제2판 추록

Corporate Governance

공 영 찬 저

- 본 내용은 제3판(2021년 1월 발행)에 추가된 내용(**부록**)으로 **제2판 추록**입니다.
- 따라서 본 인쇄물은 **제2판을 소지한 학생들을 위한 것**이니 이용에 참고하시기 바랍니다.
- 본 내용은 제2판 교재 p.190에 이어서 사용하시면 됩니다.
- 수험생 여러분의 합격을 기원합니다.

CNE 도서출판 원

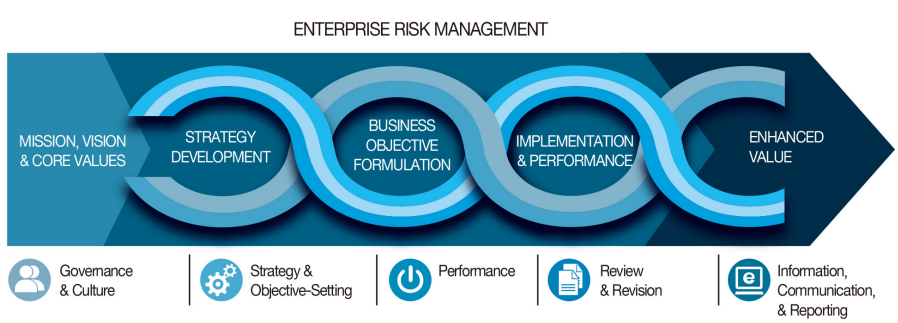
Appendix

COSO's ERM Framework – Recent Update

In recognition of the changing complexity of risk, the emergence of new risks, and the enhanced awareness of risk management by both boards and executive oversight bodies, COSO published ERM - Integrating with Strategy and Performance in 2017.

Similar in format to COSO's 2013 internal control update, COSO's 2017 ERM framework has a principles-based approach. In addition to adopting a more principles-based approach, other key changes to COSO's 2017 ERM framework include the following:

- It simplifies the definition of enterprise risk management.
- It emphasizes the relationship between risk and value.
- It renews the focus on the integration of enterprise risk management.
- It examines the role of culture.
- It elevates the discussion of strategy.
- It enhances the alignment between performance and enterprise risk management.
- It links enterprise risk management into decision-making more explicitly.
- It delineates between enterprise risk management and internal control.
- It refines risk appetite and tolerance.



1 Definition of ERM

Enterprise risk management is the culture, capabilities, and practices, integrated with strategy-setting and performance, that organizations rely on manage risk in creating, preserving, and realizing value.

1.1. Key concepts

1.1.1. Mission, vision, and core values

Mission, vision, and core values define what an entity strives to be and how it wants to conduct business.

① Mission

Mission represents the core purpose of the entity. The mission represents why the company exists and what it hopes to accomplish.

② Vision

Vision represents the aspirations of the entity and what it hopes to achieve over time

③ Core values

Core values represent an organization's beliefs and ideals about what is good or bad, acceptable and unacceptable, and they influence the behavior of the organization.

1.1.2. Culture, capabilities, and practices

① Culture

Culture represents the collective thinking of the people within an organization. Individuals have unique points of reference that influence how they identify, assess, and respond to risk. Culture plays an important role in shaping decisions regarding risk. (Core value correlate with culture)

② Capabilities (competitive advantage)

Competitive advantage produces value for an entity. Exploitation of competitive advantage and adaptation to change are skill sets embedded within ERM.

③ Practices

ERM is an organizational practice continually applied to the entire scope of activities of the business. It is part of management decisions at all levels of the entity. It is neither static nor is it an adjunct or add-on to the business.

1.1.3. Integration with strategy-setting and performance

Strategy is set in a manner that aligns with mission and vision. Business objectives flow from strategy. Business objectives drive the activities of all business units and functions.

ERM integrates with strategy-setting and operating activities to promote an understanding of how risk potentially affects the entity overall.

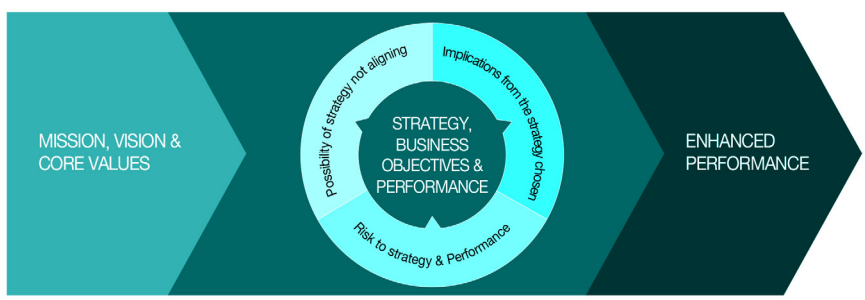
Mission and vision correlate with strategy and business objectives.

1.2. ERM interrelationships

ERM is depicted as a series of sequential yet intertwined components that drive an organization toward enhanced value.

The tone at the top and communication are linked, and weave into the similarly linked efforts to develop overall strategy, specific business objectives, and manage performance to the achievement of value

Mission, vision, and values drive the process but also affected by performance, as management constantly reviews its risks and its ability to create value.



1.3. Managing risk linked to value

ERM practices are intended to provide the management and the board with a reasonable expectation that the organization's overall strategy and business objectives can be achieved. Reasonable expectation means the amount of risk of achieving strategy and business objectives is appropriate for that entity. An organization must continually review and manage the types and amounts of risk it is willing to accept in its pursuit of value.

1.3.1. Risk appetite

Risk appetite represents the types and amount of risk that an organization is willing to accept in pursuit of value. Risk appetite is a range rather than a specific limit and provides guidance on the practices an organization is encouraged to pursue or not pursue.

Risk appetite is expressed first in mission and vision. Risk appetite varies between products, business units, or over time in line with changing capabilities for managing risks and must be flexible enough to adapt to changing business conditions without approvals.

1.3.2. Relationship of value and risk appetite

Managing risk within risk appetite enhances an organization's ability to create, preserve, and realize value. ERM seeks to align anticipated value creation with risk appetite and capabilities for managing risk over time.

1.3.3. Value

The underlying premise of ERM is that every entity exists to provide value for stakeholders and that all entities face risk in the pursuit of value for their stakeholders. Management decisions will affect the development of value, including its creation, preservation, erosion, and realization.

① **Value creation**

Value is created when benefits of value exceed the cost of resources used. Resources may include people, financial capital, technology, process, and brand (market presence). A successful and profitable launch of new product line represents value creation.

② **Value preservation**

Value is preserved when ongoing operations efficiently and effectively sustain created benefits. High customer satisfaction with profitable product lines is evidence of value preservation.

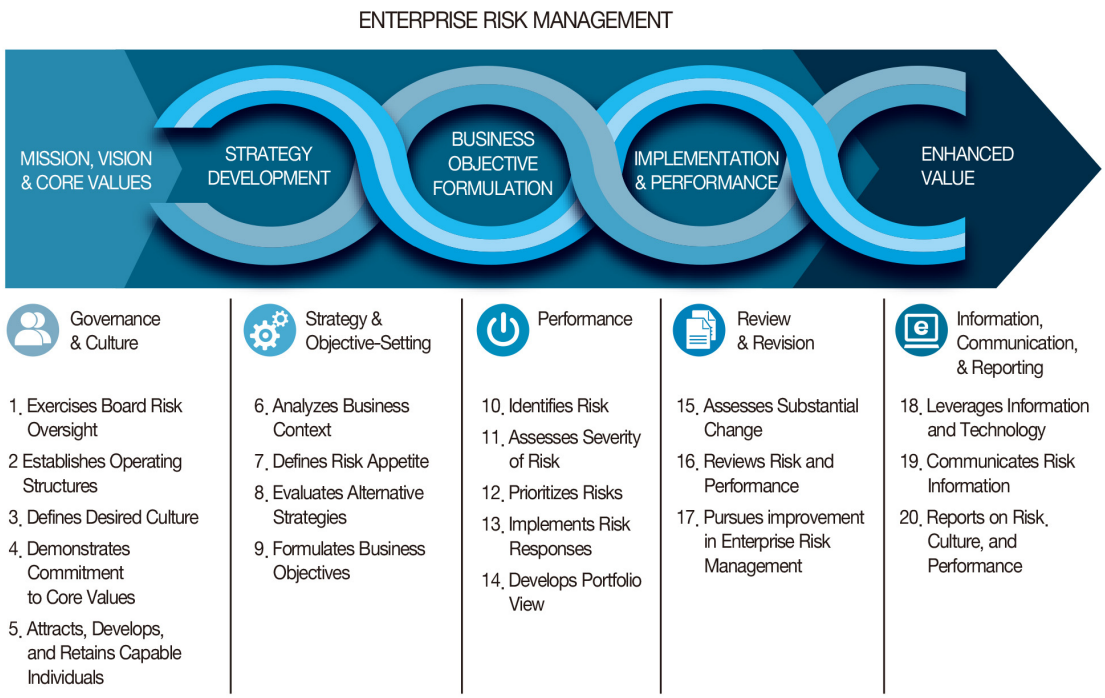
③ **Value erosion**

Value is eroded when faulty strategy and inefficient or ineffective operations cause value to decline. An unsuccessful launch of new product line represents value erosion. Not only are financial resources lost, but the brand name suffers as well.

④ **Value realization**

Value is realized when benefits created by the organization are received by stakeholders in either monetary or nonmonetary form. Value realization is illustrated by increased profitability and stock prices for company owner, increased customer satisfaction, consistent product and brand usage, market leadership, and consistent innovation that not only enhances the company but improves the economy.

2 Components of ERM



2.1. Governance and Culture

Governance sets the organization's tone, reinforcing the importance of, and establishing oversight responsibilities for, enterprise risk management. Culture pertains to ethical values, desired behaviors, and understanding of risk in the entity.

2.1.1. Exercises board oversight

The board of directors provides oversight for an entity's strategy and carries out governance responsibilities to support management in achieving strategy and business objectives. The board is expected to have the skills, experience, and business knowledge to understand the entity's strategy; stay informed on relevant issues; and maintain an active and accountable role that is independent and conscious of potential bias. (Active and accountable board oversight is often characterized by frequent conversations with management to determine the suitability of ERM design and effectiveness in enhancing value)

2.1.2. Establishes operating structure

Operating structures are established to pursue strategy and business objectives. Operating structures describe how an entity organizes and carries out its day-to-day operations and contributes to the alignment of risk management practices with core values.

2.1.3. Defines desired culture

The organization defines the desired behaviors that characterize the entity's desired culture. An entity's culture influences how the organization identifies risk, what types of risk it accepts, and how it manages risk. The ability of an organization to successfully achieve its strategy and business objectives is impeded when the behaviors and decisions of the organization (culture) do not align with its core values.

2.1.4. Demonstrates commitment to core values

The organization demonstrates a commitment to the entity's core values. Without support from the top of the organization, risk awareness can be undermined and risk-inspired decisions may be inconsistent with those values.

2.1.5. Attracts, develops, and retains capable individuals (employees)

Commitment to building human capital in alignment with the strategy and business objectives is a principle of the governance and culture component. The ultimate accountability for development and retention of capable individuals starts with the board and its selection of executive leadership. The selection of team members is typically delegated to appropriate levels of management. Human resources professionals assist management in assembling competent team members through consideration of the following factors;

- Knowledge, skills, and experience
- Nature and degree of judgment and limitations of authority to applied to a specific position
- The costs and benefit of different skill level and experience

The ongoing process of attracting, developing, and retaining individuals includes attracting or seeking out competent individuals and training them, then mentoring, evaluating, and ultimately retaining them with appropriate incentives and rewards. No less important than maintenance of the current talent pool is preparation for succession, a process that may involve identifying more than one person who could fill a crucial role.

2.2. Strategy and Objective-Setting

Enterprise risk management, strategy, and objective-setting work together in the strategic-planning process. A risk appetite is established and aligned with strategy; business objectives put strategy into practice while serving as a basis for identifying, assessing, and responding to risk.

2.2.1. Analyzes business context

Business context is the trends, events, relationships, and other factors that may influence, clarify, or change an entity's current and future strategy and business objectives. Consideration of the potential effects of business context on risk profile is a principle supporting the strategy and objective-setting component. Business context may be dynamic, complex, and even unpredictable. Business context usually considers both external and internal environments.

2.2.2. Defines risk appetite

The organization defines risk appetite in the context of creating, preserving, and realizing value. Entities consider risk appetite in qualitative terms, while others may be quantitative. The best approach for an entity is one that aligns with the analyses used to assess risk in general, whether that is qualitative or quantitative. General terms such as "low appetite" or "high appetite" are sufficient expressions of risk appetite. Referencing "target", "ranges", "ceilings", or "floors" may also be used. Ultimately, risk appetite is expressed in the context of objectives.

2.2.3. Evaluates alternative strategies

Evaluation of alternative strategies and the potential effect on risk profile is a principle supporting the strategy and objective-setting component. Strategy is evaluated from two perspectives;

- The possibility that the strategy does not align with the mission, vision, and core values of the entity
- The implications from the chosen strategy

Misaligned strategies may impede achievement of the mission, and fulfilment of the entity's mission. The implications of each strategy include risks and opportunities of each strategy. Identified risks collectively form a risk profile and serve as the basis for developing and evaluating alternative strategies.

The development of alternative strategies considers the supporting assumptions relating to the business context, resources, and capabilities. The level of confidence associated with each supporting assumption will affect the risk profile of each of the strategies. Development of a risk profile for a strategy enables consideration of the types and amount risk faced by the organization. Successful strategy is carried out within the organization's risk appetite. Strategy may change as the evaluation of risk or the ability to perform changes.

2.2.4. Formulates business objectives

Business objectives are the measurable steps that an organization makes to achieve its strategy. The alignment of business objectives to strategy supports the entity in achieving its mission and vision.

Business objectives are developed that are specific, measurable or observable, attainable, and relevant to the achievement of strategy. Business objectives may relate to financial performance, customer aspirations, operational efficiency, compliance obligations, or innovation.

The organization sets targets to monitor the performance of the entity and support the achievement of its business objectives. Monitoring performance includes the concept of tolerance. Tolerance is the range of acceptable outcomes related to achieving a business objective within the risk appetite. Tolerance is also referred to as the acceptable variance in performance.

2.3. Performance

Risks that may impact the achievement of strategy and business objectives need to be identified and assessed. Risks are prioritized by severity in the context of risk appetite. The organization then selects risk responses and takes a portfolio view of the amount of risk it has assumed. The results of this process are reported to key risk stakeholders.

2.3.1. Identifies risks

Organizations identify risks that affect their performance in achieving strategy and business objectives. New and emerging risks are identified, and currently assessed risks are reevaluated using various techniques.

2.3.2. Assesses severity of risk

The severity of risk is evaluated after it has been identified. Resources and capabilities are deployed to keep the risk within the entity's risk appetite based on the assessment.

The severity of a risk is assessed at multiple levels (across divisions, functions, and operating units) in line with the business objectives it may affect. Risks deemed severe at the operating level may be less of a concern at division or entity level.

Severity measures relate to impact (result or effect of the risk) and likelihood (possibility of the risk occurring). Likelihood may be expressed qualitatively or quantitatively.

Risk assessment includes the concepts of inherent risk, target residual risk, and actual residual risk.

- Inherent risk is the risk to an entity in the absence of any direct, or focused actions by management to alter its severity.
- Target residual risk is the amount of risk that an entity prefers to assume in the pursuit of its strategy and business objectives knowing that management will implement or has implemented direct or focused actions to alter the severity of the risk.
- Actual residual risk is the risk remaining after management has taken action.

The organization strives to identify triggers that will prompt a reassessment of severity when required.

2.3.3. Prioritizes risk

Prioritization of risk as a basis for determining risk response is a principle underlying the performance component. Risks that result in the entity approaching the risk appetite for specific business objectives are typically given high priority.

2.3.4. Implements risk responses

① **Accept**

No action is taken to change the severity of the risk. Acceptance is most appropriate as a risk response when risk to strategy and business objectives is within the entity's risk appetite.

② **Avoid**

Action is taken to remove the risk (leaving a line of business, etc.). Avoidance is appropriate when an entity cannot devise a risk response that will mitigate the risk to objectives.

③ **Pursue**

Action is taken that accepts increased risk to achieve improved performance. Pursuit of risk is appropriate when management understands the nature and extent of any changes required to achieve desired performance while not exceeding the boundaries of acceptable tolerance.

④ **Reduce**

Action is taken to reduce the severity of the risk. Management designs risk mitigation techniques to reduce risk to an amount of severity aligned with the target risk profile and risk appetite.

⑤ **Share**

Action is taken to reduce the severity of the risk. Sharing risk with such techniques as outsourcing and insurance lowers residual risk in alignment with risk appetite.

2.3.5. Develops portfolio view

The organization develops and evaluates a portfolio (entity-wide) view of risk. A portfolio view allows management and the board of directors to consider the type, severity, and interdependencies of risks and how they may affect performance and align with the overall risk appetite.

2.4. Review and Revision

By reviewing entity performance, an organization can consider how well the enterprise risk management components are functioning over time and in light of substantial changes, and what revisions are needed.

2.4.1. Assesses substantial change

The entity identifies and assesses changes that may substantially affect strategy and business objectives. Assessments may include identifying internal and external environmental changes related to the business context as well as changes in culture.

2.4.2. Reviews risk and performance

The organization reviews entity performance and considers risk, including the capabilities and practices of the organization. Evaluations may relate to potentially incorrect assumptions, poorly implemented practices, entity capability, or cultural factors.

2.4.3. Pursues improvement in ERM

The organization pursues improvement of ERM. Opportunities to revisit and improve efficiency and usefulness may occur in any area.

2.5. Information, Communication, and Reporting

Enterprise risk management requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across the organization.

2.5.1. Leverages information and technology

The organization leverages the entity's information and technology systems to support the organization with relevant information. Relevant information helps the organization be more agile in its decision making and provides a competitive advantage.

Different types of information support different levels of the decision making;

- Governance and culture-related practices
  The organization may need information on the standards of conduct and individual performance.
- Strategy and objective-setting practices
  The organization may need information on stakeholder expectations about risk appetite.
- Performance-related practices
  The organization may need information on its competitors to assess changes in the amount of risk.
- Review and revision-related practices
  The organization may need information on emerging trends in ERM.

Information is generally characterized as structured (e.g., database files, etc.) and unstructured (e.g., volumes of e-mail, photos, etc.). The ability to accumulate and analyze data effectively is constantly evolving. Classifying information using common risk categories helps with risk assessment (e.g., information from internal audit, information from management, etc.)

Data management is integral to risk-aware decisions. Effective data management considers three key elements;

- Data and information governance promote standardization of high-quality data.
- Processes and controls promote data reliability.
- Data management architecture refers to the fundamental design of the technology. Design is driven by value defined by management's needs.

2.5.2. Communicates risk information

The organization uses communication channels to support ERM. Communications are made to internal and external stakeholders and with the board of directors. Communication techniques vary widely. Communication methods must be evaluated for effectiveness.

2.5.3. Reports on risk, culture, and performance

The organization reports on risk, culture, and performance at multiple levels and across the entity. Reporting may be either quantitative or qualitative and be made to a wide range of users, including management, risk owners, assurance providers, external stakeholders, and others.

Types of reports include portfolio view of risk (outlining the severity of risk at the entity level) and profile view of risk (outlining the severity of risk at different levels within the entity, e.g., a division, etc.).

Reporting on culture seeks to measure and provide feedback on behavior and attitudes. Reporting can be complex and may be embodied by;

- Analytics of cultural trends
- Benchmarking to other entities or standards
- Compensation schemes and the potential influence on decision making
- "Lessons learned" analysis
- Reviews of behavioral trends
- Surveys of risk attitudes and risk awareness

The frequency of reporting should be commensurate with the severity and priority of risk.