READING 3: CORPORATE GOVERNANCE AND RISK MANAGEMENT

Crouhy, Galai, and Mark, Chapter 4

EXAM FOCUS

This reading continues the coverage of risk management concepts in a qualitative and non-technical manner. For the exam, pay close attention to the best practices in corporate governance and risk management. In addition, understand the purpose and function of the main board committees, such as risk management, compensation, and audit.

MODULE 3.1: CORPORATE GOVERNANCE AND RISK MANAGEMENT

LO 3.a: Compare and contrast best practices in corporate governance with those of risk management.

Corporate Governance

The board of directors should be comprised of a majority of independent members in order to maintain a sufficient level of objectivity with regard to making decisions and approving management's decisions. All members should possess a basic knowledge of the firm's business and industry, even if they are outside of the industry. Additionally, those who lack knowledge should be provided some supplemental training prior to joining the board.

The board should be watching out for the interests of the shareholders. For example, on a general level, the board would have to approve management's decision to assume a certain risk given its expected return. Also, the board would watch out for the interests of other stakeholders, such as debtholders, by considering if any of management's decisions contain extreme downside risk.

The board should be aware of any agency risks whereby management may have the incentive to take on greater risks in order to maximize personal remuneration (e.g., based on short-term increases in stock price) that are not consistent with the objectives of the stakeholders in terms of long-term risk levels. As a starting point, the compensation committee within the board should design management compensation plans so they are congruent with corporate goals in addition to minimizing or reducing agency risk.

The board should maintain its independence from management. A key measure involved would be that the chief executive officer (CEO) would not also be the chairman of the board because there is already an inherent conflict with the CEO being on both the management

team and the board of directors. As a result, the CEO should not be given additional powers on the board.

The board should consider the introduction of a chief risk officer (CRO). The CRO would technically be a member of management but would attend board meetings. The CRO's objective would be to link the corporate governance duties to the firm's risk management objectives. In terms of reporting, the CRO could report to the board and/or the management team, depending on the specific nature of the CRO role within the firm.

Risk Management

The board of directors should demand substance over form. For example, business and risk management strategies should strive for economic performance, not accounting performance. To promote a robust risk management process within the firm, the board should ensure sufficient upward mobility in terms of risk management careers, appropriate staff remuneration, and logical reporting relationships.

The board should set up an ethics committee (either within the board or within the firm) to require all staff to adhere to the firm's high ethical standards. The committee could also be responsible for monitoring duties to ensure that those standards are upheld.

Similar to the issue of agency risk under corporate governance, the board should ensure that performance measurement and compensation for all staff is consistent with the firm's goals and the shareholders' interests. Specifically, compensation should be determined based on performance on a risk-adjusted basis.

The board must provide approval on all major transactions after ensuring the transactions are within the established risk appetite and consistent with the firm's overall business strategy. In addition, the board should be prepared to pose probing and relevant questions to management and other staff in the context of professional skepticism. Corroborating information from a variety of sources and staff should increase the reliability and validity of the answers obtained.

The board should have a risk committee in place. Similar to the corporate governance best practice of having all members possessing a basic knowledge of the firm's business and industry, all risk committee members need to understand the technical risk issues (e.g., risk appetite, relevant time period) in order to ask appropriate questions and make informed decisions.

The risk committee should be separate from the audit committee given the different knowledge base and skills required in each area. However, it may be useful to have at least one board member on both committees to ensure that the committees are working toward the same corporate objectives.

LO 3.b: Assess the role and responsibilities of the board of directors in risk governance.

LO 3.d: Distinguish the different mechanisms for transmitting risk governance throughout an organization.

In terms of risk governance, the board has some important responsibilities that could be facilitated with the involvement of a risk advisory director. Given the specialized role of the

risk management and compensation committees, the specific duties of the risk advisory director are highlighted here.

Risk Advisory Director

A risk advisory director would be a board member who is a risk specialist who attends risk committee and audit committee meetings and provides advice to increase effectiveness. The risk advisory director also meets with senior management on a regular basis and could be viewed as a liaison between the board and management. Overall, the role would involve educating members on best practices in both corporate governance and risk management.

More specific duties of the director (and the board in general) would include the review and analysis of the following:

- The firm's risk management policies.
- The firm's periodic risk management reports.
- The firm's risk appetite and its impact on business strategy.
- The firm's internal controls.
- The firm's financial statements and disclosures.
- The firm's related parties and related party transactions.
- Any audit reports from internal or external audits.
- Corporate governance best practices for the industry.
- Risk management practices of competitors and the industry.

Risk Management Committee

Using a bank as an example, the risk management committee (within the board) is responsible for identifying, measuring, and monitoring financial risks (i.e., credit, market, liquidity). The committee is responsible for approving credit facilities that are above certain limits or within limits but above a specific threshold. In addition, the committee monitors the composition of the bank's lending and investment portfolios in light of the current economic environment in terms of credit, market, and liquidity risk to determine if any changes in the portfolio composition are required.

The risk management committee usually maintains an open line of communication with the external audit, internal audit, and management teams.

Compensation Committee

As discussed previously, the existence of agency risk necessitates the board to implement a compensation committee to ensure appropriate risk taking in relation to the long-term risks assumed. The compensation committee is independent of management. Its role is to discuss and approve the remuneration of key management personnel.

Management compensation above base salary should be congruent with the goals of the other stakeholders. In that regard, the committee should avoid designing compensation plans with bonuses based on short-term profits or revenues given the relative ease in which management may manipulate those amounts. Also, there could be the absence of any guaranteed bonuses or a cap could be implemented on bonuses. Furthermore, the committee may consider

introducing elements of downside risk with management compensation. For example, compensation may be deferred until longer-term results are known or there could be clawbacks of previous bonuses paid if long-term results are inconsistent with short-term results.

Stock-based compensation is a potential solution to align management and shareholder interests. However, it is not a perfect solution because there is still potential for management to take excessive risks; their upside potential is theoretically unlimited based on the stock price increase but their downside potential is limited if the stock becomes worthless. Another idea would be to provide "bonus bonds" as compensation that would be taken away should a specific regulatory ratio requirement be breached.

Audit Committee

LO 3.f: Assess the role and responsibilities of a firm's audit committee.

The audit committee (as part of the board) has traditionally been responsible for the reasonable accuracy of the firm's financial statements and its regulatory reporting requirements. It must ensure that the firm has taken all steps to avoid the risk that the financial statements are materially misstated as a result of undiscovered errors and/or fraud. In addition to the more visible verification duties, the audit committee monitors the underlying systems in place regarding financial reporting, regulatory compliance, internal controls, and risk management. In that respect, the audit committee may be able to rely on some or all of the work of the internal audit team, which usually reports directly to the audit committee.

All members of the audit committee must possess sufficient financial knowledge in order to perform in their role. This requires an understanding of the relevant accounting rules (e.g., U.S. GAAP, IFRS), financial statements, and internal controls. As a collective, there should be a proper balance of independence, knowledge of the business, and ability to ask probing and relevant questions. The audit committee is largely meant to be independent of management but it should work with management and communicate frequently to ensure that any issues arising are addressed and resolved.

Finally, there should be responsibilities for the audit committee in terms of meeting minimum (or higher) standards in areas such as legal, compliance, and risk management. There could also be duties related to optimizing the firm's operations in terms of effectiveness and efficiency.

Risk Appetite and Business Strategy

LO 3.c: Evaluate the relationship between a firm's risk appetite and its business strategy, including the role of incentives.

A firm's risk appetite reflects its tolerance (especially willingness) to accept risk. The subsequent implementation of the risk appetite into defining the firm's risk limits sets some bounds to its business strategy and to its ability to exploit business opportunities. The board needs to develop/approve the firm's risk appetite as well as assist management in developing the firm's overall strategic plan.

There must be a logical relationship between the firm's risk appetite and its business strategy. As a result, business strategy planning meetings require input from the risk management team right from the outset to ensure the consistency between risk appetite and business strategy. For example, planning activities are often focused on maximizing the firm's profit but some planned activities may need to be eliminated or modified because they exceed the stated risk appetite. Furthermore, the scope of some planned activities may be too large in the context of the firm's total assets or equity. Consideration must also be given to the downside risks of any business strategy.

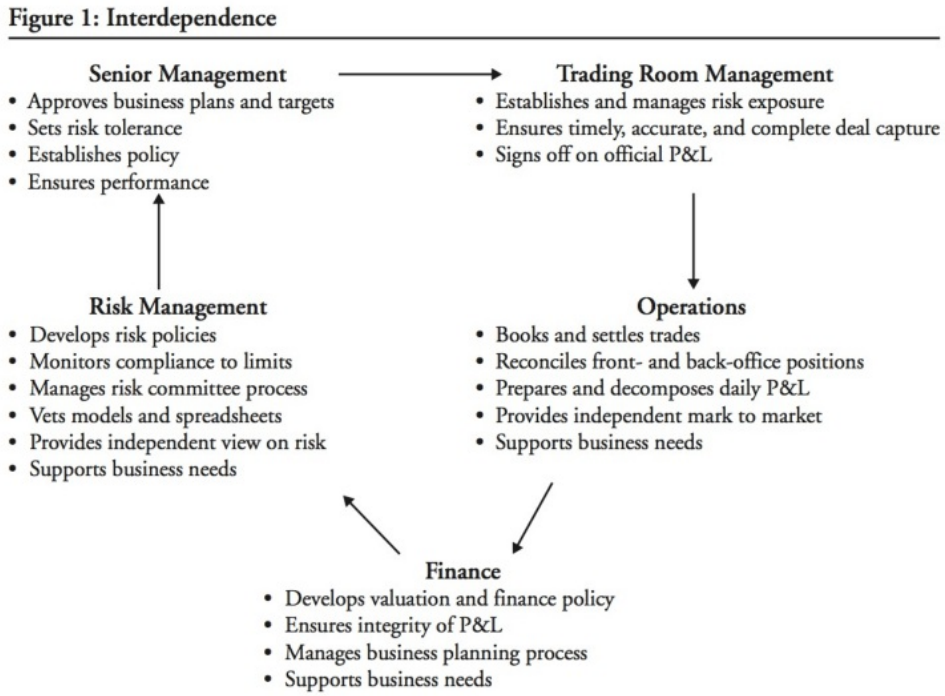
To make sure that a firm's risk management plan aligns risk appetite with business decisions, the firm should rely on its risk infrastructure while taking into account incentive compensation plans. An appropriate infrastructure should be in place to allow the firm to identify, evaluate, and manage all relevant risks. The results of incentive compensation plans should also be monitored to ensure that the firm's risk-adjusted return on capital meets the long-term expectations of stakeholders.

Interdependence of Functional Units

LO 3.e: Illustrate the interdependence of functional units within a firm as it relates to risk management.

The various functional units within a firm are dependent on one another when it comes to risk management and reporting. All transactions must be recorded correctly and in the appropriate period in order to ensure the accuracy of the periodic profit and loss (P&L) statements. Using an investment bank, consider five separate units: (1) senior management, (2) risk management, (3) trading room management, (4) operations, and (5) finance. The interdependence of managing risk among these functional units is illustrated in Figure 3.1.

Figure 3.1: Interdependence



Crouhy, M., Galai, D., & Mark, R. (2014). Chapter 4: Corporate Governance and Risk Management (Figure 4-2).

There are many examples of interdependence among the functional units. Overall, the operations unit is extremely important to all the other units in terms of generating and maintaining the data needed to manage risk. All trades are recorded and all reconciliations are performed within operations.

The finance unit develops valuation and finance policies. Those valuation policies are subsequently applied by the operations unit when it prepares asset valuations. The P&L statement (i.e., income statement) is developed by the operations and finance units and ultimately approved by trading room management. Note the consistent support of the bank's business needs by the risk management, operations, and finance units.

MODULE QUIZ 3.1

1. Which of the following statements about best practices in corporate governance and risk management is most accurate?
    A. The board should keep the risk committee separate from the audit committee.
    B. The board should ensure that it has the firm's chief risk officer as a member of the board.
    C. The board should focus on management's actions and their impact on the interests of the firm's shareholders.
    D. The board should focus on accounting performance instead of economic performance because of the importance of maintaining or enhancing the firm's stock price.

2. The role of the risk advisory director on the board is important in ensuring sufficient risk oversight of the firm by the board. Which of the following specific items would the risk advisory director review and analyze?
    I. Internal audit reports.
    II. Information on the firm's related parties.
    A. I only.
    B. II only.
    C. Both I and II.
    D. Neither I nor II.

3. Which of the following statements regarding the firm's risk appetite and/or its business strategy is most accurate?
    A. The firm's risk appetite does not consider its willingness to accept risk.
    B. The board needs to work with management to develop the firm's overall strategic plan.
    C. Management will set the firm's risk appetite and the board will provide its approval of the strategic plan.
    D. Management should obtain the risk management team's approval once the business planning process is finalized.

4. The various responsibilities surrounding the profit and loss (P&L) statement illustrate the importance of understanding the interdependence of managing risk within a firm. Within an investment bank, which functional unit is most likely to provide final approval of the P&L?
    A. Finance.
    B. Operations.
    C. Senior management.
    D. Trading room management.

5. Which of the following statements regarding the role of the firm's audit committee is most accurate?
    A. At least one member of the audit committee must possess sufficient financial knowledge.
    B. The audit committee may consist of some members of the management team.

C. The audit committee is only responsible for the accuracy of the financial statements.
D. The audit committee is meant to work dependently with management.

KEY CONCEPTS

LO 3.a

There are numerous best practices in corporate governance, including:

- Board is comprised of a majority of independent members with basic knowledge of the firm's business and industry.
- Board watches out for the interests of all stakeholders, including shareholders and debtholders who may have somewhat differing interests.
- Board is aware of any agency risks and takes steps to reduce them (e.g., compensation committee).
- Board maintains its independence from management (e.g., CEO is not the chairman of the board).
- Board should consider the introduction of a chief risk officer.

There are numerous best practices in risk management, including:

- Board should focus on the firm's economic performance over accounting performance.
- Board should promote a robust risk management process within the firm (e.g., upward mobility for risk management careers).
- Board should set up an ethics committee to uphold high ethical standards within the firm.
- Board should ensure that compensation is based on risk-adjusted performance.
- Board should approve all major transactions.
- Board should always apply professional skepticism to ask probing and relevant questions to management.
- Board should have a risk committee in place.

LO 3.b

The role of the board of directors in governance would include the review and analysis of:

- The firm's risk management policies.
- The firm's periodic risk management reports.
- The firm's appetite and its impact on business strategy.
- The firm's internal controls.
- The firm's financial statements and disclosures.
- The firm's related parties and related party transactions.
- Any audit reports from internal or external audits.
- Corporate governance best practices for the industry.
- Risk management practices of competitors and the industry.

LO 3.c

A firm’s risk appetite reflects its tolerance (especially willingness) to accept risk. There is subsequent implementation of the risk appetite into defining the firm’s risk limits. Ultimately, there must be a logical relationship between the firm’s risk appetite and its business strategy.

LO 3.d

Two mechanisms for transmitting risk governance throughout a firm are the audit committee of the board and the use of a risk advisory director. Additionally, the role of the risk management committee and the compensation committee further transmit risk governance.

LO 3.e

The various functional units within a firm are dependent on one another when it comes to risk management and reporting. Using an investment bank as an example, areas such as valuations, the profit and loss statement, and risk policy require input from more than one of the following units: (1) senior management, (2) risk management, (3) trading room management, (4) operations, and (5) finance.

LO 3.f

The audit committee is responsible for the reasonable accuracy of the firm’s financial statements and its regulatory reporting requirements. It must ensure that the firm has taken all steps to avoid the risk that the financial statements are materially misstated as a result of undiscovered errors and/or fraud. In addition to the more visible verification duties, the audit committee monitors the underlying systems in place regarding financial reporting, regulatory compliance, internal controls, and risk management.

ANSWER KEY FOR MODULE QUIZ

Module Quiz 3.1

1. **A** The risk committee should be separate from the audit committee given the different knowledge base and skills required in each area.

   Choice B is not correct because the firm's chief risk officer (CRO) is technically a member of management but does attend board meetings regularly. Although the CRO may report to management and/or the board, the CRO should not be a member of the board. Choice C is not correct because the board should consider the impact on all of the firm's stakeholders (i.e., debtholders, shareholders) and not just the shareholders. Choice D is not correct because the board should ensure that business and risk management strategies should strive for economic performance, not accounting performance. (LO 3.a)

2. **C** The risk advisory director should review and analyze internal audit reports and information on the firm's related parties because they are directly relevant in assessing the firm's risk level from the board's perspective. (LO 3.b)

3. **B** The board needs to develop/approve the firm's risk appetite as well as assist management in developing the firm's overall strategic plan.

   Choice A is not correct because the firm's risk appetite considers its willingness to accept risk. Choice C is not correct because both management and the board will set the firm's risk appetite. Choice D is not correct because management should involve the risk management team in the business planning process right from the outset to ensure the consistency between risk appetite and business strategy. (LO 3.c)

4. **D** Trading room management is responsible for signing off on the official P&L. Choice A is not correct because the finance unit ensures the integrity of the P&L. Choice B is not correct because the operations unit prepares and decomposes the daily P&L. Choice C is not correct because senior management does not have any responsibilities for the P&L from a risk management perspective. (LO 3.e)

5. **B** The audit committee consists primarily of non-management members but there may be some management members (e.g., chief financial officer).

   All members of the audit committee must possess sufficient financial knowledge. The audit committee is responsible for the accuracy of the financial statements but that alone does not comprise its main responsibility. Additionally, the audit committee monitors the underlying systems in place regarding financial reporting, regulatory compliance, internal controls, and risk management. The audit committee is largely meant to be independent of management but it should work with management and communicate frequently to ensure that any issues arising are addressed and resolved. (LO 3.f)

READING 4: WHAT IS ERM?

Lam, Chapter 4

EXAM FOCUS

Enterprise risk management (ERM) is a relatively recent concept that emerged in response to moving away from the traditional approach to risk management under which each risk was assessed, managed, and mitigated separately by a specific unit within the firm. In this reading, you will gain familiarity with the concept and definitions of ERM, its benefits and costs, and the seven major components of ERM. The role of the chief risk officer can also be a critical component in the implementation and success of the ERM program across the firm. For the exam, be familiar with the three motivations of the ERM program, and understand each of the seven components of a successful ERM program.

MODULE 4.1: ENTERPRISE RISK MANAGEMENT

LO 4.a: Describe Enterprise Risk Management (ERM) and compare and contrast differing definitions of ERM.

Companies face a variety of risks that arise from company operations, including but not limited to: credit, market, liquidity, operational, business, and information technology (IT) risks. Within the traditional approach to risk management, each of these primary risk types was evaluated by a specific unit within the organization in isolation, independent of the other risk types. For example, a company's traders were responsible for managing market risk, actuaries managed insurance risk, and management analyzed business risk.

While the traditional approach may have been adequate in a less volatile market environment, it suffers from the shortcoming of ignoring the dynamic nature of risks and their interdependencies. One risk type can affect another, and risks (or their hedges) can be offsetting if viewed from the perspective of the entire company. Treating each primary risk type in isolation ignores these interdependencies and can result in inefficient and costly overhedging of risks at the firm level. In addition, the various functional units responsible for evaluating and measuring risks may all use different methodologies and formats in their risk measurements. Without a centralized risk management system, a company's senior management and its board of directors would receive fragmented information from the various units, each potentially utilizing different measurement methods.

Given the noted shortcomings of the traditional approach, an integrated and centralized framework would significantly increase the efficiency of managing company risks. Such a centralized approach is referred to as **enterprise risk management (ERM)**.

ERM Definitions

Since the concept of ERM is relatively new and is still evolving, there is a lack of a standard ERM definition. ERM is often defined as a process or activity to manage risks. For example, the following definition was provided by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) in 2004:

> "ERM is a process, effected by an entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its appetite, to provide reasonable assurance regarding the achievement of entity objectives."

The International Organization of Standardization (ISO 3000) provides the following definition:

> "Risk is the effect of uncertainty on objectives and risk management refers to coordinated activities to direct and control an organization with regard to risk."

Both of the previous definitions contain useful ideas of ERM, but they do not define it as a value-added concept. As a result, a more useful definition of ERM is as follows:

> "Risk is a variable that can cause deviation from an expected outcome. ERM is a comprehensive and integrated framework for managing key risks in order to achieve business objectives, minimize unexpected earnings volatility, and maximize firm value."[1]

ERM is crucial in establishing a firm-wide, integrated set of policies, procedures, and standards. From senior management's perspective, an ERM system provides an invaluable overall risk perspective and control.

ERM Benefits and Costs

LO 4.b: Compare the benefits and costs of ERM and describe the motivations for a firm to adopt an ERM initiative.

There are three primary motivations for a firm to implement an ERM initiative: (1) integration of risk organization, (2) integration of risk transfer, and (3) integration of business processes. The respective benefits are better organizational effectiveness, better risk reporting, and improved business performance. However, implementation of an integrated firm-wide initiative is costly (both capital and labor intensive) and time-consuming. This process could last several years and requires ongoing senior management and board support.

Integration of Risk Organization: Increased Organizational Effectiveness

While most companies have many individual risk management functions, including market, credit, and various other risk units, an effective ERM strategy aggregates these risks under a centralized risk management process. Under a centralized process, the role of a chief risk officer (CRO) is often created, which reports to the company's chief executive officer (CEO) and/or the board, while the various risk management units report to the CRO. The benefit of a centralized approach is a top-down, coordinated framework that factors in the relationships and interdependencies of various risks.

Integration of Risk Transfer: Better Risk Reporting

Under the traditional, non-ERM approach, the various risks facing the company were evaluated by individual units within the organization, where each unit managed its own risk. For example, market risk was managed through derivatives, while operational risk was managed with insurance. This approach is useful in mitigating isolated risks, but it does not account for diversification within or across the various risk types, which could lead to over-hedging of risks or taking out excessive insurance coverage. Further, since no one unit is responsible for overall risk reporting, reporting of risks can be inconsistent and contradictory.

By contrast, ERM enables the company to take a holistic view of all risks and risk hedges used in order to hedge only those undesirable residual risks that still remain after factoring in diversification across risks. Risks are categorized under a risk dashboard of key risks, which includes an enterprise level description of key exposures, total losses, policy exceptions, and even early warning indicators. Senior management and the board are, therefore, able to take a big picture view of the interplay between each of the risks and can take appropriate measures to mitigate any residual risk.

Integration of Business Processes: Improved Business Performance

The third element of ERM is integrating risk management into the company's business processes. ERM can optimize business performance through business decisions, including capital allocation, product development and pricing, and efficient allocation of resources. This optimization results in reduced risk and only takes on the most profitable risks (i.e., maintains only those risks whose cost is less than the benefit of the corresponding project). Traditional risk measures such as value at risk (VaR) and risk-adjusted return on capital (RAROC) have been increasingly used to measure not only market risk but also credit and operational risk, while alternative risk measures such as credit derivatives are increasingly used to mitigate additional risks. The end result is a reduction in losses, lower earnings volatility, increased earnings, and higher shareholder value.

An effective ERM initiative allows company management to understand the major risk exposures and to set up adequate risk reporting. At the same time, auditors and regulators assess the company's ERM and set the necessary capital and compliance requirements for the board and senior management. In order to adequately address these requirements, the role of a "risk champion" has become more widespread, typically in the position of a CRO.

Chief Risk Officer

LO 4.c: Describe the role and responsibilities of a Chief Risk Officer (CRO) and assess how the CRO should interact with other senior management.

The specific role of the CRO was created in the early 1990s in response to the emergence of new financial instruments and the integration of capital markets. The CRO is responsible for all risks facing a company, including market, credit, operational, and liquidity risks, and specifically responsible for developing and implementing an ERM strategy. The role is prominent among financial firms, firms with significant investment activities or foreign operations, and energy firms.

The CRO is a top-level executive responsible for overall risk management in a centralized role. Reporting to the CRO typically are the heads of the various risk functions, including the heads of credit, market, operational, and insurance risks. The CRO provides overall leadership, vision, and direction for ERM and develops a framework of management policies, including setting the overall risk appetite of the firm. This includes measuring and quantifying risks and setting risk limits, developing the requisite risk systems, and communicating a clear vision of the firm's risk profile to the board and to key stakeholders.

Within the firm's hierarchy, the CRO typically reports to the CEO or the chief financial officer (CFO); however, the role is placed somewhere between the CEO/CFO and the board. Often there is a dotted line relationship with dual reporting to both the CEO/CFO and to the board. The dotted line relationship is intended to minimize any potential friction between the CRO and the firm's CEO or other top executives due potentially to excessive risk taking, regulatory issues, or outright fraud by the CEO or executives. In order to properly establish the reporting structure, it is important that the role of the CRO is clearly defined with clear goals and responsibilities for hiring and firing decisions.

Of course, the creation of the CRO role is not the only solution to establishing top-level risk oversight. The firm's audit committee could also take on this role; however, the audit functions are typically already stretched in their capacity to take on additional oversight roles. The centralization of all risk responsibilities could also be assigned to the CEO or CFO; however, there is strong support for establishing a separate oversight function in the role of the CRO who has experience and focused responsibility for risk management.

Over the last couple of decades, the CRO position, with its focused approach to risk management, has provided greater visibility and effectiveness to the role and to ERM. The role now represents the culmination of the risk executive functions with escalating salaries, and a company's CRO is often a contender for the highest executive roles including the role of the CEO. An ideal CRO possesses five critical skills: (1) leadership, (2) power of persuasion, (3) ability to protect the firm's assets, (4) technical skills to understand all risks, and (5) consulting skills to educate the board and business functions on risk management.

ERM Framework Components

LO 4.d: Describe the key components of an ERM program.

There are seven components of a strong ERM framework: (1) corporate governance, (2) line management, (3) portfolio management, (4) risk transfer, (5) risk analytics, (6) data and technology resources, and (7) stakeholder management.

Corporate governance is critical in the implementation of a successful ERM program and ensures that senior management and the board have the requisite organizational practices and processes to adequately control risks. Corporate governance practices have evolved considerably through recent regulatory initiatives including the Turnbull Report and the Sarbanes-Oxley Act. A successful corporate governance framework requires that senior management and the board adequately define the firm's risk appetite and risk and loss tolerance levels. In addition, management should remain committed to risk initiatives and ensures that the firm has the required risk management skills and organizational structure to successfully implement the ERM program. An effective framework also requires that all key

risks are successfully integrated into the ERM program and those responsible for implementing the program have clearly defined risk roles and responsibilities, including the role of the CRO. Oversight, audit, and monitoring targets are also crucial components of the ERM governance process.

Line management is the management of activities that relate directly to producing a firm's products and services. Line management is critical as it integrates business strategy into corporate risk policy, assesses the relevant risks, and incorporates them into pricing and profitability decisions. The assessment process should include adequate due diligence to determine which risks line managers can accept without senior management or board approval. In terms of addressing relevant risks, managers should include the cost of risk capital and expected losses in decisions about product pricing or investment returns.

Portfolio management provides a holistic view of the firm's risks if these risks are viewed as individual components of the aggregate risks facing the firm. Active portfolio management aggregates risk exposures and allows for diversification of risks (partly through offsetting risk positions) and prudent monitoring of risk concentrations against preset limits. Firms that manage each of their financial risks independently will need to integrate these risks into a comprehensive ERM process to optimize firm risk and return.

Risk transfer reduces or transfers out risks that are either undesirable risks or are desirable but considered concentrated (i.e., excessive risks). Concentrated risks can be especially risky for a company, and it is crucial that these positions are adequately monitored and mitigated. Risks could also be transferred to third parties if it is more cost effective to manage them externally. Risks can be offloaded through derivatives, insurance, and hybrid products. Natural hedges within the portfolio could also be incorporated into the risk transfer process to reduce hedging and insurance costs, even in the absence of third-party protection.

Risk analytics quantifies risk exposures for use in risk analysis, measurement, and reporting. Many of the risks facing the firm can be quantified including credit, market, and operational risk. Risk analytics can be used to calculate the cost-effective way of reducing risk exposures. It is also useful in evaluating the cost of managing risks in-house or externally as long as the cost of managing them externally is cheaper. The analysis and quantification of various risks can ultimately increase shareholder value, boosting net present value (NPV) and economic value added (EVA).

Data technology and resources improve the quality of data used in evaluating risks. Management faces the challenge that various systems used by the firm capture different price, volatility, or correlation metrics. Data technology and resources can mitigate these challenges by being incorporated into the firm's ERM program. Even if the technological resources available to the firm are not perfect, firms should incorporate them into the ERM system as early as possible.

Stakeholder management facilitates communicating a firm's internal risk management process to external stakeholders, including shareholders, creditors, regulators, and the public. The information shared with stakeholders is also important for rating agencies and analysts as they use this information in developing their research and credit opinions. A firm's internal risk management should be transparent to stakeholders, should provide adequate assurances that management follows prudent risk practices, and should include regular updates on the key risk factors facing the organization.

MODULE QUIZ 4.1

1. The basis of enterprise risk management (ERM) is that:
   A. risks are managed within each risk unit but centralized at the senior management level.
   B. the silo approach to risk management is the optimal risk management strategy.
   C. risks should be managed and centralized within each risk unit.
   D. it is necessary to appoint a chief risk officer to oversee most risks.

2. Jimi Chong is a risk analyst at a mid-sized financial institution. He has recently come across an article that described the enterprise risk management (ERM) process. Chong does not believe this is a well-written article, and he identified four statements that he thinks are incorrect. Which of the following statements identified by Chong is actually correct?
   A. One of the drawbacks of a fully centralized ERM process is over-hedging risks and taking out excessive insurance coverage.
   B. Effective ERM has three key benefits: improved business performance, better risk reporting, and stronger stakeholder management.
   C. Managing downside risk and earnings volatility are optional ERM strategies.
   D. A prudent ERM strategy allows a firm to accept more of the profitable risks.

3. Which of the following statements regarding the responsibilities of the chief risk officer (CRO) is least accurate?
   A. The CRO should provide the vision for the organization's risk management.
   B. In addition to providing overall leadership for risk, the CRO should communicate the organization's risk profile to stakeholders.
   C. Although the CRO is responsible for top-level risk management, he is not responsible for the analytical or systems capabilities for risk management.
   D. The CRO may have a solid line reporting to the CEO or a dotted line reporting to the CEO and the board.

4. Luke Drake has been recently appointed as the chief risk officer (CRO) of a non-profit organization. Drake is looking to implement a comprehensive enterprise risk management (ERM) program and had several discussions with senior management on this topic. During one of these discussions, Drake made the following statements:

   Statement 1: "Risk analytics is a key component of ERM and refers to the integration of risk management into the revenue generating activities of the organization."

   Statement 2: "While an organization can hedge desirable risks, it is unable to hedge undesirable risks."

   Is Drake correct regarding risk analytics and risk hedging?

	Risk analytics	Risk hedging
A.	Correct	Incorrect
B.	Incorrect	Incorrect
C.	Correct	Correct
D.	Incorrect	Correct

5. Allen Richards sits on the board of directors of a Canadian financial institution. Richards read the following statements in a presentation made to the board of directors by management on the institution's enterprise risk management strategies:

   Statement 1: "To manage undesirable risks, the institution could use third-party protection, including insurance products."

   Statement 2: "Although third-party protection is expensive, this is a cost of business, and it is not possible to reduce these costs."

   Richards believes both of these statements are incorrect. Richards' assessment is accurate with respect to:
   A. Statement 1 only.

B. Statement 2 only.
C. Both statements.
D. Neither statement.

KEY CONCEPTS

LO 4.a

An integrated and centralized approach under ERM is significantly more effective in managing a company's risks than under the traditional silo approach of managing and centralizing risks within each risk/business unit. ERM is a comprehensive and integrated framework for managing a firm's key risks to meet business objectives, minimize unexpected earnings volatility, and maximize firm value.

LO 4.b

The key motivations of an ERM initiative include integration of risk organization, integration of risk transfer, and integration of business processes, which lead to increased organizational effectiveness, better risk reporting, and improved business performance, respectively.

LO 4.c

The chief risk officer (CRO) is responsible for all risks facing a company, including market, credit, and operational risks and is responsible for developing and implementing an ERM strategy. The CRO provides overall leadership for ERM and develops policies and standards, including setting the firm's overall risk appetite, measuring and quantifying risks and setting risk limits, and developing risk systems.

The CRO generally reports to the CEO or CFO but could also have a dotted line relationship to both the CEO/CFO and to the board to minimize any potential friction between the CRO and the CEO/CFO (due to excessive risk taking, regulatory issues, or fraud).

An ideal CRO possesses five critical skills: (1) leadership, (2) power of persuasion, (3) ability to protect the firm's assets, (4) technical skills to understand all risks, and (5) consulting skills to educate the board and business functions on risk management.

LO 4.d

A strong ERM framework has seven main components: (1) corporate governance, (2) line management, (3) portfolio management, (4) risk transfer, (5) risk analytics, (6) data and technology resources, and (7) stakeholder management.

---

1. James Lam, *Enterprise Risk Management: From Incentives to Controls*, 2nd Edition, (Hoboken, NJ: John Wiley & Sons, 2014), 53.

ANSWER KEY FOR MODULE QUIZ

Module Quiz 4.1

1. **A** The basis of enterprise risk management (ERM) is that risks are managed within each risk unit but centralized at the senior management level.

   The traditional approach to risk management was the silo approach, under which each firm unit was responsible for managing its own risks, setting its own policies and standards, without coordination between the risk units. ERM is a superior approach because management benefits from an integrated approach to handling all risks (for example, management can see risks within the firm that cancel out and, therefore, do not need to be separately hedged). It is common, but not necessary, to appoint a chief risk officer to oversee all risks under ERM. (LO 4.a)

2. **D** A strong ERM strategy allows a firm to accept more of the profitable risks and reject unprofitable risks.

   Over-hedging risks and taking out excessive insurance coverage are issues faced by companies that do not have an integrated ERM strategy. In addition to improved business performance and better risk reporting, the third benefit of effective ERM is improved organizational effectiveness. Managing downside risk and earnings volatility are strategies typical of companies with a defensive approach to risk management, whereas effective ERM focuses on optimizing performance, influencing pricing, and allocating resources effectively. (LO 4.b)

3. **C** While it is accurate that the CRO is responsible for top-level risk management, he is also responsible for the analytical or systems capabilities for risk management. (LO 4.c)

4. **B** Both of Drake's statements are incorrect. Line management, not risk analytics, refers to the management of activities that relate directly to producing a firm's products and services. Line management is critical as it integrates business strategy into corporate risk policy.

   Through risk transfer, management can utilize a successful ERM program to transfer out both undesirable risk and desirable, concentrated risks. Hedging is typically done with derivatives, insurance, and hybrid products. (LO 4.d)

5. **B** Richards was wrong in identifying Statement 1 as being incorrect. Statement 1 is, in fact, correct because when managing undesirable risks, an institution could use third-party protection, including various hedges and insurance products.

   Richards accurately identified Statement 2 as being incorrect. While it is true that third-party protection can be expensive, by incorporating natural hedges in a risk portfolio, the institution could reduce its hedging and insurance costs. (LO 4.d)