integrated Risk Management principles designed to address the learning objectives set forth by GARP®. This topic is also covered in:

Principles for the Sound Management of Operational Risk

Topic 38

Exam Focus

This is a descriptive topic that addresses the principles of sound operational risk management as proposed by the Basel Committee on Banking Supervision. The committee describes a three lines of defense approach, which includes business line management, independent operational risk management, and independent reviews. The committee suggests that a bank should have a corporate operational risk function (CORF) that is commensurate with the size and complexity of the banking organization. For the exam, understand the 11 principles of operational risk management as outlined by the Basel Committee. Know the specific responsibilities of the board of directors and senior managers as they relate to the 11 principles of operational risk management. Be able to explain the critical components of the bank's operational risk management framework documentation, and know the features of an effective control environment. Lastly, understand the committee's recommendations for managing technology and outsourcing risk.

Operational Risk Governance

LO 38.1: Describe the three "lines of defense" in the Basel model for operational risk governance.

The Basel Committee on Banking Supervision defines **operational risk** as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events." The committee states that the definition excludes strategic and reputational risks but includes legal risks. Operational risk is inherent in banking activities. Risks range from those arising from national disasters, such as hurricanes, to the risk of fraud. The committee intends to improve operational risk management throughout the banking system.

Sound operational risk management practices cover governance, the risk management environment, and the role of disclosure. Operational risk management must be fully integrated into the overall risk management processes of the bank.

The three common "lines of defense" employed by firms to control operational risks are:

1. **Business line management.** Business line management is the first line of defense. Banks now, more than ever, have multiple lines of business, all with varying degrees of operational risk. Risks must be identified and managed within the various products, activities, and processes of the bank.

2. An **independent operational risk management function**. This is the second line of defense and is discussed in the next section.

3. **Independent reviews** of operational risks and risk management. The review may be conducted internally with personnel independent of the process under review or externally.

Corporate Operational Risk Function (CORF)

The bank's specific business lines monitor, measure, report, and manage operational and other risks. The corporate operational risk function (CORF), also known as the corporate operational risk management function, is a functionally independent group that complements the business lines' risk management operations. The CORF is responsible for designing, implementing, and maintaining the bank's operational risk framework. Responsibilities of the CORF may include:

- Measurement of operational risks.
- Establishing reporting processes for operational risks.
- Establishing risk committees to measure and monitor operational risks.
- Reporting operational risk issues to the board of directors.

In general, the CORF must assess and challenge each business line's contributions to risk measurement, management, and reporting processes.

Larger, more complex banking institutions will typically have a more formalized approach to the implementation of the lines of defense against operational risks, including the implementation of the CORF. For example, a large bank may have a fully staffed group skilled specifically in operational risk management, while a smaller bank may simply fold operational risk management into the broader risk management function of the bank.

Principles of Operational Risk Management

LO 38.2: Summarize the fundamental principles of operational risk management as suggested by the Basel committee.

Operational risks must be proactively managed by a bank's board of directors and senior managers as well as its business line managers and employees. The 11 fundamental principles of operational risk management suggested by the Basel Committee are:

1. The maintenance of a **strong risk management culture** led by the bank's board of directors and senior managers. This means that both individual and corporate values and attitudes should support the bank's commitment to managing operational risks.

2. The operational risk framework (referred to as the "Framework" in this topic) must be **developed and fully integrated into the overall risk management processes** of the bank.

3. The board should **approve and periodically review** the Framework. The board should also oversee senior management to ensure that appropriate risk management decisions are implemented at all levels of the firm.

4. The board must identify the types and levels of operational risks the bank is willing to assume as well as approve **risk appetite and risk tolerance statements**.

5. Consistent with the bank's risk appetite and risk tolerance, senior management must **develop a well-defined governance structure** within the bank. The structure must be implemented and maintained throughout the bank's various lines of business, its processes, and its systems. The board of directors should approve this governance structure.

6. Senior management must **understand the risks, and the incentives related to those risks, inherent in the bank's business lines and processes**. These operational risks must be identified and assessed by managers.

7. New lines of business, products, processes, and systems should require an **approval process that assesses the potential operational risks**. Senior management must make certain this approval process is in place.

8. A **process for monitoring operational risks and material exposures to losses** should be put in place by senior management and supported by senior management, the board of directors and business line employees.

9. Banks must put strong **internal controls, risk mitigation, and risk transfer strategies** in place to manage operational risks.

10. Banks must have plans in place to survive in the event of a major business disruption. **Business operations must be resilient.**

11. Banks should make **disclosures** that are clear enough that outside stakeholders can assess the bank's approach to operational risk management.

The Role of the Board and Senior Management

LO 38.3: Explain guidelines for strong governance of operational risk, and evaluate the role of the board of directors and senior management in implementing an effective operational risk framework.

The attitudes and expectations of the board of directors and senior management are critical to an effective operational risk management program.

With respect to Principle 1, the board of directors and/or senior management should:

- **Provide a sound foundation for a strong risk management culture** within the bank. A strong risk management culture will generally mitigate the likelihood of damaging operational risk events.

- **Establish a code of conduct (or ethics policy) for all employees** that outlines expectations for ethical behavior. The board of directors should support senior managers in producing a code of conduct. Risk management activities should reinforce the code of conduct. The code should be reflected in training and compensation as well as risk management. There should be a balance between risks and rewards. Compensation should be aligned not just with performance, but also with the bank's risk appetite, strategic direction, financial goals, and overall soundness.
- **Provide risk training** throughout all levels of the bank. Senior management should ensure training reflects the responsibilities of the person being trained.

With respect to Principle 2, the board of directors and/or senior management should:

- **Thoroughly understand both the nature and complexity of the risks** inherent in the products, lines of business, processes, and systems in the bank. Operational risks are inherent in all aspects of the bank.
- Ensure that the **Framework is fully integrated in the bank's overall risk management plan** across all levels of the firm (i.e., business lines, new business lines, products, processes, and/or systems). Risk assessment should be a part of the business strategy of the bank.

With respect to Principle 3, the board of directors and/or senior management should:

- **Establish a culture and processes** that help bank managers and employees understand and manage operational risks. The board must develop comprehensive and dynamic oversight and control mechanisms that are integrated into risk management processes across the bank.
- **Regularly review the Framework.**
- **Provide senior management with guidance** regarding operational risk management and approve policies developed by senior management aimed at managing operational risk.
- Ensure that the Framework is subject to **independent review.**
- **Ensure that management is following best practices** in the field with respect to operational risk identification and management.
- **Establish clear lines of management responsibility** and establish strong internal controls.

With respect to Principle 4, the board of directors and/or senior management should:

- **Consider all relevant risks** when approving the bank's risk appetite and tolerance statements. The board must also consider the bank's strategic direction. The board should approve risk limits and thresholds.
- **Periodically review** the risk appetite and tolerance statements. The review should specifically focus on:
  - Changes in the market and external environment.
  - Changes in business or activity volume.
  - Effectiveness of risk management strategies.
  - The quality of the control environment.
  - The nature of, frequency of, and volume of breaches to risk limits.

With respect to Principle 5, the board of directors and/or senior management should:

- **Establish systems to report and track operational risks** and maintain an effective mechanism for resolving problems. Banks should demonstrate the effective use of the three lines of defense to manage operational risk, as outlined by the Basel Committee.

- Translate the Framework approved by the board into **specific policies and procedures** used to manage risk. Senior managers should clearly assign areas of responsibility and should ensure a proper management oversight system to monitor risks inherent in the business unit.
- Ensure that operational risk managers **communicate clearly** with personnel responsible for market, credit, liquidity, interest rate, and other risks and with those procuring outside services, such as insurance or outsourcing.
- Ensure that CORF managers should have **sufficient stature** in the bank, commensurate with market, credit, liquidity, interest rate, and other risk managers.
- Ensure that the staff is **well trained in operational risk management**. Risk managers should have independent authority relative to the operations they oversee.
- Develop a **governance structure of the bank that is commensurate with the size and complexity** of the firm. Regarding the governance structure, the bank should consider:
  - *Committee structure*: for large, complex banks, a board-created firm level risk committee should oversee all risks. The management-level operational risk committee would report to the enterprise level risk committee.
  - *Committee composition*: committee members should have business experience, financial experience, and independent risk management experience. Independent, non-executive board members may also be included.
  - *Committee operation*: committees should meet frequently enough to be productive and effective. The committee should keep complete records of committee meetings.

With respect to Principle 6, the board of directors and/or senior management should:

- **Consider both internal and external factors** to identify and assess operational risk. Examples of tools that may be used to identify and assess risk are described in LO 38.4.

With respect to Principle 7, the board of directors and/or senior management should:

- **Maintain a rigorous approval process for new products and processes**. The bank should make sure that risk management operations are in place from the inception of new activities because operational risks typically increase when a bank engages in new activities, new product lines, enters unfamiliar markets, implements new business processes, puts into operation new technology, and/or engages in activities that are geographically distant from the main office.
- Thoroughly **review new activities and product lines**, reviewing inherent risks, potential changes in the bank's risk appetite or risk limits, necessary controls required to mitigate risks, residual risks, and the procedures used to monitor and manage operational risks.

With respect to Principle 8, the board of directors and/or senior management should:

- **Continuously improve the operational risk reporting**. Reports should be manageable in scope but comprehensive and accurate in nature.
- Ensure that **operational risk reports are timely**. Banks should have sufficient resources to produce reports during both stressed and normal market conditions. Reports should be provided to the board and senior management.
- Ensure that operational risk reports include:
  - Breaches of the bank's risk appetite and tolerance statement.
  - Breaches of the bank's thresholds and risk limits.
  - Details of recent operational risk events and/or losses.
  - External events that may impact the bank's operational risk capital.
  - Both internal and external factors that may affect operational risk.

With respect to Principle 9, the board of directors and/or senior management should have a sound internal control system as described in LO 38.5 (an effective control environment) and LO 38.6 (managing technology and outsourcing risks).

Banks may need to transfer risk (e.g., via insurance contracts) if it cannot be adequately managed within the bank. However, sound risk management controls must be in place and thus **risk transfer should be seen as a complement to, rather than a replacement for, risk management controls**. New risks, such as counterparty risks, may be introduced when the bank transfers risk. These additional risks must also be identified and managed.

With respect to Principle 10, the board of directors and/or senior management should:

- **Establish continuity plans** to handle unforeseen disruptive events (e.g., disruptions in technology, damaged facilities, pandemic illnesses that affect personnel, and so on). Plans should include impact analysis and plans for recovery. Continuity plans should identify key facilities, people, and processes necessary for the business to operate. The plan must also identify external dependencies such as utilities, vendors, and other third party providers.
- **Periodically review continuity plans**. Personnel must be trained to handle emergencies and, where possible, the bank should perform disaster recovery and continuity tests.

With respect to Principle 11, the board of directors and/or senior management should:

- Write public disclosures such that stakeholders can assess the bank's operational risk management strategies.
- **Write public disclosures that are consistent** with risk management procedures. The disclosure policy should be established by the board of directors and senior management and approved by the board of directors. The bank should also be able to verify disclosures.

Operational Risk Management Framework

The operational risk management framework (i.e., the Framework) must define, describe, and classify operational risk and operational loss exposure. The Framework helps the board and managers understand the nature and complexities of operational risks inherent in the bank's products and services. The components of the Framework should be fully integrated into the bank's overall risk management plan. The Framework must be documented in the board of directors' approved policies.

Framework documentation, which is overseen by the board of directors and senior management, should:

- Describe reporting lines and accountabilities within the governance structure used to manage operational risks.
- Describe risk assessment tools.
- Describe the bank's risk appetite and tolerance.
- Describe risk limits.
- Describe the approved risk mitigation strategies (and instruments).
- With respect to inherent and residual risk exposures, describe the bank's methods for establishing risk limits and monitoring risk limits.
- Establish risk reporting processes and management information systems.
- Establish a common language or taxonomy of operational risk terms to create consistency of risk identification and management.

- Establish a process for independent review of operational risk.
- Require review of established policies and procedures.

Tools for Identifying and Assessing Operational Risk

LO 38.4: Describe tools and processes that can be used to identify and assess operational risk.

Tools that may be used to identify and assess operational risk include:

- **Business process mappings**, which do exactly that, map the bank's business processes. Maps can reveal risks, interdependencies among risks, and weaknesses in risk management systems.
- **Risk and performance indicators** are measures that help managers understand the bank's risk exposure. There are *Key Risk Indicators* (KRIs) and *Key Performance Indicators* (KPIs). KRIs are measures of drivers of risk and exposures to risk. KPIs provide insight into operational processes and weaknesses. Escalation triggers are often paired with KRIs and KPIs to warn when risk is approaching or exceeding risk thresholds.
- **Scenario analysis** is a subjective process where business line managers and risk managers identify potential risk events and then assess potential outcomes of those risks.
- **Measurement** involves the use of outputs of risk assessment tools as inputs for operational risk exposure models. The bank can then use the models to allocate economic capital to various business units based on return and risk.
- **Audit findings** identify weaknesses but may also provide insights into inherent operational risks.
- Analysis of **internal operational loss data**. Analysis can provide insight into the causes of large losses. Data may also reveal if problems are isolated or systemic.
- Analysis of **external operational loss data** including gross loss amounts, dates, amount of recoveries and losses at other firms.
- **Risk assessments**, or *risk self-assessments* (RSAs), address potential threats. Assessments consider the bank's processes and possible defenses relative to the firm's threats and vulnerabilities. *Risk Control Self-Assessments* (RCSA) evaluate risks before risk controls are considered (i.e., inherent risks). Scorecards translate RCSA output into metrics that help the bank better understand the control environment.
- **Comparative analysis** combines all described risk analysis tools into a comprehensive picture of the bank's operational risk profile. For example, the bank might combine audit findings with internal operational loss data to better understand the weaknesses of the operational risk framework.

Features of an Effective Control Environment

LO 38.5: Describe features of an effective control environment and identify specific controls that should be in place to address operational risk.

An effective control environment must include the following five components:

1. A control environment.

2. Risk assessment.

3. Control activities.

4. Information and communication.

5. Monitoring activities.

Senior managers should conduct top-level reviews of progress toward stated risk objectives, verify compliance of standards and controls, review instances of non-compliance, evaluate the approval system to ensure accountability, and track reports of exceptions to risk limits and management overrides and deviations from risk policies and controls. Managers should also ensure that duties are segregated and conflicts of interest are identified and minimized.

Specific controls that should be in place in the organization to address operational risk include:

- Clearly established lines of authority and approval processes for everything from new products to risk limits.
- Careful monitoring of risk thresholds and limits.
- Safeguards to limit access to and protect bank assets and records.
- An appropriately sized staff to manage risks.
- An appropriately trained staff to manage risks.
- A system to monitor returns and identify returns that are out of line with expectations (e.g., a product that is generating high returns but is supposed to be low risk may indicate that the performance is a result of a breach of internal controls).
- Confirmation and reconciliation of bank transactions and accounts.
- A vacation policy that requires officers and employees to be absent for a period not less than two consecutive weeks.

Managing Technology Risk and Outsourcing Risk

LO 38.6: Explain the Basel Committee's suggestions for managing technology risk and outsourcing risk.

Technology can be used to mitigate operational risks. For example, automated procedures are generally less prone to error than manual procedures. However, technology introduces its own risks. The Basel Committee recommends an integrated approach to identifying, measuring, monitoring, and managing technology risks.

Technology risk management tools are similar to those suggested for operational risk management and include:

- Governance and oversight controls.
- Policies and procedures in place to identify and assess technology risks.
- Written risk appetite and tolerance statements.
- Implement a risk control environment.
- Establish risk transfer strategies to mitigate technology risks.
- Monitor technology risks and violations of thresholds and risk limits.
- Create a sound technology infrastructure (i.e., the hardware and software components, data and operating environments).

Outsourcing involves the use of third parties to perform activities or functions for the firm. Outsourcing may reduce costs, provide expertise, expand bank offerings, and/or improve bank services. The board of directors and senior management must understand the operational risks that are introduced as a result of outsourcing. Outsourcing policies should include:

- Processes and procedures for determining which activities can be outsourced and how the activities will be outsourced.
- Processes for selecting service providers (e.g., due diligence).
- Structuring the outsourcing agreement to describe termination rights, ownership of data, and confidentiality requirements.
- Monitor risks of the arrangement including the financial health of the service provider.
- Implement a risk control environment and assess the control environment at the service provider.
- Develop contingency plans.
- Clearly define responsibilities of the bank and the service provider.

Key Concepts

LO 38.1

The Basel Committee on Banking Supervision defines operational risk as, "the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events."

The Basel Committee recognizes three common lines of defense used to control operational risks. These lines of defense are: (1) business line management, (2) independent operational risk management function, and (3) independent reviews of operational risks and risk management.

LO 38.2

The 11 fundamental principles of operational risk management suggested by the Basel Committee are:

1. The maintenance of a strong risk management culture led by the bank's board of directors and senior management.

2. The operational risk framework (i.e., the "Framework") must be developed and fully integrated in the overall risk management processes of the bank.

3. The board should approve and periodically review the Framework. The board should also oversee senior management to ensure that appropriate risk management decisions are implemented at all levels of the firm.

4. The board must identify the types and levels of operational risks the bank is willing to assume as well as approve risk appetite and risk tolerance statements.

5. Consistent with the bank's risk appetite and risk tolerance, senior management must develop a well-defined governance structure within the bank.

6. Operational risks must be identified and assessed by managers. Senior management must understand the risks, and the incentives related to those risks, inherent in the bank's business lines and processes.

7. New lines of business, products, processes, and systems should require an approval process that assesses the potential operational risks.

8. A process for monitoring operational risks and material exposures to losses should be put in place by senior management and supported by senior management, the board of directors, and business line employees.

9. Banks must put strong internal controls and risk mitigation and risk transfer strategies in place to manage operational risks.

10. Banks must have plans in place to survive in the event of a major business disruption. Business operations must be resilient.

11. Banks should make disclosures that are clear enough that outside stakeholders can assess the bank's approach to operational risk management.

LO 38.3

The board of directors and senior management must be engaged with operational risk assessment related to all 11 of the fundamental principles of operational risk management. The operational risk management framework must define, describe, and classify operational risk and operational loss exposure. The Framework must be documented in the board of directors approved policies.

LO 38.4

There are several tools that may be used to identify and assess operational risk. The tools include business process mappings, risk and performance indicators, scenario analysis, using risk assessment outputs as inputs for operational risk exposure models, audit findings, analyzing internal and external operational loss data, risk assessments, and comparative analysis.

LO 38.5

An effective control environment should include the following five components: (1) a control environment, (2) risk assessment, (3) control activities, (4) information and communication, and (5) monitoring activities.

LO 38.6

Technology can be used to mitigate operational risks but it introduces its own risks. The Basel Committee recommends an integrated approach to identifying, measuring, monitoring, and managing technology risks. Technology risk management tools are similar to those suggested for operational risk management.

Outsourcing involves the use of third parties to perform activities or functions for the firm. Outsourcing may reduce costs, provide expertise, expand bank offerings, and/or improve bank services. The board of directors and senior management must understand the operational risks that are introduced as a result of outsourcing.

Concept Checkers

1. Griffin Riehl is a risk manager at Bluegrass Bank and Trust, a small, independent commercial bank in Kentucky. Riehl has recently read the Basel Committee on Banking Supervision's recommendations for sound operational risk management and would like to put several controls in place. He would like to start with the three lines of defense suggested by the committee. Which of the following is not one of the three common "lines of defense" suggested by the Basel Committee for operational risk governance?
   A. Business line management.
   B. Board of directors and senior management risk training programs.
   C. Creating an independent operational risk management function in the bank.
   D. Conducting independent reviews of operational risks and risk management operations.

2. Garrett Bridgewater, a trader at a large commercial bank, has continued to increase his bonus each year by producing more and more profit for the bank. In order to increase profits, Bridgewater has been forced to increase the riskiness of his positions, despite the written risk appetite and tolerance statements provided to all employees of the bank. The bank seems happy with his performance so Bridgewater takes that as a sign of approval of his methods for improving profitability. Which of the following pairs of the 11 fundamental principles of risk management has the bank most clearly violated in this situation?
   A. Principle 1 (a strong risk management culture) and Principle 11 (the bank should make clear disclosures of operational risks to stakeholders).
   B. Principle 2 (develop an integrated approach to operational risk management) and Principle 7 (establish a rigorous approval process for new lines of business).
   C. Principle 3 (approve and review the operational risk framework) and Principle 4 (develop risk appetite and tolerance statements).
   D. Principle 5 (develop a well-defined governance structure) and Principle 6 (understand the risk and incentives related to risk inherent in the bank's business lines and processes).

3. Gary Hampton is providing descriptions of the operational risk management assessment tools, reporting lines, and accountabilities to the board of directors. Hampton is most likely working on:
   A. Framework documentation.
   B. A corporate operational risk function (CORF) handbook of operations.
   C. An outline of the fundamental principles of operational risk management.
   D. An open group operational framework diagram.

4. George Mathis works in risk analysis and management at a large commercial bank. He uses several tools to identify and assess operational risk. He has asked several business line managers to identify some risk events that would disrupt business. Each manager has also provided their thoughts on what would happen given worst case operational failures. The risk assessment tool Mathis is most likely using in this case is(are):
   A. risk indicators.
   B. comparative analysis.
   C. scenario analysis.
   D. business process mappings.

5. A risk management officer at a small commercial bank is trying to institute strong operational risk controls, despite little support from the board of directors. The manager is considering several elements as potentially critical components of a strong control environment. Which of the following is not a required component of an effective risk control environment as suggested by the Basel Committee on Banking Supervision?
   A. Information and communication.
   B. Monitoring activities.
   C. A functionally independent corporate operational risk function.
   D. Risk assessment.

Concept Checker Answers

1. **B** The three common "lines of defense" suggested by the Basel Committee on Banking Supervision and employed by firms to control operational risks are: (1) business line management, (2) an independent operational risk management function, and (3) independent reviews of operational risks and risk management.

2. **D** Based on the choices provided, the best match for the scenario is a violation of Principles 5 and 6. It is clear that the bank has not considered the incentives that are related to risk taking in the bank. Bridgewater has been given the risk appetite and tolerance statements but senior managers keep rewarding Bridgewater for high returns and seem to be ignoring the fact that they are the result of higher risks. Thus, there are incentives linked to increasing risk. The governance structure may or may not be well defined, but regardless, is not being adhered to.

3. **A** The operational risk management framework (i.e., the Framework) must define, describe, and classify operational risk and operational loss exposure. Hampton is likely working on Framework documentation. Framework documentation is overseen by the board of directors and senior management.

4. **C** Mathis is asking for managers to identify potential risk events, which he will use to assess potential outcomes of these risks. This is an example of scenario analysis. Scenario analysis is a subjective process where business line managers and risk managers identify potential risk events and then assess potential outcomes of those risks.

5. **C** A functionally independent corporate operational risk function is desirable in a bank but is not necessary for an effective control environment. This is especially true for a small bank, which might roll all risk management activities into one risk management group (i.e., not segregated by type of risk). An effective control environment should include the following five components: (1) a control environment, (2) risk assessment, (3) control activities, (4) information and communication, and (5) monitoring activities.

The following is a review of the Operational and Integrated Risk Management principles designed to address the learning objectives set forth by GARP®. This topic is also covered in:

Enterprise Risk Management: Theory and Practice

Topic 39

Exam Focus

Enterprise risk management (ERM) is the process of managing all of a corporation's risks within an integrated framework. This topic describes how ERM can be implemented in a way that enables a company to manage its total risk-return tradeoff in order to better carry out its strategic plan, gain competitive advantage, and create shareholder value. Key issues include why it may be optimal to hedge diversifiable risk and how to differentiate between core risks the firm should retain and noncore risks the firm should layoff. Also discussed is the determination of the optimal amount of corporate risk and the importance of ensuring that managers at all levels take proper account of the risk-return tradeoff. For the exam, understand the framework for developing and implementing ERM.

Creating Value With ERM

LO 39.1: Define enterprise risk management (ERM) and explain how implementing ERM practices and policies can create shareholder value, both at the macro and the micro level.

A business can manage its risks separately, one at a time, or all together in a cohesive framework. **Enterprise risk management** (ERM) is the process of managing all of a corporation's risks within an integrated framework.

The benefit of ERM is that a comprehensive program for managing risk allows the business to achieve its ideal balance of risk and return.

Macro Level

At the macro level, ERM allows management to optimize the firm's risk/return tradeoff. This optimization assures access to the capital needed to execute the firm's strategic plan.

The perfect markets view of finance implies that a company's cost of capital is unrelated to its diversifiable risk. Rather, the cost of capital is determined by the firm's **systematic risk** (also referred to as nondiversifiable, market, or beta risk). According to this view, efforts to hedge diversifiable risk provide no benefit to shareholders, who can eliminate this risk by diversifying their portfolios.

However, reducing diversifiable risk can be beneficial when markets are imperfect. Suppose a firm experiences a large and unexpected drop in its operating cash flow and does not have

funds sufficient to fund valuable investment opportunities. In perfect markets, the firm would be able to raise funds on fair terms to fund all of its value-creating projects. When markets are not perfect (i.e., investors' information about project values is incomplete), the firm may not be able to raise the needed funds on fair terms. This can lead to the "underinvestment problem," where the company passes up valuable strategic investments rather than raise equity on onerous terms. The inability to fund strategic investments on a timely basis can result in a permanent reduction in shareholder value, even if the cash shortfall is temporary. By hedging diversifiable risks, the company reduces the likelihood of facing the underinvestment problem. Thus, the primary function of corporate risk management is to protect the company's strategic plan by ensuring timely investment. The ability to carry out the strategic plan in a timely manner confers an advantage over competitors who are unable to do so.

Micro Level

In order for ERM to achieve the objective of optimizing the risk/return tradeoff, each project must be evaluated not only for the inherent risk of the project but also for the effect on the overall risk of the firm. Thus, ERM requires that managers throughout the firm be aware of the ERM program. This decentralization of evaluating the risk/return tradeoff has two components:

- Any managers evaluating new projects must consider the risks of the project in the context of how the project will affect the firm's total risk.
- Business units must be evaluated on how each unit contributes to the total risk of the firm. This gives the individual managers an incentive to monitor the effect of individual projects on overall firm risk.

There are three reasons why decentralizing the risk-return tradeoff in a company is important:

1. *Transformation of the risk management culture:* A consistent, systematic assessment of risks by all business units ensures that managers consider the impact of all important risks.

2. *Every risk is owned:* Because performance evaluations are based on risk, managers have an incentive to consider important risks in their decision making.

3. *Risk assessment by those closest to the risk:* Managers in the individual business units have the knowledge and expertise needed to assess and manage the risks of the business unit.

Development and Implementation

LO 39.2: Explain how a company can determine its optimal amount of risk through the use of credit rating targets.

LO 39.3: Describe the development and implementation of an ERM system, as well as challenges to the implementation of an ERM system.

In developing an ERM, management should follow this framework:

- *Determine the firm's acceptable level of risk.* The critical component of this determination is selecting the probability of financial distress that maximizes the value of the firm. Financial distress in this context means any time the firm must forego projects with positive net present values, due to inadequate resources. The likelihood of financial distress could be minimized by investing all funds into U.S. Treasury securities, but this should not be the firm's objective. The objective should be maximizing firm value by selecting an appropriate probability of distress. For many firms, the proxy used for measuring the probability of distress is the firm's credit rating assigned by external agencies. Thus, the firm may determine that the objective under ERM is to avoid a minimum credit rating below BBB. If the firm is currently rated AA, for example, the likelihood of falling below BBB can be estimated by average data supplied by the rating agency.
- *Based on the firm's target debt rating, estimate the capital (i.e., buffer) required to support the current level of risk in the firm's operations.* In other words, how much capital does the firm need to have (on hand or available externally) to ensure that it can avoid financial distress. A company with liquid assets sufficient to fund all of its positive NPV projects would not be exposed to the underinvestment problem when it encountered cash flow deficits. Thus, risk management can be viewed as a substitute for investing equity capital in liquid assets. Keeping a large amount of equity in the form of liquid assets is costly. Instead of maintaining a large liquid asset buffer, a company can institute a risk management program to ensure (at some level of statistical significance) that its operating cash flow will not fall below the level needed to fund valuable projects. That is, the firm can take actions to limit the probability of financial distress to a level that maximizes firm value. The goal of ERM is to optimize (not eliminate) total risk by trading off the expected returns from taking risks with the expected costs of financial distress.
- *Determine the ideal mix of capital and risk that will achieve the appropriate debt rating.* At this level of capital, the firm will be indifferent between increasing capital and decreasing risk.
- *Decentralize the risk/capital tradeoff by giving individual managers the information and the incentive they need to make decisions appropriate to maintain the risk/capital tradeoff.*

The implementation steps of ERM are as follows:

Step 1: *Identify the risks of the firm.* For many banks, risks are classified as falling into one of three categories: market, credit, or operational. Other financial institutions broaden the list to include asset, liability, liquidity, and strategic risks. Identification of risks should be performed both top-down (by senior management) and bottom-up (by individual managers of business units or other functional areas).

Step 2: Develop a consistent method to evaluate the firm's exposure to the risks identified above. If the methodology is not consistent, the ERM system will fail because capital will be mis-allocated across business units.

Implementation of an ERM system is challenging, and it is important that the entire organization supports the system. Thus, it is critical for all levels of the organization to understand how the system is designed and how it can create value. Monitoring the ERM system may be neglected due to its time-consuming nature. However, the inability to identify relevant risks on a regular basis could lead to corporate failures.

Economic Value vs. Accounting Value

Credit ratings are typically based on accounting data, combined with some level of subjective assessment by analysts. Economic value, as determined by management, may very well be a more accurate reflection of the true value of the firm.

In determining whether accounting value or economic value is more relevant, the firm must consider its objective. If the objective is to manage the probability of default, the question of how default is determined becomes important. If default is determined by failure to meet certain accounting measures (e.g., debt ratio, interest coverage), then accounting measures will be a critical component of meeting the objectives.

If the objective is to manage the present value of future cash flows, then economic measures may be more appropriate than accounting measurements that do not accurately capture economic reality. Management must consider that managing economic value may lead to more volatile accounting earnings, which may ultimately affect economic value as well.

Risk Aggregation

LO 39.4: Describe the role of and issues with correlation in risk aggregation, and describe typical properties of a firm's market risk, credit risk, and operational risk distributions.

Firms that use value at risk (VaR) to assess potential loss amounts will ultimately have three different VaR measures to manage. Market risk, credit risk, and operational risk will each produce their own VaR measures. The trick to accurately measuring and managing firm-wide risk, and in turn **firm-wide VaR**, is to understand how these VaR measures interact. Market risks will typically follow a normal distribution; however, the distributions for credit risks and operational risks are usually asymmetric in shape, due to the fat-tail nature of these risks.

Due to diversification effects of aggregating market, credit, and operational risk, firm-wide VaR will be less than the sum of the VaRs from each risk category. This suggests that the correlation among risks is some value less than one. It can be difficult to determine this correlation amount, so firms typically use average correlation values within their respective industry. However, firms should recognize that correlations can be influenced by firm-specific actions as well as external events such as a financial crisis.

Capital Allocation

LO 39.5: Distinguish between regulatory and economic capital, and explain the use of economic capital in the corporate decision making process.

Regulatory capital requirements may differ significantly from the capital required to achieve or maintain a given credit rating (**economic capital**). If regulatory requirements are less than economic capital requirements, then the firm will meet the regulatory requirements as part of its ERM objectives, and there will be no effect on the firm's activities.

However, if regulatory capital requirements are greater than economic capital requirements, then the firm will have excess capital on hand. If competitors are subject to the same requirements, this excess capital will amount to a regulatory tax. If competing firms are not subject to the excess capital requirement, they will have a competitive advantage.

Because regulatory capital requirements are typically based on accounting capital, rather than economic capital, a firm with economic values in excess of accounting values may be penalized, and may have to maintain higher amounts in liquid assets to cover the shortfall.

The economic capital of the firm must be put to productive use. If a firm accumulates excess economic capital that is not employed productively, investors will reduce the value of the firm. This reduction will be consistent with the failure of existing management to earn the cost of capital on the excess amount.

As a firm takes on new projects, the probability of financial distress increases. One way to offset this increased risk is to raise enough additional capital to bring the risk of financial distress back to the level that existed prior to the new project.

For example, assume that a firm has a value at risk (VaR) measure of $1 billion. As a result of a new expansion project, assume the VaR figure increases to $1.1 billion. In order to offset the risk of the new project, the firm would need to do the following:

1. Raise additional capital of $100 million.

2. Invest this additional capital without increasing the overall risk of the firm.

If the cost of the additional capital is 6%, and the new project is expected to last one year, then the new project would need to generate an additional $6 million to maintain the economic capital of the firm. Looked at another way, the expected benefit of the new project should be reduced by $6 million to compensate for the incremental risk to the firm.

These decisions regarding how the risk of new projects will affect the total risk of the firm are further complicated by the correlations of the expected returns of the projects. If two new projects are less than perfectly correlated, the incremental increase in total risk will be less. One way to account for any possible diversification benefits is to reduce the cost of capital of projects that are expected to have lower correlations with existing operations.

Risks to Retain and Risks to Layoff

Many risks can be hedged inexpensively with derivatives contracts. Examples include exposures to changes in exchange rates, interest rates, and commodities prices. Rather than face the risk that unexpected cash shortfalls due to these exposures might negatively affect the ability of the firm to carry out its strategic plan, the firm should hedge these exposures.

Other risks cannot be inexpensively hedged. These are risks where the firm's management either has an informational advantage over outsiders or the ability to manage the outcome of the risk-taking activity. A counterparty to a transaction that hedges such risks would require very high compensation to be willing to take on the transferred risks. The firm's business risks fall into this category.

The guiding principle in deciding whether to retain or layoff risks is the **comparative advantage** in risk bearing. A company has a comparative advantage in bearing its strategic and business risks, because it knows more about these risks than outsiders do. Because of this informational advantage, the firm cannot transfer these risks cost effectively. Moreover, the firm is in the business of managing these "core" risks. On the other hand, the firm has no comparative advantage in forecasting market variables such as exchange rates, interest rates, or commodities prices. These "noncore" risks can be laid off. By reducing noncore exposures, the firm reduces the likelihood of disruptions to its ability to fund strategic investments and increases its ability to take on business risks.

Key Concepts

LO 39.1

Enterprise risk management (ERM) is the process of managing all a corporation's risks within an integrated framework.

The macro benefit of ERM is that hedging corporate diversifiable risk improves management's ability to invest in value-creating projects in a timely manner and improves the firm's ability to carry out the strategic plan.

The micro benefit of ERM requires decentralizing risk management to ensure that each project's total risk is adequately assessed by project planners during the initial evaluation of the project. The two main components of decentralizing the risk-return tradeoff are consideration of the marginal impact of each project on the firm's total risk and a performance evaluation system that considers unit contributions to total risk.

LO 39.2

The goal of risk management is to optimize (not eliminate) total risk by trading off the expected returns from taking risks with the expected costs of financial distress. Financial distress in this case is defined as circumstances where the firm is forced to forego positive NPV projects.

LO 39.3

The conceptual framework of ERM is a four-step process:

- Determine the firm's risk appetite.
- Estimate the amount of capital needed to support the desired level of risk.
- Determine the optimal combination of capital and risk that achieves the target credit rating.
- Decentralize the management of risk.

LO 39.4

Due to diversification effects of aggregating market, credit, and operational risk, firm-wide VaR will be less than the sum of the VaRs from each risk category. This suggests that the correlation among risks is some value less than one.

LO 39.5

Regulatory capital requirements may differ significantly from the capital required to achieve or maintain a given credit rating (economic capital).

Because regulatory capital requirements are typically based on accounting capital, rather than economic capital, a firm with economic values in excess of accounting values may be penalized, and may have to maintain higher amounts in liquid assets to cover the shortfall.

The economic capital of the firm must be put to productive use. If a firm accumulates excess economic capital that is not employed productively, investors will reduce the value of the firm.

Concept Checkers

1. Reducing diversifiable risk creates value:
   A. only when markets are perfect.
   B. because it is costly for shareholders to eliminate diversifiable risk through their own actions.
   C. because reducing diversifiable risk mitigates the underinvestment problem that can occur when investors have imperfect information about the firm's projects.
   D. only when it results in a permanent reduction in cash flow.

2. Effective enterprise risk management includes all of the following except:
   A. centralized evaluation of every project's risk.
   B. a project is only accepted if its return is adequate after considering the cost of the project's contribution to total firm risk.
   C. the project's planners perform the initial evaluation of project risk.
   D. periodic evaluations of the performance of business units consider each unit's contribution to total risk.

3. The goal of enterprise risk management (ERM) can best be described as maximizing firm value by:
   A. eliminating the total risk of the firm.
   B. minimizing the total risk of the firm.
   C. optimizing the total risk of the firm.
   D. eliminating the probability of financial distress.

4. In determining the relative importance of economic value compared to accounting performance in its enterprise risk management program, a firm should:
   A. rely on accounting performance because it will be more accurate.
   B. rely on economic value because it will be more accurate.
   C. base its decision on the input of project-level managers.
   D. base its decision on the objective of the ERM program.

5. Which risk is least likely to be beneficial for a company to layoff?
   A. Currency exchange rate risk.
   B. Business risk.
   C. Commodities price risk.
   D. Interest rate risk.

Concept Checker Answers

1. C When markets are not perfect (i.e., investors' information about project values is incomplete), the firm may not be able to raise funds on fair terms. For a firm faced with an unexpected drop in operating cash flow, this can lead to the underinvestment problem, where the company passes up valuable strategic investments rather than raise equity on onerous terms. The inability to fund strategic investments can result in a permanent reduction in shareholder value even if the cash shortfall is temporary. Hedging diversifiable risk mitigates the underinvestment problem and creates value, even though shareholders can eliminate diversifiable risk at low cost by diversifying their portfolios.

2. A Central to ERM is the idea that a *decentralized* approach to the evaluation of project risks focuses managers throughout the firm on the importance of properly considering the risk and return implications of projects.

3. C The goal of ERM is to optimize the total risk of the firm. Eliminating total risk is not possible. Minimizing total risk would preclude accepting risky projects that would allow the firm to expand and maximize value. These risky projects will increase the probability of financial distress. The goal of ERM is to optimize the risk of distress relative to the potential returns from the risky projects.

4. D There are certain situations where either accounting values or economic values will more accurately reflect the firm's situation. The determining factor in choosing between economic values and accounting values is the objective of the program. For example, if the objective is maintaining a rating, based in large part on accounting numbers, then accounting numbers will assume more relative importance.

5. B A company has a comparative advantage in bearing its strategic and business risks because it knows more about these risks than outsiders do. The firm is in the business of managing these "core" risks. The firm has no comparative advantage in forecasting market variables such as exchange rates, interest rates, or commodities prices. These "noncore" risks can be laid off.

The following is a review of the Operational and Integrated Risk Management principles designed to address the learning objectives set forth by GARP®. This topic is also covered in:

Observations on Developments in Risk Appetite Frameworks and IT Infrastructure

Topic 40

Exam Focus

This topic discusses the concept of a risk appetite framework (RAF). For the exam, understand the elements and benefits of an RAF, and be familiar with best practices for an effective RAF. Also, be able to identify metrics that can be monitored as part of an effective RAF. Finally, understand the elements and benefits of a robust risk data infrastructure as well as best practices relating to data aggregation.

Risk Appetite Framework

LO 40.1: Describe the concept of a risk appetite framework (RAF), identify the elements of an RAF, and explain the benefits to a firm of having a well-developed RAF.

A **risk appetite framework** (RAF) is a strategic decision-making tool that represents the firm's core risk strategy. It sets in place a clear, future-oriented perspective of the firm's target risk profile in a number of different scenarios and maps out a strategy for achieving that risk profile. It also specifies which types of risk the firm is willing to take and under what conditions as well as which types of risk the firm is unwilling to take.

An RAF should start with a risk appetite statement that is essentially a mission statement from a risk perspective. This statement should cover some or all of the following elements:

- Desired business mix and balance sheet composition (i.e., capital structure—trade-off between debt and equity).
- Risk preferences (i.e., how much credit or market risk to take on or hedge)
- Acceptable trade-off between risk and reward.
- Acceptable limits for volatility (based on standard deviation).
- Capital thresholds (i.e., regulatory and economic capital).
- Tolerances for post-stress losses.
- Target credit ratings.
- Optimum liquidity ratios.

The benefits of a well-developed RAF are as follows:

- It improves a firm's strategic planning and tactical decision-making.
- The inherent flexibility allows firms to adapt to market changes, especially if appropriate opportunities arise that require adjustments to the RAF.

- It assists firms in preparing for the unexpected; requires business line strategy reviews and maintains an open dialogue regarding the management of unexpected economic or market events in particular geographies or products.
- It focuses on the future and sets expectations regarding the firm's consolidated risk profile after performing relevant stress tests and scenario analyses. Thus, it helps the firm set up a plan for risk taking, loss mitigation, and use of contingency measures.

Developing and Implementing an Effective RAF

LO 40.2: Describe best practices for a firm's Chief Risk Officer (CRO), Chief Executive Officer (CEO), and Board of Directors in the development and implementation of an effective RAF.

Chief Risk Officer (CRO) Best Practices

Board members involved with risk issues should be able to directly contact the CRO and engage in frequent communication about on-going key risk issues. A best practice could be to create a board risk committee that is directly involved in performance review and compensation decisions regarding the CRO. A strong alliance between the CRO (risk management function) and the CFO (budgetary considerations) is key to spreading the use of the RAF throughout the organization. Specifically, a best practice would be for the CRO and CFO to report to the board at every meeting by commenting on the firm's risk profile in comparison to the RAF. The CRO discussion could be broad and strategic in nature, and the CFO discussion could discuss financial impacts.

Chief Executive Officer (CEO) Best Practices

The CEO should strongly support the RAF and refer/use it to support challenging risk and strategic decisions. The willingness of the CEO to give the CRO the final word on many risk decisions is a best practice since it strengthens the importance of the risk management function. Where any instances of non-compliance with the RAF exist, a best practice would be for the CRO and/or the CEO to advise the board of directors on the corrective measures that will be undertaken.

Board of Directors (Board) Best Practices

The board needs to spend a considerable amount of time conveying the firm's risk appetite statement throughout the firm to ensure it is properly implemented. In challenging management to operate the firm in a way that is congruent with the RAF, the board must focus on strategic and forward-looking issues rather than dwelling on past actions. A best practice would be for the board to state its expectations to management in advance so that management can establish appropriate strategic plans.

When a board challenges management and requires a thorough vetting of the RAF, the end product is more complete and relevant. A best practice is to have the active involvement of the board with senior management in continually revising the RAF until everyone

is satisfied. Additionally, another best practice is the development of a concrete way of assessing when the RAF needs to be amended to reflect a changing environment.

With regard to technical knowledge of members, there should be a sufficient balance in board composition to ensure all members have a reasonable and congruent understanding of the firm's risks and to avoid situations where there are marked divisions between "experts" and "non-experts." A best practice is to provide detailed technical training to board members on relevant concepts. Additionally, requiring cross-membership amongst the major committees helps ensure that those functions have members with a strong technical base. The training and cross-membership practices should serve as supplements to existing expertise.

Boards must be proactive in stating the nature and frequency of the information they need. As a best practice, reporting to the board should be thorough and broad in scope and not overly simplified. Additionally, communication from management should include a business aspect and not be focused on just technical aspects. Finally, as another best practice, the board should be willing to push back to management if they feel the information provided is not sufficient for their needs.

Reputation risk needs to have a significant amount of the board's attention. As a best practice, the board should set up a reputational risk committee to analyze marketplace changes and approve transactions on the basis of geography or product line. Attempting qualitative measures of reputation risk should also be done via monitoring industry headlines and reporting trends to the board as well as hiring external parties to conduct relevant surveys.

Using RAF to Manage Business Lines

LO 40.3: Explain the role of an RAF in managing the risk of individual business lines within a firm.

Generally speaking, the RAF helps to ensure that each business line's strategies are congruent with the firm's desired risk profile. The various business line managers each submit a medium-term business plan to senior management and/or the board to determine if it is consistent with the RAF. Such determinations are often made with stress tests or scenario analyses. Afterward, the RAF will set the risk limits allocated to each business line based on its desired risk profile.

Additionally, the RAF considers the integrated nature of the business lines within the firm. For example, the RAF can help determine how much a given business line's medium-term business plans has to be amended in order to allow another business line's proposal to be approved. In other words, there may be some borrowing of the risk appetite allotment from a business line in order to take advantage of the current opportunity in another business line. Familiarity with the RAF by business line managers would dramatically decrease the number of plans that fall well outside acceptable bounds. A clear RAF assists the firm in preventing risk appetite drift when economic conditions change.

Effective RAF Metrics

LO 40.4: Describe the classes of risk metrics to be communicated to managers within the firm.

Examples of metrics that can be monitored as part of an effective RAF are as follows:

- Capital targets (economic capital, tangible common equity, total leverage) or capital-at-risk amounts.
- Liquidity ratios, terms, and survival horizons.
- Net interest income volatility or earnings-at-risk calculations.
- Value at risk (VaR) limits.
- Risk sensitivity limits.
- Risk concentrations by internal and/or external credit ratings.
- Expected loss ratios.
- The firm's own credit spreads.
- Asset growth ceilings by business line or exposure type.
- Performance of internal audit ratings.
- Economic value added.
- Post-stress-test targets for capital, liquidity, and earnings.

It is important to ensure that the metrics used to monitor risk are appropriate to the users of the information. Therefore, the risk metrics should be divided into classes, depending on who is receiving the information within the firm. For example:

- Directors should receive high-level metrics (less detail) that reflect the firm's key risks.
- CEO, CFO, CRO should receive more detailed metrics than directors.
- Business line leaders should receive very detailed metrics, especially in relation to their respective business lines.

Risk Data Infrastructure

LO 40.5: Explain the benefits to a firm from having a robust risk data infrastructure, and describe key elements of an effective IT risk management policy at a firm.

A benefit of a robust risk data infrastructure is the ability to aggregate timely and accurate data to report on credit, market, liquidity, and operational risks. This, in turn, allows management to make proper decisions regarding the firm's strategy, risk appetite, and risk management during periods of constant and frequent changes. Another benefit is the ability to sufficiently document and convey the firm's risk reporting requirements. Such requirements include: specific metrics, data accuracy expectations, element definitions, time frames, supervisory expectations, and regulatory reporting requirements.

Key elements of an effective IT risk management policy at a firm are described as follows:

- Clearly defined standards and internal risk reporting requirements to ensure a proper IT infrastructure and internal reporting.
- Sufficient funding is provided to develop IT systems for the purpose of internal risk reporting; they compete equally with proposals that are revenue generating, for example.

- Assessing IT infrastructure and capacity prior to approving new products.
- Post-implementation reviews of IT systems performed anywhere from 6–18 months afterward as a check that the systems meet the risk personnel's needs.
- The level of governance for outsourced IT activities is the same as if they were done in-house. There are no impediments to implementation or access to data due to outsourcing.
- The existence of effective project management offices (PMOs) to ensure that timelines and deliverables are met. Specifically, one person is in charge of the PMO, which seems to result in stronger coordination and communication between project staff.
- There is a data administrator as well as a data owner, and the data owner must ensure a sufficiently high level of data accuracy, integrity, and availability. This helps to ensure that IT projects are meeting the users' needs.
- The board is able to implement relevant internal audit programs to allow for periodic reviews of data maintenance processes and functions. The monitoring could be continuous or specific to a product or business line. This would allow for the quick correction of any weaknesses detected by internal audit.

Poor or Fragmented IT Infrastructure

LO 40.6: Describe factors that could lead to poor or fragmented IT infrastructure at an organization.

There are five major factors to consider with regard to poor or fragmented IT infrastructures.

1. *No common understanding of long-term business strategy between business lines and IT management.* This factor often results due to internal competition for funding, thereby not permitting important IT infrastructure projects to be completed.

2. *Management only makes decisions based on short-term profits.* As a result of this factor, many IT infrastructure projects are scaled back, delayed, or eliminated.

3. *Significant turnover in important IT roles within the firm.* This factor has resulted in delays in completing IT projects.

4. *Insufficient data governance and insufficient data management plan within the firm.* This factor results in inconsistency across business lines in how to upgrade systems; this is costly if the systems end up being incompatible because of the inconsistencies.

5. *Merger and acquisition activities.* This factor results in multiple systems running simultaneously within the recently merged firm. Data aggregation across products and business lines becomes a significant challenge.

Data Aggregation Best Practices

LO 40.7: Explain the challenges and best practices related to data aggregation at an organization.

The existence of several IT systems being operated simultaneously within a firm results in a lack of integrated IT systems. This, in turn, requires a significant amount of manual data entry to allow for proper aggregation of risk data. Best practices related to data aggregation at an organization are explained as follows:

- To increase efficiency and accuracy, minimize the amount of manual intervention and manual data manipulation (i.e., spreadsheets) by automating the risk data aggregation process.
- Aggregated risk data needs to be accurate, timely, and comprehensive in order to have value. Therefore, there must be standards, cutoff times, and timelines regarding the production of internal risk reports.
- Single platform centralized databases with single identifiers and/or consistent naming conventions could allow for the timely retrieval of multiple records of risk data across the firm. They also permit data segmentation when required to produce specific data (i.e., risk concentrations).
- Create data warehouses that will take information from various subsystems and store them in a warehouse. The data is then filtered and reorganized so that customized reports can be created using specific data from the warehouse.
- Automated reconciliation will reduce the risk of manual errors and incomplete information. For example, off-balance sheet data should not be omitted.
- Periodic reconciliation of risk and financial data will ensure the accuracy and proper operation of the IT system.
- For merger and acquisition transactions, ensuring that legacy IT systems are integrated into the chosen IT system as soon as possible.
- When obtaining approvals for new IT purchases, involve the appropriate technical staff to ensure that the existing systems can process and aggregate data from these new items.

Key Concepts

LO 40.1

A risk appetite framework (RAF) sets in place a clear, future-oriented perspective of the firm's target risk profile in a number of different scenarios and maps out a strategy for achieving that risk profile. An RAF should start with a risk appetite statement that is essentially a mission statement from a risk perspective. Benefits of a well-developed RAF include assisting firms in preparing for the unexpected and greatly improving a firm's strategic planning and tactical decision-making.

LO 40.2

The chief risk officer (CRO) should be easily available to the board of directors (board) and there should be a strong alliance between the CRO and the chief financial officer (CFO).

The chief executive officer (CEO) should strongly support the RAF and give the CRO the final word on risk decisions.

The board should: be willing to challenge management to operate the firm consistent with the RAF, actively work with senior management to continually revise the RAF, have sufficient technical and business understanding of the risks facing the firm, be proactive in stating the nature and frequency of the information they need, and set up a reputational risk committee.

LO 40.3

The RAF helps to ensure that each business line's strategies are congruent with the firm's desired risk profile. It also considers the integrated nature of the business lines within the firm.

LO 40.4

Many metrics can be monitored as part of an effective RAF. Risk metrics should be divided into classes, depending on who is receiving the information within the firm.

LO 40.5

A robust data infrastructure results in management being able to make proper decisions regarding a firm's strategy, risk appetite, and risk management. Additionally, it allows for the ability to sufficiently document and convey the firm's risk reporting requirements.

Key elements of an effective IT risk management policy include: clearly defined standards and internal risk reporting requirements, sufficient funding to develop IT systems, assessing IT infrastructure and capacity prior to approving new products, timely post-implementation reviews of IT systems, and sufficient governance for outsourced IT activities.

LO 40.6

Poor or fragmented IT infrastructures result from a lack of common understanding of long-term business strategies between business lines and IT management, managers thinking only about short-term profits, significant turnover in IT roles, insufficient data governance, and merger and acquisition activities.

LO 40.7

The lack of integrated IT systems is the major challenge related to data aggregations. Many best practices regarding data aggregations exist including: minimizing the amount of manual data processes, using single platform centralized databases, creating data warehouses, automated and periodic data reconciliations, and timely integration of legacy IT systems.

Concept Checkers

1. Which of the following statements regarding the risk appetite framework (RAF) is correct?
   A. The RAF represents the firm's core risk strategy.
   B. The RAF should be amended to take advantage of all profitable opportunities.
   C. The RAF focuses on which risks the firm is willing to take and under what conditions.
   D. The RAF begins with the risk appetite statement that contains many elements, including examining the composition of the income statement.

2. As a best practice, which of the following members of senior management should have the final word on significant risk decisions at a firm?
   A. Chief executive officer.
   B. Chief financial officer.
   C. Chief operating officer.
   D. Chief risk officer.

3. Which of the following statements regarding the role of a risk appetite framework (RAF) in managing the risk of individual business lines within a firm is correct?
   A. Individual business lines may collectively cause the firm's RAF to drift when market conditions change.
   B. Sensitivity analysis is a robust tool to assist senior management and/or the board to determine consistency with the RAF.
   C. Each individual business line's risk appetite allotment according to the RAF is independent of the others to ensure objectivity in the process.
   D. The business line managers submit long-term business plans to senior management and/or the board to determine if they are consistent with the RAF.

4. Which of the following statements is incorrect regarding the key elements of an effective IT risk management policy?
   A. Having a single person in charge of the project management office.
   B. Comparable funding for IT projects and revenue-generating projects.
   C. Post-implementation reviews of IT systems at least 24 months after implementation.
   D. Outsourced and in-house IT activities being subjected to the same level of monitoring.

5. Which of the following items is a best practice related to data aggregation at an organization?
   A. Integrating legacy IT systems into the new IT system immediately.
   B. The use of one master spreadsheet to accumulate all of the data in one place.
   C. Periodic manual reconciliations to reduce the risk of errors and incomplete information.
   D. Allowing individual departments as much time as they require to produce internal reports that are accurate, timely, and comprehensive.

Concept Checker Answers

1. **A** The RAF represents the firm's core risk strategy. The RAF does not necessarily need to be amended every time there is a profitable opportunity; doing so would cause the RAF to lose its value. The RAF also focuses on which risks the firm is unwilling to take. The risk appetite statement would not likely include an examination of the composition of the income statement; it would more likely be the balance sheet (i.e., debt, equity).

2. **D** The willingness of the CEO to give the CRO the final word on many risk decisions is a best practice, which has strengthened the importance of the risk management function.

3. **A** Individual business lines may collectively cause the firm's RAF to drift when market conditions change. Sensitivity analysis only examines one change in a variable at a time. More robust tools would be stress tests and scenario analyses, for example. Each business line's risk appetite allotment according to the RAF may be amended if another business line encounters an opportunity that requires more capital. The business line managers submit medium-term business plans to senior management and/or the board.

4. **C** Post-implementation reviews should be performed 6–18 months after implementation; 24 months or more would likely be too long. Having one person in charge of the project management office seems to have resulted in stronger coordination and communication between project staff.

5. **A** For merger and acquisition transactions, it is best that legacy IT systems are integrated into the chosen IT system as soon as possible. Spreadsheets are a form of manual data manipulation and, because they are not automated, they would not be a best practice. Automated reconciliations should be performed, not manual. One of the key points about internal risk reports is that they should be produced on a timely basis, therefore, there must be standards, cutoff times, and timelines regarding their production.

The following is a review of the Operational and Integrated Risk Management principles designed to address the learning objectives set forth by GARP®. This topic is also covered in:

Information Risk and Data Quality Management

Topic 41

Exam Focus

This topic is a qualitative examination of data quality issues. Organizations must understand the risks involved with data issues and be able to identify ways to protect one of their most valuable resources, their data. For the exam, focus on the important features of acceptable data as well as details surrounding data quality scorecards.

Poor Data Quality

The following is a list of negative impacts on a business from poor data quality.

Financial impacts:

- Businesses may experience lower revenues (e.g., lost sales), higher expenses (e.g., penalties, re-work costs), and lower cash flows as a result of inaccurate or incomplete data.

Confidence-based impacts:

- Managers may make incorrect business decisions based on faulty data.
- Poor forecasting may result due to input errors.
- Inaccurate internal reporting may occur with unreliable information.

Satisfaction impacts:

- Customers may become dissatisfied when the business processes faulty data (e.g., billing errors).
- Employees may become dissatisfied when they are unable to properly perform their job due to flawed data.

Productivity impacts:

- Additional (corrective) work may be required, thereby reducing production output.
- Delays or increases in processing time.

Risk impacts:

- Underestimating credit risks due to inaccurate documentation, thereby exposing a lender to potential losses (e.g., Basel II Accords for quantifying credit risk).
- Underestimating investment risk, thereby exposing an investor to potential losses.

Compliance impacts:

- A business may no longer be in compliance with regulations (e.g., Sarbanes-Oxley) if financial reports are inaccurate.

Data Errors

LO 41.1: Identify the most common issues that result in data errors.

The most common data issues that increase risk for an organization are as follows:

- Data entry errors.
- Missing data.
- Duplicate records.
- Inconsistent data.
- Nonstandard formats.
- Complex data transformations.
- Failed identity management processes.
- Undocumented, incorrect, or misleading metadata (description of content and context of data files).

From a financial perspective, such data errors (accidental or not) may lead to inconsistent reporting, incorrect product pricing, and failures in trade settlement.

Examples of risks arising out of data errors include:

- Fraudulent payroll overpayments to fictitious employees or those who are no longer employed by the firm.
- Underbilling for services rendered.
- Underestimating insurance risk due to missing and inaccurate values (e.g., insured value).

Acceptable Data

LO 41.2: Explain how a firm can set expectations for its data quality and describe some key dimensions of data quality used in this process.

A fundamental step in managing risks due to flawed data would be to set user expectations for data quality and then establish criteria to monitor compliance with such expectations. In order to define and measure these expectations, they can be categorized into key dimensions of data quality. The important (but not complete) set of dimensions that characterize acceptable data include accuracy, completeness, consistency, reasonableness, currency, and uniqueness.

Accuracy

The concept of accuracy can be described as the degree to which data correctly reflects the real world object. Measurement of accuracy can occur by manually comparing the data to an authoritative source of correct information—for example, the temperature recorded in a thermometer compared to the real temperature.

Completeness

Completeness refers to the extent to which the *expected* attributes of data are provided. There may be mandatory and optional aspects of completeness. For example, it may be mandatory to have a customer's primary phone number, but if the secondary phone number (optional) is not available, then the data requirement for the phone number is still considered complete.

Note that although data may be complete, it may not necessarily be accurate. For example, customers may have moved and their mailing addresses may not have been updated yet.

Consistency

Consistency refers to reasonable comparison of values between multiple data sets. The concept of consistency is broad and could require that data values from each data set do not conflict (e.g., a bank account is closed but the statement still shows account activity) or that they meet certain pre-defined constraints.

Note that consistency does not necessarily imply accuracy.

There are three types of consistency:

1. *Record level*: consistency between one set of data values and another set within the same record.

2. *Cross-record level*: consistency between one set of data values and another set in different records.

3. *Temporal level*: consistency between one set of data values and another set within the same record at different points in time.

Reasonableness

Reasonableness refers to conformity with consistency expectations. For example, the income statement value for interest expense should be consistent or within an acceptable range when compared to the corresponding balance sheet value for long-term debt.

Currency

Currency of data refers to the lifespan of data. In other words, is the data still considered relevant and useful, given that the passage of time will gradually render it less current and less correct? Measurement of currency would consist of determining the frequency in which the data needs to be updated, and determining whether the existing data is still up-to-date.

Uniqueness

Uniqueness of data is tied into the data error involving duplicate records. Uniqueness suggests that there can only be one data item within the data set. For example, within a

client list, there should only be one Mr. Jack Lee with a date of birth of January 1, 1970 living at 1234 Anywhere Street in New York City.

Operational Data Governance

LO 41.3: Describe the operational data governance process, including the use of scorecards in managing information risk.

Operational data governance refers to the collective set of rules and processes regarding data that allow an organization to have sufficient confidence in the quality of its data.

Specifically, a data governance program should exist that clarifies the roles and responsibilities in managing data quality. A **data quality scorecard** could be used to monitor the success of such a program.

In short, operational data governance aims to detect data errors early on and then set into motion the steps needed to sufficiently deal with the errors on a timely basis. As a result, there should be minimal or no subsequent impact on the organization.

Data Quality Inspection vs. Data Validation

Data validation is a one-time step that reviews and assesses whether data conforms to defined business specifications. In contrast, **data quality inspection** is an on-going set of steps aimed to:

1. reduce the number of errors to a tolerable level,
2. spot data flaws and make appropriate adjustments to allow data processing to be completed, and
3. solve the cause of the errors and flaws in a timely manner.

The goal of data quality inspection is to catch issues early on before they have a substantial negative impact on business operations.

Data Quality Scorecard

A **base-level metric** is straightforward in that it is measured against clear data quality criteria. It is relatively easy to quantify whether the criteria is met in terms of arriving at a data quality score.

In contrast, a **complex metric** is a combined score that could be a weighted average of several different metrics (customized to the specific user(s)). Such a combined metric allows for a qualitative reporting of the impact of data quality on the organization. A data quality scorecard could report the metric in one of three ways: by issue, by business process, or by business impact.

Complex Metric Scorecard Viewpoints

Data quality issues view:

- Considers the impact of a specific data quality problem over multiple business processes.
- The scorecard shows a combined and summarized view of the impacts for each data problem. By going into more detail, one can obtain further information on the sources of data problems. This allows for prioritization in terms of solving individual problems.

Business process view:

- For each business process, the scorecard has complex metrics that quantify the impact of each data quality problem.
- It allows for the ability to determine exactly where in the business process the data problem is originating. This will assist in solving the problem efficiently.

Business impact view:

- The scorecard provides a high-level understanding of the risks embedded in data quality problems (i.e., a combined and summarized view). It considers various data quality problems that occur in various business processes.
- By going into more detail, one can identify the business processes where the problems occur. An even more detailed examination will reveal the specific problems within each business process.

Motivation

Business managers may wish to take advantage of an opportunity to assess the relationship between the impacts of flawed data versus the pre-defined parameters of acceptable data quality. Such an assessment could occur with a data quality scorecard, with data being measured against the benchmark (acceptable data quality). The scorecard, therefore, serves as a strong management technique if it can summarize important organizational information as well as provide warning signs to management when corrective actions are required.

Mechanics

Regardless of the preferred view, a data quality scorecard is comprised of a hierarchy of base-level and complex metrics that tie into different levels of accountability within the organization. With regard to metrics, the same measurement might be used in different contexts, which allows for different error tolerances and weights. Finally, scorecards can be customized to present varying levels of detail depending on the intended user(s).

Key Concepts

LO 41.1

Data errors (e.g., missing data, inconsistent data, nonstandard formats) whether they are accidental or not, may lead to inconsistent reporting, incorrect product pricing, or failures in trade settlement.

LO 41.2

Key dimensions that characterize acceptable data include: accuracy, completeness, consistency, reasonableness, currency, and uniqueness.

LO 41.3

Operational data governance refers to the collective set of rules and processes regarding data that allow an organization to have sufficient confidence in the quality of its data.

Three different viewpoints regarding scorecards include: data quality issues view, business process view, and business impact view.

Data quality scorecards serve as a strong management technique if they are able to summarize important organizational information as well as provide warning signs to management when corrective actions are required.

Concept Checkers

1. Ryan Vail is a corporate manager who recently made a series of incorrect business decisions as a result of faulty data obtained internally. Which of the following negative business impacts best describes his incorrect decisions?
   A. Compliance impact.
   B. Confidence-based impact.
   C. Financial impact.
   D. Risk impact.

2. Data consistency is important to ensure that there are no clear conflicts in data values between data sets. Which of the following types of data consistency refers to consistency between one set of data values and another set of data values in different records?
   A. Record level.
   B. Temporal level.
   C. Cross-record level.
   D. Cross-temporal level.

3. Which of the following data issues is least likely to increase risk for an organization?
   A. Duplicate records.
   B. Data normalization.
   C. Nonstandard formats.
   D. Data transformations.

4. Which of the following statements regarding data quality inspection is correct? It attempts to:
   A. catch errors early in the process.
   B. reduce the number of errors to zero.
   C. solve the cause of any errors immediately.
   D. review and assess whether data conforms with defined business specifications.

5. Which of the following viewpoints regarding data quality scorecards is best described as providing a high-level understanding of the risks embedded in data quality problems?
   A. Business impact view.
   B. Business process view.
   C. Data quality issues view.
   D. Data process issues view.

Concept Checker Answers

1. **B** An example of a confidence-based (negative) impact would be a manager who makes incorrect business decisions based on faulty data.

2. **C** Record level consistency is consistency between one set of data values and another set within the same record. Cross-record level consistency is consistency between one set of data values and another set in different records.

3. **B** Data normalization is a process to better organize data in order to minimize redundancy and dependency, so it is least likely to increase risk. All of the other data issues are likely to increase risk, especially complex data transformations.

4. **A** Data quality inspection is intended to catch issues early on before they have a substantial negative impact on business operations. The idea is to reduce the number of errors to a tolerable level, not necessarily to zero. In addition, it aims to solve the cause of the errors in a timely manner, not necessarily immediately.

5. **A** With the business impact view, the scorecard provides a high-level understanding of the risks embedded in data quality problems (i.e., a combined and summarized view). It considers various data quality problems that occur in various business processes.

The following is a review of the Operational and Integrated Risk Management principles designed to address the learning objectives set forth by GARP®. This topic is also covered in:

OpRisk Data and Governance

Topic 42

Exam Focus

This topic discusses the seven level 1 categories of operational risk (OpRisk) events defined in Basel II and describes level 2 examples of operational risk events for each category. For the exam, understand how the collection and reporting of loss data, the risk control self assessment (RCSA), identification of key risk indicators (KRIs), and scenario analysis are all important elements of a firm's OpRisk process. Also, be familiar with the OpRisk profiles across various financial sectors with emphases on the highest frequency percentages and severity percentages. Finally, be prepared to describe the typical progression through four organizational risk designs for large firms.

Event-Driven Risk Categories

LO 42.1: 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 operational risk (OpRisk) framework requirements. OpRisk models are concerned with identifying and mitigating operational risks of the firm that are a function of people, systems, and external events. The seven Basel II event risk categories are described in Figure 1 and are intended to capture all potential operational risks. Every loss event should be mapped to the risk event categories outlined in the firm's operational risk management policies and procedures. However, some loss events may fall under more than one category.

It is important to recognize that the severity and frequency of losses can vary dramatically among the categories. For example, loss events are small but occur very frequently in the *Execution, Delivery, and Process Management* category. Whereas, losses are much less frequent but typically have a large dollar amount in the *Clients, Products, and Business Practices* category as these loss events commonly arise from substantial litigation suits.

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 operational risk management 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. In order 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 process of identifying and classifying risks is commonly referred to as **OpRisk taxonomy**.

Figure 1: 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.*

Each of these seven level 1 categories identified in Figure 1 is then further broken down into a level 2 subcategory. As mentioned previously, the first two event types in Figure 1 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 2 identifies the six level 2 categories for the event type identified in level 1 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 in order 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 and the number of occurrences is necessary for managing these OpRisks.

Figure 2: 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 Basel II category listed in Figure 1 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 3 provides the level 2 subcategories with examples for the CPBP category.

Figure 3: 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 II 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 p.m. EST. 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 II level 1 *External Fraud* category 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 II level 1 *Internal Fraud* category also 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 II 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 OpRisk 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.

Collecting and Reporting Internal Loss Data

LO 42.2: Summarize the process of collecting and reporting internal operational loss data, including the selection of thresholds, the timeframe for recoveries, and reporting expected operational losses.

The foundation of an OpRisk framework is the internally created loss database. Any event that meets a firm's definition of an operational risk event should be recorded in the loss event database and classified based on guidelines in the operational risk event policy. Many firms adopt Basel II categories at the highest level and then customize lower level entries to match their firm's specific needs. A minimum of five years of historical data is required to satisfy Basel II regulatory guidelines. Collecting and analyzing operational risk events provides valuable insights into a firm's operational risk exposures. When loss data is not collected, it could be perceived by regulators that operational risk management issues are not a concern. Usually once a firm begins to collect loss data, the organization gains a new appreciation of its operational risks.

The collection of data is challenging because large amounts of data must be gathered over diverse geographical areas. The process of gathering data must ensure that it accurately reflects all loss information from all locations. The process should have checks and balances to ensure human errors are not present in gathering data and sending it to the central data collection point. Basel II regulations require a high degree of reliability in the loss data flow from all areas of the financial institution.

Financial institutions often create OpRisk filters to identify potential operational events used in the calculation of operational losses. These OpRisk filters are typically the most expensive cost in the process. However, filters provide important added assurance for regulators regarding the accuracy of the data collection process.

Basel II requirements allow financial institutions to select a **loss threshold** for loss data collection. This threshold amount will have significant implications for the risk profile of business units within the firm. OpRisk managers should not set the threshold for collecting loss data too low (e.g., $0) if there are business units that have a very large number of smaller losses, because it would require a very high amount of reporting. OpRisk managers should also not just think in terms of large OpRisk threshold amounts. The following example illustrates how setting a threshold too high will bias the total losses and therefore the risk profile for a financial institution.

Suppose the OpRisk manager for Bank XYZ sets the threshold at $50,000. Bank XYZ categorized all losses by the amount of the loss into loss brackets or buckets illustrated in Figure 4. The first row of Figure 4 states that there were two losses greater than $4,000,000 in the past year and the total amount of loss from these two events was $18,242,000. These two losses accounted for 25.3% of the total losses for the year. If a loss threshold was set at $50,000, then the last two rows or 28.3% of the total losses for the year would not be reported. Therefore, if the firm did not set a loss threshold for collecting data they would show that they actually had $72,136,148 of total losses instead of $51,724,314 (computed as $72,136,148 – $4,480,627 – $15,931,207).

Figure 4: Bank XYZ Total Annual Losses

Loss Bracket	*Events*	*Loss Amount*	*Percentage*
Over $4,000,000	2	$18,242,000	25.3%
$1,000,000 to $4,000,000	8	$17,524,400	24.3%
$500,000 to $1,000,000	9	$7,850,425	10.9%
$250,000 to $500,000	7	$1,825,763	2.5%
$100,000 to $250,000	10	$1,784,632	2.5%
$75,000 to $100,000	15	$1,948,971	2.7%
$50,000 to $75,000	18	$2,548,123	3.5%
$25,000 to $50,000	50	$4,480,627	6.2%
Less than $25,000	1230	$15,931,207	22.1%
Total		$72,136,148	100.0%

When quantifying capital requirements, Basel II does not allow **recoveries** of losses to be included in the calculation. Regulators require this rule because gross losses are always considered for capital calculations to provide a more realistic view of the potential of large losses that occur once every 1,000 years.

Another important issue to consider in the process of collecting loss data is the **timeframe for recoveries**. The financial crisis of 2007–2009 illustrated that the complexity of some loss events can lead to very long time horizons from the start of the loss event to the final closure. Complex litigation cases from this financial crisis took five to six years for resolutions. Sometimes loss events will take lawyers and OpRisk managers several years to estimate the loss amount.

While firms could create reserves for these losses, they seldom do to avoid giving the impression that they may owe a certain amount prior to reaching a judgment. The fact that many firms do not have legal expertise within the firm to handle these complex cases adds to the cost, because outsourcing of lawyers is often required. It is important for firms to have a policy in place for the processing of large long timeframe losses.

To help firms know what to report, the International Accounting Standards Board (IASB) prepared IAS37, which establishes guidelines on **loss provisions** or the reporting of expected operational losses after the financial crisis in 2007–2009. Three important requirements for the reporting of expected operational losses are as follows:

1. Loss provisions are not recognized for future operating losses.

2. Loss provisions are recognized for onerous contracts where the costs of fulfilling obligations exceed expected economic benefits.

3. Loss provisions are only recognized for restructuring costs when a firm has a detailed restructuring plan in place.

The IAS37 report states that loss provisions of restructuring costs should not include provisions related to relocation of staff, marketing, equipment investments, or distribution investments. Loss provisions must be recognized on the balance sheet when the firm has a current obligation regarding a past loss event. Balance sheet reporting of loss events is required when the firm is likely to be obligated for a loss and it is possible to establish a reliable estimate of the amount of loss. Gains from the disposal of assets or expected reimbursements linked to the loss should not be used to reduce the total expected loss amount. Reimbursements can only be recognized as a separate asset.

Identifying, Controlling, and Assessing Operational Risk

LO 42.3: Explain the use of a Risk Control Self-Assessment (RCSA) and key risk indicators (KRIs) in identifying, controlling, and assessing operational risk exposures.

The control environment plays an important role in mitigating operational losses. The OpRisk manager should map each business unit's processes, risks, and control mechanisms associated with the processes. For example, Figure 5 illustrates the equity settlement process for an equity trading firm. All major processes for the business unit are identified as the first step in managing risks.

Figure 5: Equity Settlement Process

A **risk control self-assessment** (RCSA) requires the documentation of risks and provides a rating system and control identification process that is used as a foundation in the OpRisk framework. Once the RCSA is created, it is commonly performed every 12–18 months to assess the business unit's operational risks. It is common for financial institutions to seek

expert opinions to help provide qualitative measures for the effectiveness of the RCSA framework. The experts perform an evaluation and color rate the performance in each process as Red, Amber, or Green (RAG) to indicate the level of risk based on historical process data.

The following four steps are commonly used in designing an RCSA program:

1. *Identify and assess risks* associated with each business unit's activities. The manager first identifies key functions in the firm and performs risk scenarios to assess potential losses, the exposure or potential loss amount, and the correlation risk to other important aspects of the firm such as financial, reputation, or performance.

2. *Controls* are then added to the RCSA program to mitigate risks identified for the firm. The manager also assesses any residual risk which often remains even after controls are in place.

3. *Risk metrics,* such as key risk indicators or internal loss events, are used to measure the success of OpRisk initiatives and are linked to the RCSA program for review. These risk metrics would also include all available external data and risk benchmarks for operational risks.

4. *Control tests* are performed to assess how effective the controls in place mitigate potential operational risks.

A major challenge for OpRisk managers is the ability to properly interpret output data of the aggregated RCSA framework. Outputs could give managers a false sense of security if risks are controlled within tolerances that are set too high. Alternatively, risk managers may weight some risks more heavily and take corrective actions that focus too intensively on specific "key" measures while spending too little focus on other important variables.

Key risk indicators (KRIs) are identified and used to quantify the quality of the control environment with respect to specific business unit processes. KRIs are used as indicators for the OpRisk framework in the same way that other quantitative measures are used in market and credit risk models. The collection of reliable data used as KRIs is an important aspect of the self-assessment process. The data collection process may be automated to improve the accuracy of the data, but there will be costs associated with implementation. Even though KRIs may be costly to measure, they provide the best means for measuring and controlling OpRisk for the firm.

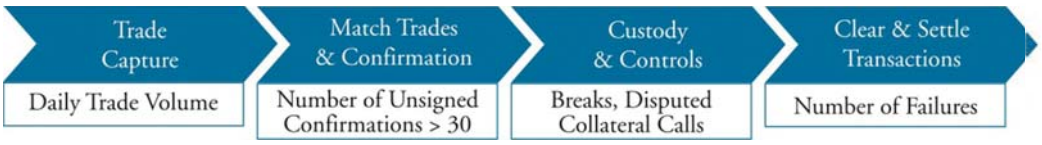
Regulators prefer the use of accurate quantitative KRIs in a control environment over more qualitative measures that only indicate whether the firm is getting better or worse based on historical losses. The more qualitative measures used in the example of the equity trading process in Figure 5 can be expanded to incorporate quantitative KRIs. Figure 6 includes examples of KRIs for the equity settlement process to help the firm self-assess the quality of the risk control environment.

The first step in creating an OpRisk model is identifying key factors that may be driving the success or failure of a business process. For example, the daily trade volume may be an important measure used to quantify how well the firm is executing the trade capture process. During the exercise of identifying KRIs, assumptions are made to determine proxies or inputs that drive the process. For example, execution errors are assumed to be greater

on high volume days. Other examples of KRIs that are used to predict execution errors are the number of securities that were not delivered, trading desk head count, and system downtime.

An important KRI for the process of matching trades and confirmation is the number of unsigned confirmations. KRIs are used as warning lights or red flags that highlight possible concerns for the firm. For example, when the number of unsigned confirmations older than 30 days as a percentage of total confirmations exceeds target percentages it indicates a problem area in the confirmation process. Similarly, the number of disputed collateral calls may be a good KRI for the custody and control step. Finally, the number of transactions that failed to clear or settle may be a good KRI for the settlement process.

Figure 6: Key Risk Indicators for an Equity Trading Firm



Collecting data at the lowest level or the cost center level allows information to be aggregated for all locations. This is very advantageous for the RCSA program because the OpRisk manager is then able to drill down or disaggregate the total data for the firm to help pinpoint where potential concerns may be originating.

Some additional examples of common internal control factors that are used to explain specific business environments are summarized in Figure 7.

Figure 7: Examples of Business Environment and Internal Control Factors (BEICFs)

Business Environment	*Factor Description*
Systems	Minutes system is down or slow
Information Security	Number of malware or hacking attacks
People	Headcount of employees, experience
Execution/Processing	Number of transactions or transaction breaks

External data such as stock market indices and market interest rate levels are also used in RCSA frameworks. For example, increased volatility in the equity market can lead to higher volume and higher operational losses for the firm. The insurance industry often relies on external databases to gather information on accidents or losses for areas or geographical regions they are less familiar with. Banks may also use external databases to gather information regarding losses for risks they have not been exposed to and therefore lack any relevant internal data.

Three common methods of gathering external data are: internal development, consortia, and vendors. Under the internal development method, the firm gathers and collates information from media such as news or magazines. This may be the least expensive method, but it may not be as accurate and has the potential to overlook large amounts of relevant data. The most popular consortium for banks is the **Operational Riskdata eXchange Association** (ORX), which contains large banks in the financial industry. While

this consortium has a relatively low loss reporting threshold, there are often no details on the losses and therefore this data can only be used for measurement. There are a number of vendors who provide detailed analysis on losses that can be used for scenario analysis. However, the loss threshold for vendor data is often much higher and the information may not always be accurate.

Scenario Analysis

LO 42.4: Describe and assess the use of scenario analysis in managing operational risk, and identify biases and challenges that can arise when using scenario analysis.

Scenario analysis is defined as the process of evaluating a portfolio, project, or asset by changing a number of economic, market, industry, or company specific factors. Scenario analysis models are especially useful tools for estimating losses when loss experiences related to emerging risks are not available to the financial institution. Inputs to scenario analysis models are collected from external data, expert opinions, internal loss trends, or key risk indicators (KRIs). Expert opinions are typically drawn from structured workshops for large financial institutions. However, surveys and individual meetings can also be used to gather expert advice. Studies suggest that most financial firms analyze between 50 and 100 scenarios on an annual basis.

One of the challenges in scenario analysis is taking expert advice and quantifying this advice to reflect possible internal losses for the firm. The following example illustrates how a firm may create a frequency distribution of loss events that can be used in scenario analysis.

Figure 8 illustrates data constructed for a financial institution based on expert inputs. Information is gathered on loss frequencies for pre-determined loss brackets. Thus, a frequency distribution is created to model the probability of losses based on the amount of loss on an annual basis. This frequency distribution is then used in the OpRisk framework for the firm.

Figure 8: Scenario Analysis Model for Loss Frequencies

Loss Bracket	*Number of Losses*	*Frequency*
Over $5,000,000	3	1.8%
$1,000,000 to $5,000,000	9	5.4%
$500,000 to $1,000,000	18	10.7%
$250,000 to $500,000	25	14.9%
$100,000 to $250,000	41	24.4%
$50,000 to $100,000	72	42.9%
Total	168	100.0%

Biases and Challenges of Scenario Analysis

One of the biggest challenges of scenario analysis is the fact that expert opinions are always subject to numerous possible biases. There is often disparity of opinions and knowledge regarding the amount and frequency of losses. Expert biases are difficult to avoid when conducting scenario analysis. Examples of possible biases are related to presentation, context, availability, anchoring, confidence, huddle, gaming, and inexpert opinion.

Presentation bias occurs when the order that information is presented impacts the expert's opinion or advice. Another similar type of bias is **context bias**. Context bias occurs when questions are framed in a way that influences the responses of those being questioned. In the case of scenario analysis, the context or framing of questions may influence the response of the experts.

Another set of biases are related to the lack of available information regarding loss data for a particular expert or for all experts. **Availability bias** is related to the expert's experience in dealing with a specific event or loss risk. For example, some experts may have a long career in a particular field and never actually experience a loss over $1 billion. The availability bias can result in over or under estimating the frequency and amount of loss events. A similar bias is referred to as anchoring bias. **Anchoring bias** can occur if an expert limits the range of a loss estimate based on personal experiences or knowledge of prior loss events. The availability an expert has to information can also result in a **confidence bias**. The expert may over or under estimate the amount of risk for a particular loss event if there is limited information or knowledge available for the risk or the probability of occurrence.

Expert opinions are often obtained in structured workshops that have a group setting. This group setting environment can lead to a number of biases. **Huddle bias** (also known as **anxiety bias**) refers to a situation described by behavioral scientists where individuals in a group setting tend to avoid conflicts and not express information that is unique because it results from different viewpoints or opinions. An example of a huddle bias would be a situation where junior experts do not voice their opinions in a structured workshop because they do not want to disagree in public with senior experts. Another concern for group environments is the possibility of **gaming**. Some experts may have ulterior motives for not participating or providing useful information in workshops. Another problem with workshop settings is the fact that top experts in the field may not be willing to join the workshop and prefer to work independently. The lack of top experts then attracts less experienced or junior experts who may have an **inexpert opinion**. These inexpert opinions can then lead to inaccurate estimates and poor scenario analysis models.

One technique that can help in scenario analysis is the **Delphi technique**. This technique originated from the U.S. Air Force in the 1950s and was designed to obtain the most reliable consensus of opinions from a group of experts. This technique is useful for many applications for analyzing cases where there is limited historical data available. More specifically, the Delphi technique is often applied in situations that exhibit some of the following issues:

- Precise mathematical models are not available but subjective opinions can be gathered from experts.
- Experts have a diverse background of experience and expertise, but little experience in communicating within expert groups.

- Group meetings are too costly due to time and travel expenses.
- A large number of opinions is required and a single face-to-face meeting is not feasible.

Under the Delphi technique, information is gathered from a large number of participants across various business units, areas of expertise, or geographical regions. The information is then presented in a workshop with representatives from each area. Recommendations are determined by this workshop group and quantified based on a pre-determined confidence level. A basic Delphi technique commonly goes through the following four steps:

1. Discussion and feedback is gathered from a large number of participants who may have diverse exposure and experience with particular risks.

2. Information gathered in step 1 is summarized and presented to a workshop group with representatives from various locations or business units surveyed.

3. Differences in feedback are evaluated from step 2.

4. Final evaluation and recommendations are made based on analysis of data and feedback from participants and/or respondents.

Operational Risk Profiles

LO 42.5: Compare the typical operational risk profiles of firms in different financial sectors.

Various business units within a financial institution are identified separately in an OpRisk profile. This allows the OpRisk manager to gather data for specific risks of each business unit. For example, an asset management unit typically has greater legal liability problems whereas an investment bank unit has more losses associated with transaction processing operational errors.

Basel II defines level 1 business units into the following categories: Trading and Sales, Corporate Finance, Retail Banking, Commercial Banking, Payment and Settlement, Agency Services, Asset Management, and Retail Brokerage. Large financial institutions typically define business units within their firm based on these Basel II definitions.

Figures 9 and 10 contrast the OpRisk profiles for five of these financial business units with respect to frequency and severity, respectively. The first columns of Figure 9 and Figure 10 summarize the type of event risk for each business unit. The frequency percentages based on the number of loss events are presented for each business unit in Figure 9. The severity percentages based on total dollar amount losses are presented for each business unit in Figure 10.

Figure 9: OpRisk Profiles Showing Frequency (%)

Event Type	*Trading & Sales*	*Corporate Finance*	*Retail Banking*	*Asset Management*	*Retail Brokerage*
Internal Fraud	1.0%	1.6%	5.4%	1.5%	5.8%
External Fraud	1.0%	5.4%	**40.3%**	2.7%	2.3%
Employment Practices	3.1%	10.1%	17.6%	4.3%	4.4%
Clients, Products, & Business Practices	**12.7%**	**47.1%**	**13.1%**	**13.7%**	**66.9%**
Physical Asset Damage	0.4%	1.1%	1.4%	0.3%	0.1%
System Failures & Business Disruptions	5.0%	2.2%	1.6%	3.3%	0.5%
Execution, Delivery, & Process Mgt	**76.7%**	**32.5%**	**20.6%**	**74.2%**	**20.0%**

Source: 2008 Loss Data collection exercise for Operational Risk BCBS (2009)

Figure 10: OpRisk Profile Showing Severity (%)

Event Type	*Trading & Sales*	*Corporate Finance*	*Retail Banking*	*Asset Management*	*Retail Brokerage*
Internal Fraud	11.0%	0.2%	6.3%	11.1%	18.1%
External Fraud	0.3%	0.1%	**19.4%**	0.9%	1.4%
Employment Practices	2.3%	0.6%	9.8%	2.5%	6.3%
Clients, Products, & Business Practices	**29.0%**	**93.7%**	**40.4%**	**30.8%**	**59.5%**
Physical Asset Damage	0.2%	0.0%	1.1%	0.2%	0.1%
System Failures & Business Disruptions	1.8%	0.0%	1.5%	1.5%	0.2%
Execution, Delivery, & Process Mgt	**55.3%**	**5.4%**	**21.4%**	**52.8%**	**14.4%**

Source: 2008 Loss Data collection exercise for Operational Risk BCBS (2009)

The two categories with the largest percentage of losses are emphasized in bold across different business units. The *Clients, Products, and Business Practices (CPBP)* unit and the *Execution, Delivery, and Process Management (EDPM)* unit have the largest losses across business units in terms of both frequency and severity of losses.

The number of losses related to the EDPM unit represented the highest frequency percentage and severity percentage for the *Trading and Sales* business unit in a 2008 survey of financial institutions. This is expected based on the number of trades executed daily by this business unit. Within this business unit, traders are required to execute trades for their firm or clients and then later settle the transactions. The complexity and wide range of products processed increases the possibility that errors may occur in the process. There is also a high frequency percentage and severity percentage related to the CPBP unit. Losses within this category arise from client or counterparty disputes, regulatory fines, and improper advisory activities.

The *Corporate Finance* business unit primarily provides consulting regarding initial public offerings, mergers and acquisitions, and other strategic planning. Figure 10 suggests that

over 93% of losses fall under the CPBP category. The majority of losses are from litigation from clients arguing IPOs were mispriced or some other improper advice.

The *Retail Banking* unit has the highest frequency of losses associated with external frauds at 40%. However, external fraud accounts for only about 20% of the total severity percentage. The largest severity percentage for the retail banking sector is the *Clients, Products, and Business Practices* category with *Execution, Delivery, and Process Management* as the next highest category.

Prior to the financial crisis of 2007–2009, *Asset Management* firms had steady increases in assets under management (AUM) as profits were realized across most financial markets in the bull market. Thus, most asset managers did not focus on operational costs. Conversely, after the crisis all costs became extremely important as AUM were reduced by as much as 40%. The lack of proper controls increased the losses beyond market related losses.

In addition to the financial crisis, one litigation case reached an unprecedented level and brought an added demand for increased controls. Bernie Madoff's Ponzi scheme caused many individuals to lose all of their investments and pension savings. These events have led to dramatic increases in OpRisk controls for the asset management industry. The asset management industry reduced operational costs by consolidating administration and distribution departments for large geographical regions. In addition, more focus is now concentrated toward reducing operational costs and risk management. Productivity has also seen changes as illustrated by select financial firms significantly reducing the number of products offered to focus on fewer products on a global scale.

OpRisk, market risk, and credit risk are all concerns for asset management firms. However, economic losses are largely due to OpRisk losses, because credit and market risks do not have an immediate impact on manager fee income. The OpRisk profile for asset management firms reveals the largest frequency and severity percentage in the *Execution, Delivery, and Process Management* area.

The OpRisk profile for firms in the *Retail Brokerage* industry can vary to some extent due to the wide range of business strategies ranging from online to brick-and-mortar broker-dealers. Changes in technologies have significantly increased the speed of trading and clients of broker-dealers now have direct market access through trading tools. Clients such as hedge funds, mutual funds, insurance companies, or wealthy individuals are able to directly access markets using the broker-dealer's market participant identifier (MPID). This greatly increases the operational risk for broker-dealers who are responsible for all trades made with their MPID. If trades are not filtered by the broker-dealer, then the risks are even greater.

For example, due to the high speed of trades driven by algorithms and large blocks of trades, a two-minute delay in detecting a mistake could lead to losses approaching three-quarters of a billion dollars. Thus, it is important to integrate pre-trade controls into the system to mitigate the risk of mistakes or entry errors. The OpRisk profile of the retail brokerage industry has the largest frequency and severity percentage in the *Clients, Products, and Business Practices* area.

There was no loss frequency or severity data provided for the *Insurance* sector. Perhaps this is due to the fact that firms in the insurance industry are still in the early stages of developing accurate OpRisk frameworks and there is no data available. The insurance sector

is divided into three major insurance types: life, health, and property and casualty. The insurance industry collects premiums for insuring individual losses and the insurer pays for losses incurred by policyholders, thus reducing the possibility of a large loss for any one individual.

In order to properly price the premiums, the insurer must have accurate actuarial calculations. In fact, OpRisk capital requirement models determined by regulators are designed after actuarial calculation models in the property and casualty insurance industry. Some major OpRisks for insurers include misselling products to clients, fraudulent sales techniques, customer frauds, discrimination litigation, and incomplete policy litigation following the 9/11 attacks.

Organizational Structures for Risk Governance

LO 42.6: Explain the role of operational risk governance and explain how a firm's organizational structure can impact risk governance.

A key factor in creating a successful OpRisk framework is the organizational design of the risk management framework. Developing an understanding of reporting lines is just as important as developing good measurement tools and key risk indicators. All stakeholders for the organization should be informed of the OpRisk framework to help ensure that data is collected accurately and reflects the systems in place. The way in which risk is managed in an organization and the internal governance is an important aspect of OpRisk management.

There are four main organizational designs for integrating the OpRisk framework within the organization. Most large firms start at design 1 and progress to design 4 over time. The four organizational designs are illustrated in Figure 11 and summarized below.

Design 1: Central Risk Function Coordinator

In the first risk organizational design, the risk manager is viewed more as a coordinator or facilitator of risk management. This risk management design typically involves only a small Central Risk group who is responsible for OpRisk management. The risk manager gathers all risk data and then reports directly to the Chief Executive Officer (CEO) or Board of Directors. Regulators believe there exists a conflict of interest for reporting risk data directly to management or stakeholders that are primarily concerned with maximizing profits. Thus, this design can only be successful if business units are responsive to the Central Risk function without being influenced by upper management who controls their compensation and evaluates their performance.

Design 2: Dotted Line or Matrix Reporting

Creating a link or dotted line from the business risk managers to the Central Risk function of the organization is the next natural progression in risk organizational design. The dotted line implies that business unit managers are still directly under the influence of the CEO who controls their compensation and evaluates their performance. Thus, this type of framework is only successful if there is a strong risk culture for each business unit that

encourages collaboration with the Central Risk function. Furthermore, this dotted line structure is preferred when there is a culture of distrust of the Central Risk function based on some historical events.

Design 3: Solid Line Reporting

For larger firms that have centralized management, the solid line reporting is more popular. The solid line indicates that each business unit has a risk manager that reports directly to the Central Risk function. This design enables the Central Risk function to more effectively prioritize risk management objectives and goals for the entire firm. The solid line reporting also creates a more homogeneous risk culture for the entire organization.

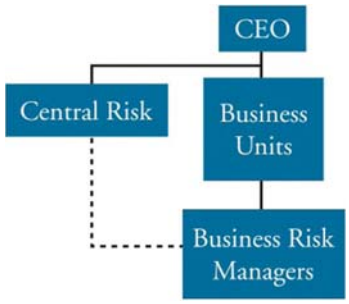
Design 4: Strong Central Risk Management

Many large firms have evolved into a strong central risk management design either voluntarily or from regulatory pressure. Under this design, there is a Corporate Chief Risk Officer who is responsible for OpRisk management throughout the entire firm. The Central Risk Manager monitors OpRisk in all business units and reports directly to the CEO or Board of Directors. Regulators prefer this structure as it centralizes risk data which makes regulatory supervision easier for one direct line of risk management as opposed to numerous risk managers dispersed throughout various business units of the firm.

Figure 11: Risk Department Organizational Designs

1. Central Risk Function Coordinator

2. Matrix Reporting (Dotted Line)



3. Central Risk Management (Solid Line)

4. Strong Central Risk Management

Key Concepts

LO 42.1

Basel II classifies loss events into seven categories. Loss events in the Execution, Delivery, and Process Management category have a small dollar amount but a very large frequency of occurrence. Losses are more infrequent but very large in the Clients, Products, and Business Practices category.

LO 42.2

Thresholds for collecting loss data should not be set too low if there are business units that have a very large number of smaller losses. Another important issue to consider in the process of collecting loss data is the timeframe for recoveries. Time horizons for complex loss events can stretch out for as much as five years or longer.

The International Accounting Standards Board (IASB) prepared IAS37, which states that loss provisions: (1) are not recognized for future operating losses, (2) are recognized for onerous contracts where the costs of fulfilling obligations exceed expected economic benefits, and (3) are only recognized for restructuring costs when a firm has a detailed restructuring plan in place.

LO 42.3

Risk control self-assessment (RCSA) requires the assessment of risks that provides a rating system and control identification process for the OpRisk framework. Key risk indicators (KRIs) are used to quantify the quality of the control environment with respect to specific business unit processes.

LO 42.4

Expert opinions are drawn from structured workshops and used as inputs in scenario analysis models. A challenge for scenario analysis is that these expert opinions may contain the following biases: presentation, context, availability, anchoring, huddle, gaming, confidence, and inexpert opinion.

LO 42.5

In general, the Clients, Products, and Business Practices unit and the Execution, Delivery, and Process Management unit have the largest losses based on OpRisk profiles across financial sectors in terms of severity and frequency of losses.

LO 42.6

There are four main organizational designs for integrating an OpRisk framework. Most large firms evolve from design 1 to design 4 over time. The primary difference in the designs is how risk is reported and the link between separate business unit risk managers and the Central Risk function.

Concept Checkers

1. Suppose a broker-dealer has a loss that occurs from a failure in properly processing and settling a transaction. According to Basel II operational risk categories, this type of event loss would be categorized as:
   A. Business Disruption and System Failures.
   B. Clients, Products, and Business Practices.
   C. Execution, Delivery, and Process Management.
   D. Employment Practices and Workplace Safety.

2. There are typically four steps used in designing the risk control self-assessment (RCSA) program for a large firm. Which of the following statements is least likely to be a step in the design of that program?
   A. Identify and assess risks associated with each business unit's activities.
   B. Controls are added to the RCSA program to mitigate risks identified for the firm.
   C. Risk metrics and all other OpRisk initiatives are linked to the RCSA program.
   D. Reports to regulators are prepared that summarize the degree of OpRisk.

3. Scenario analysis is often used by financial institutions in determining the amount and frequency of losses. Because historical data is often limited for all possible losses, the opinions of experts are often obtained from workshops. These expert opinions are often subject to biases. Which of the following biases refers to the problem that can arise in this group setting where an expert may not be willing to share a conflicting opinion?
   A. Huddle bias.
   B. Context bias.
   C. Availability bias.
   D. Anchoring bias.

4. Based on OpRisk profiles across financial sectors, which of the following loss event type categories have the highest frequency and severity of losses?
   A. Business Disruption and System Failures.
   B. Clients, Products, and Business Practices.
   C. External Fraud.
   D. Internal Fraud.

5. Which of the following risk organizational design frameworks is preferred by regulators?
   A. Central risk function coordinator.
   B. Matrix reporting using dotted lines.
   C. Solid line reporting to central risk management.
   D. Strong central risk management.

Concept Checker Answers

1. C Basel II classifies losses from failed transaction processing or process management from relations with trade counterparties and vendors under the Execution, Delivery, and Process Management category.

2. D The last step in the design of a risk control self-assessment (RCSA) program involves control tests to assess how well the controls in place mitigate potential risks.

3. A Huddle bias suggests that groups of individuals tend to avoid conflicts that can result from different viewpoints or opinions. Availability bias is related to the expert's experience in dealing with a specific event or loss risk. Anchoring bias occurs when an expert limits the range of a loss estimate based on personal knowledge. Context bias occurs when questions are framed in a way that influences the responses of those being questioned.

4. B From the choices listed the Clients, Products, and Business Practices unit has the highest frequency percentages and severity of loss percentages across business units. The Execution, Delivery, and Process Management unit also has large losses across business units in terms of frequency and severity of losses, however, this category was not listed as a possible choice.

5. D Regulators prefer the strong central risk management design because they can streamline their supervision over one direct line of risk management as opposed to numerous risk managers throughout the firm.