The content of **BEC Study Unit 2, Subunit 2**, has undergone extensive edits due to the 2017 COSO ERM framework overhaul, which becomes testable on April 2, 2018. Instead of producing a change document that details every edit, which would be quite extensive and possibly confusing, we have reproduced the entire subunit in this book update. Please see below for a summary of the changes; then use the rest of this PDF to update the relevant pages in your book. These pages include the changes for outlines and questions.

Content on the COSO enterprise risk management (ERM) framework in Subunit 2 was updated to reflect the new COSO ERM framework, *Enterprise Risk Management -- Integrating with Strategy and Performance*. Major changes include the following:

- Greater emphasis on integrating risk management with strategy-setting and performance
- Redefined the terms “enterprise risk management” and “risk”
- Introduced the terms “risk profile” and “portfolio view”
- Replaced the eight components with five new components
- Introduced 20 principles that are distributed among the components

**Study Unit 2 – COSO Frameworks**

Pages 35-40 and 44-46, Subunit 2.2, outline and questions: The replacement subunit begins on the next page.
2.2 COSO FRAMEWORK -- ENTERPRISE RISK MANAGEMENT (ERM)

1. COSO Risk Management Framework
   a. Enterprise Risk Management – Integrating with Strategy and Performance (COSO ERM framework) is a framework that complements, and incorporates some concepts of, the COSO internal control framework.
   b. The COSO ERM framework provides a basis for coordinating and integrating all of an organization’s risk management activities. Effective integration (1) improves decision making and (2) enhances performance.

2. ERM Definition and Concepts
   a. ERM is based on the premise that every organization exists to provide value for its stakeholders. Accordingly, ERM is defined as
      The culture, capabilities, and practices, integrated with strategy-setting and performance, that organizations rely on to manage risk in creating, preserving, and realizing value. [emphasis added]
   b. Key concepts and phrases.
      1) Culture consists of “[t]he attitudes, behaviors, and understanding about risk, both positive and negative, that influence the decisions of management and personnel and reflect the mission, vision, and core values of the organization.” [emphasis added]
         a) Mission is the organization’s core purpose.
         b) Vision is the organization’s aspirations for what it intends to achieve over time.
         c) Core values are the organization’s essential beliefs about what is acceptable or unacceptable.
      2) Capabilities are the skills needed to carry out the entity’s mission and vision.
      3) Practices are the collective methods used to manage risk.
      4) Integrating strategy setting and performance.
         a) Risk must be considered in setting strategy, business objectives, performance targets, and tolerance.
            i) Strategy communicates how the organization will (a) achieve its mission and vision and (b) apply its core values.
            ii) Business objectives are the steps taken to achieve the strategy.
            iii) Tolerance is the range of acceptable variation in performance results. (This term is identical to “risk tolerance” in the COSO internal control framework.)
         b) The organization considers the effect of strategy on its risk profile and portfolio view.
            i) Risk profile is a composite view of the types, severity, and interdependencies of risks related to a specific strategy or business objective and their effect on performance. A risk profile may be created at any level (e.g., entity, division, operating unit, or function) or aspect (e.g., product, service, or geography) of the organization.
ii) **Portfolio view** is similar to a risk profile. The difference is that it is a composite view of the risks related to entity-wide strategy and business objectives and their effects on entity performance.

5) **Managing risk.**

   a) **Risk** is “[t]he possibility that events will occur and affect the achievement of strategy and business objectives.”

   b) **Opportunity** is any action or potential action that creates or alters goals or approaches for the creation, preservation, or realization of value.

   c) Effective ERM practices provide **reasonable expectation** (not absolute assurance) that the risk assumed is appropriate.

   d) **Risk inventory** consists of all identified risks that affect strategy and business objectives.

   e) **Risk capacity** is the maximum amount of risk the organization can assume.

   f) **Risk appetite** consists of the amount and types of risk the organization is willing to accept in pursuit of value.

   g) **Inherent risk** is the risk in the absence of management actions to alter its severity.

   i) **Actual residual risk** remains after management actions to alter its severity.

   h) **Risk response** is an action taken to bring identified risks within the organization’s risk appetite.

   i) A **residual risk profile** includes risk responses.

   i) **Target residual risk** is the risk the entity prefers to assume knowing that management has acted or will act to alter its severity.
6) **Value** is
   
a) **Created** when the benefits obtained from the resources used exceed their costs.
   
b) **Preserved** when the value of resources used is sustained.
   
c) **Realized** when benefits are transferred to stakeholders.
   
d) **Eroded** when management’s strategy does not produce expected results or management does not perform day-to-day tasks.

3. **ERM Roles and Responsibilities**
   
a. The **board** provides risk oversight of ERM culture, capabilities, and practices. Certain board committees may be formed for this purpose. Examples are (1) an **audit** committee (often required by regulators), (2) a **risk** committee that directly oversees ERM, (3) an **executive compensation** committee, and (4) a **nomination or governance** committee that oversees selection of directors and executives.
   
b. **Management** has **overall responsibility** for ERM and is generally responsible for the **day-to-day** managing of risk, including the implementation and development of the COSO ERM framework.
      
1) Within management, the **CEO** has **ultimate responsibility** for ERM and achievement of strategy and business objectives.
   
c. An organization may designate a **risk officer** as a centralized coordinating point to facilitate risk management across the entire enterprise.
   
d. **Three lines of management accountability:**
      
1) The first line consists of the principal owners of risk. They manage performance and risks taken to achieve strategy and objectives.
   
2) The second line consists of the supporting (business-enabling) functions (e.g., risk officer) that (a) provide guidance on performance and ERM requirements, (b) evaluate adherence to standards, and (c) challenge the first line to take prudent risks.
   
3) The third line (assurance) (e.g., internal auditing) (a) audits (reviews) ERM, (b) identifies issues and improvements, and (c) informs the board and executives of matters needing resolution.

4. **ERM Components**

![Enterprise Risk Management Diagram](image)

**Figure 2-3**

a. The COSO ERM framework consists of **five interrelated components**. Twenty principles are distributed among the components.

1) The **supporting aspect** components are
   
a) Governance and culture and
   
b) Information, communication, and reporting.
2) The **common process** components are
   a) Strategy and objective-setting,
   b) Performance, and
   c) Review and revision.

5. **Governance and Culture**
   a. Governance sets the organization’s tone and establishes responsibilities for ERM.
      Culture relates to the desired behaviors, values, and overall understanding about risk held by personnel within the organization. **Five principles** relate to governance and culture:
   
   1) The **board** exercises risk **oversight**.
      a) The full board ordinarily is responsible for risk oversight. However, the board may delegate risk oversight to a board committee, such as a **risk committee**.
      b) The board’s oversight role may include, but is not limited to,
         i) Reviewing and challenging decisions related to strategy, risk appetite, and significant business decisions (e.g., mergers and acquisitions).
         ii) Approving management compensation.
         iii) Participating in stakeholder relations.
      c) Risk oversight is most effective when the board
         i) Has the necessary **skills, experience, and business knowledge** to (a) understand the organization’s strategy and industry and (b) maintain this understanding as the business context changes.
         ii) Is **independent** of the organization.
         iii) Determines whether ERM capabilities and practices enhance value.
         iv) Understands the **organizational biases** influencing decision making and challenges management to minimize them.
   
   2) The organization establishes **operating structures**.
      a) They describe how the entity is organized and carries out its day-to-day operations.
      b) They generally are aligned with the entity’s legal structure and management structure.
         i) The **legal structure** determines how the entity operates (e.g., as a single legal entity or as multiple, distinct legal entities).
         ii) The **management structure** establishes reporting lines (e.g., direct reporting versus secondary reporting), roles, and responsibilities. Management is responsible for clearly defining roles and responsibilities.
      c) Factors to consider when establishing and evaluating operating structures include the entity’s
         i) Strategy and business objectives, including related risks;
         ii) Nature, size, and geographic distribution;
         iii) Assignment of authority, accountability, and responsibility at all levels;
         iv) Types of reporting lines and communication channels; and
         v) Reporting requirements (e.g., financial, tax, regulatory, and contractual).
3) The organization defines the desired culture.
   a) The board and management are responsible for defining culture.
   b) Culture is shaped by internal and external factors.
      i) **Internal** factors include (a) the level of judgment and autonomy allowed to personnel, (b) standards and rules, and (c) the reward system in place.
      ii) **External** factors include (a) legal requirements and (b) expectations of stakeholders (e.g., customers and investors).
   c) The organization’s definition of culture determines its placement on the culture spectrum, which ranges from risk averse to risk aggressive.

   ![Culture Spectrum Diagram](image)

4) The organization demonstrates commitment to core values.
   a) The organization’s core values should be reflected in all its actions and decisions.
   b) The **tone of the organization** is the manner in which core values are communicated across the organization.
   c) When risk-aware culture and tone are aligned, stakeholders have confidence that the organization is abiding by its core values.

5) The organization attracts, develops, and retains capable individuals.
   a) Management is responsible for defining the human capital necessary (the needed competencies) to achieve strategy and business objectives.
   b) The **human resources function** assists management in developing competency requirements through processes that attract, train, mentor, evaluate, reward, and retain competent individuals.
   c) **Contingency plans** should be developed to prepare for succession. Such plans train selected personnel to assume responsibilities vital to ERM. An example is training a risk manager to assume the position of risk officer.

6. **Strategy and Objective Setting**
   a. Strategy must support the organization’s mission, vision, and core values. The integration of ERM with strategy setting helps to understand the risk profile related to strategy and business objectives. **Four principles** relate to strategy and objective setting:
      1) The organization analyzes **business context** and its effect on the risk profile.
         a) Business context pertains to the relationships, events, trends, and other factors that influence the organization’s strategy and business objectives. Accordingly, business context includes the organization’s internal and external environments.
         i) The **internal environment** consists of factors related to four categories: (a) capital (e.g., assets), (b) people (e.g., skills and attitudes), (c) processes (e.g., tasks, policies, and procedures), and (d) technology.
ii) The external environment consists of factors related to six categories: (a) political (government intervention and influence), (b) economic (e.g., interest rates and availability of credit), (c) social (e.g., consumer preferences and demographics), (d) technological (e.g., R&D activity), (e) legal (laws, regulations, and industry standards), and (f) environmental (e.g., climate change).

b) Business context may be

i) Dynamic. New, emerging, and changing risks can appear at any time (e.g., low barriers of entry allow new competitors to emerge).

ii) Complex. A context may have many interdependencies and interconnections (e.g., a transnational company has several operating units around the world, each with unique external environmental factors).

iii) Unpredictable. Change occurs rapidly and in unanticipated ways (e.g., currency fluctuations).

c) The effect of business context on the risk profile may be analyzed based on past, present, and future performance.

2) The organization defines risk appetite (the amount of risk it is willing to accept in pursuit of value).

a) The organization considers its mission, vision, culture, prior strategies, and risk capacity (the maximum risk it can assume) to set its risk appetite.

b) In setting risk appetite, the optimal balance of opportunity and risk is sought.

i) Risk appetite is rarely set above risk capacity.

c) Risk appetite may be expressed qualitatively (e.g., low, moderate, high) or quantitatively (e.g., as a percentage of a financial amount). But it should reflect how risk assessment results are expressed.

d) The board approves the risk appetite, and management communicates it throughout the organization.

3) The organization evaluates alternative strategies and their effects on the risk profile.

a) Approaches to evaluating strategy include SWOT (Strengths-Weaknesses-Opportunities-Threats) analysis, competitor analysis, and scenario analysis.

b) The organization must evaluate

i) The strategy’s alignment with its mission, vision, core values, and risk appetite and

ii) The implications of the chosen strategy (its risks, opportunities, and effects on the risk profile).

c) Strategy should be changed if it fails to create, realize, or preserve value.

4) The organization establishes business objectives that align with and support strategy.

a) Business objectives are (1) specific, (2) measurable, (3) observable, and (4) obtainable.

b) Business objectives may relate to, among others, financial performance, operational excellence, or compliance obligations.

c) Performance measures, targets, and tolerances (the range of acceptable variation in performance) are established to evaluate the achievement of objectives.
7. **Performance**

   a. Performance relates to ERM practices that support the organization’s decisions in pursuit of value. Those practices consist of identifying, assessing, prioritizing, responding to, and developing a portfolio view of risk. **Five principles** relate to performance:

   1) The organization **identifies risks** that affect the performance of strategy and business objectives.
      
      a) The organization should identify risks that disrupt operations and affect the **reasonable expectation** of achieving strategy and business objectives.
      
      b) **New, emerging, and changing** risks are identified. Examples are risks resulting from changes in business objectives or the business context.
         
         i) **Opportunities** (actions or potential actions that create or alter goals or approaches for the creation, preservation, or realization of value) also are identified. They differ from **positive events**, occurrences in which performance exceeds the original target.
      
      c) Risk identification **methods and approaches** include (1) day-to-day activities (e.g., budgeting, business planning, or reviewing customer complaints), (2) simple questionnaires, (3) facilitated workshops, (4) interviews, or (5) data tracking.
      
      d) The **risk inventory** consists of all risks that could affect the entity.
      
      e) Risk and opportunity identification should be comprehensive across all levels and functions of the entity.

   2) The organization assesses the **severity of risk**. Severity is a measure of such considerations as impact, likelihood, and the time to recover from events.

      a) Common measures of severity include combinations of impact and likelihood.
         
         i) **Impact** is the result or effect of the risk. Impact may be positive or negative.
         
         ii) **Likelihood** is the possibility that an event will occur. Likelihood may be expressed qualitatively (e.g., a remote probability), quantitatively (e.g., a 75% probability), or in terms of frequency (e.g., once every 6 months).
      
      b) The **time horizon** to assess risk should be identical to that of the related strategy and business objective. For example, the risk affecting a strategy that takes 2 years to achieve should be assessed over the same period.
      
      c) Risk is assessed at **multiple levels** (e.g., entity, division, operating unit, and function) of the organization and linked to the related strategy and business objective.
         
         i) The severity of a risk may vary across levels. For example, a risk with high severity at the operating unit level may have low or moderate severity at the entity level.
      
      d) Qualitative and quantitative methods may be used to assess risk.
         
         i) **Qualitative** methods are more efficient and less costly than quantitative methods. Examples are interviews, surveys, and benchmarking.
         
         ii) **Quantitative** methods are more precise than qualitative methods. Examples are decision trees, modeling (probabilistic and nonprobabilistic), and Monte Carlo simulation.
      
      e) The organization should **reassess severity** whenever triggering events occur, such as changes in business context and risk appetite.
f) The risk assessment should consider inherent risk, target residual risk, and actual residual risk.

g) Assessment results may be presented using a **heat map**, which highlights the relative severity of each risk. The warmer the color, the more severe the risk.

**Business Objective Heat Map**

![Heat Map](image)

3) The organization **prioritizes risks** at all levels.

a) Risk prioritization enables the organization to optimize the allocation of its limited resources.

b) In addition to severity (e.g., impact and likelihood), the following factors are considered when prioritizing risks:

i) Agreed-upon criteria,

ii) Risk appetite,

iii) The importance of the affected business objective(s), and

iv) The organizational level(s) affected.

c) **Agreed-upon criteria** are used to evaluate the characteristics of risks and to determine the entity’s capacity to respond appropriately. Higher priority is given to risks that most affect the criteria. Example criteria include the following:

i) **Complexity** is the nature and scope of a risk, e.g., interdependence of risks.

ii) **Velocity** is the speed at which a risk affects the entity.

iii) **Persistence** is how long a risk affects the entity, including the time it takes the entity to recover.

iv) **Adaptability** is the entity’s capacity to adjust and respond to risks.

v) **Recovery** is the entity’s capacity (not the time) to return to tolerance.

d) Higher priority also is assigned to risks that

i) Approach or exceed risk appetite,

ii) Cause performance levels to approach the outer limits of tolerance, or

iii) Affect the entire entity or occur at the entity level.
4) The organization identifies and selects **risk responses**, recognizing that risk may be managed but not eliminated. Risks should be managed within the business context and objectives, performance targets, and risk appetite.

   a) The following are the five categories of risk responses:
      i) **Acceptance.** No action is taken to alter the severity of the risk. Acceptance is appropriate when the risk is within the risk appetite.
      ii) **Avoidance.** Action is taken to remove the risk (e.g., discontinuing a product line or selling a subsidiary). Avoidance typically suggests no response would reduce the risk to an acceptable level.
      iii) **Pursuit.** Action is taken to accept increased risk to improve performance without exceeding acceptable tolerance.
      iv) **Reduction.** Action is taken to reduce the severity of the risk so that it is within the target residual risk profile and risk appetite.
      v) **Sharing.** Action is taken to reduce the severity of the risk by transferring a portion of the risk to another party. Examples are insurance, hedging, joint ventures, and outsourcing.

   b) The following are the **factors** considered in selecting and implementing risk responses:
      i) They should be chosen for, or adapted to, the **business context**.
      ii) **Costs and benefits** should be proportionate to the severity of the risk and its priority.
      iii) They should further **compliance** with obligations (e.g., industry standards) and achievement of **expectations** (e.g., mission, vision, and stakeholder expectations).
      iv) They should bring risk within **risk appetite** and result in performance outcomes within **tolerance**.
      v) Risk response should reflect risk severity.

   c) **Control activities** are designed and implemented to ensure risk responses are carried out. (COSO guidance for control activities is outlined in item 7. in Subunit 2.1.)

5) The organization develops and evaluates its **portfolio view of risk**.

   a) The culmination of risk identification, assessment, prioritization, and response is the full portfolio view of risk.

   b) The following four risk views have different levels of risk integration:
      i) **Risk view (minimal integration).** Risks are identified and assessed. Emphasis is on the event, not the business objective.
      ii) **Risk category view (limited integration).** Identified and assessed risks are categorized, e.g., based on operating structures.
      iii) **Risk profile view (partial integration).** Risks are linked to the business objectives they affect, and any dependencies between objectives are identified and assessed. For example, an objective of increased sales may depend on an objective to introduce a new product line.
      iv) **Portfolio view (full integration).** This composite view of risks relates to **entity-wide** strategy and business objectives and their effect on **entity** performance. At the top level, greater emphasis is on strategy. Thus, responsibility for business objectives and specific risks **cascades** through the entity.

   c) Using a portfolio view of risk, management determines whether the entity’s **residual risk profile** (risk profile inclusive of risk responses) aligns with overall **risk appetite**.
d) Qualitative and quantitative methods may be used to evaluate how changes in risk may affect the portfolio view of risk.
   i) Qualitative methods include benchmarking, scenario analysis, and stress testing.
   ii) Quantitative methods include statistical analysis.

8. Review and Revision
   a. The organization reviews and revises its current ERM capabilities and practices based on changes in strategy and business objectives. Three principles relate to review and revision:
      1) The organization identifies and assesses changes that may substantially affect strategy and business objectives.
         a) Changes in the organization’s business context and culture are most likely to substantially affect strategy and business objectives.
         b) Such changes may result from changes in the organization’s internal or external environment.
            i) Substantial changes in the internal environment include those due to rapid growth, innovation, and turnover of key personnel.
            ii) Substantial changes in the external environment include those in the economy or regulations.
      2) The organization reviews entity performance results and considers risk.
         a) Performance results that deviate from target performance or tolerance may indicate (1) unidentified risks, (2) improperly assessed risks, (3) new risks, (4) opportunities to accept more risk, or (5) the need to revise target performance or tolerance.
      3) The organization pursues improvement of ERM.
         a) The organization must continually improve ERM at all levels, even if actual performance aligns with target performance or tolerance.
         b) Methods of identifying areas for improvement include continual or separate evaluations and peer comparisons (reviews of industry peers). (COSO guidance for monitoring activities is outlined in item 9. in Subunit 2.1.)

9. Information, Communication, and Reporting
   a. The organization must capture, process, manage (organize and store), and communicate timely and relevant information to identify risks that could affect strategy and business objectives. Three principles relate to information, communication, and reporting:
      1) The organization leverages its information systems to support ERM.
         a) Data are raw facts collectible for analysis, use, or reference. Information is processed, organized, and structured data about a fact or circumstance. Information systems transform data (e.g., risk data) into relevant information (e.g., risk information).
            i) Knowledge is data transformed into information.
            ii) Information is relevant if it helps the organization be more agile in decision making, giving it a competitive advantage.
         b) Structured data are generally well organized and easily searchable (e.g., spreadsheets, public indexes, or database files).
            i) Unstructured data are unorganized or lack a predefined pattern (e.g., word processing documents, videos, photos, or email messages).
c) **Data management** practices help ensure that risk information is useful, timely, relevant, and of high quality. The following are the elements of effective data management:

i) **Data and information governance.** Standards are established for the delivery, quality, timeliness, security, and architecture of data. Roles and responsibilities also are defined for risk information owners and data owners.

ii) **Processes and controls.** Activities are implemented to ensure established data standards are reinforced and corrections are made as necessary.

iii) **Data management architecture.** Information technology is designed that determines what data are collected and how the data are used.

d) Information systems must be **adaptable to change.** As the organization adapts its strategy and business objectives in response to changes in the business context, its information systems also must change.

2) The organization uses **communication channels** to support ERM.

a) Communications about risk.

i) Management communicates the organization’s strategy and business objectives to internal (e.g., personnel and the board) and external (e.g., shareholders) stakeholders.

ii) Communications between management and the board should include continual discussions about **risk appetite**.

b) Channels and methods.

i) Organizations should adopt **open communication channels** to allow risk information to be sent and received both ways (e.g., to and from personnel or suppliers).

ii) **Communication methods** include written documents (e.g., policies and procedures), electronic messages (e.g., email), public events or forums (e.g., town hall meetings), and informal or spoken communications (e.g., one-on-one discussions).

iii) The board may hold **formal** quarterly meetings or call **extraordinary** meetings (special meetings to discuss urgent matters).

3) The organization reports on risk, culture, and performance at multiple levels and across the entity.

a) The purpose of reporting is to support personnel in their

i) Understanding of the relationships among risk, culture, and performance.

ii) Decision making related to (a) setting strategy and objectives, (b) governance, and (c) day-to-day operations.

b) Reporting combines qualitative and quantitative risk information, with greater emphasis on information that supports **forward-looking** decisions.

c) **Management** is responsible for implementing **controls** to ensure reports are accurate, complete, and clear.

d) The **frequency of reporting** is based on the severity and priority of the risk.

e) Reports on **culture** may be communicated, among other means, in surveys and lessons-learned analyses.

f) **Key indicators of risk** should be reported with key performance indicators to emphasize the relationship of risk and performance.
10. **Assessing ERM**
   a. The COSO ERM framework provides criteria for assessing whether the organization’s ERM culture, capabilities, and practices together effectively manage risks to strategy and business objectives.
   b. When the **components**, **principles**, and supporting **controls** are present and functioning, ERM is **reasonably expected** to manage risks effectively and to help create, preserve, and realize **value**.
      1) **Present** means the components, principles, and controls exist in the design and implementation of ERM to achieve objectives.
      2) **Functioning** means the components, principles, and controls continue to operate to achieve objectives.

11. **ERM Limitations**
   a. Limitations of ERM result from the possibility of
      1) Faulty human judgment,
      2) Cost-benefit considerations,
      3) Simple errors or mistakes,
      4) Collusion, and
      5) Management override of ERM practices.

Stop and review! You have completed the outline for this subunit. Study multiple-choice questions 11 through 20 beginning on the next page.
2.2 COSO Framework -- Enterprise Risk Management (ERM)

11. According to COSO, the benefits of enterprise risk management (ERM) include all of the following except

A. Decreased performance variability.
B. Elimination of all risks.
C. Improved resource allocation.
D. Improved risk identification and management.

Answer (B) is correct.

REQUIRED: The item not a benefit of ERM.

DISCUSSION: ERM helps to manage risks, but it does not eliminate risks. Answer (A) is incorrect. ERM helps management decrease performance variability by setting performance tolerances that align with strategy, business objectives, and risk appetite. Answer (C) is incorrect. ERM helps to improve resource allocation by deploying resources based on the severity and priority of risks. Answer (D) is incorrect. ERM helps improve risk identification and management by integrating ERM practices throughout the entire organization, starting with strategy selection through performance results.

12. Management considers risk appetite for all of the following reasons except

A. Aligning with development of strategy.
B. Aligning with business objectives.
C. Implementing risk responses.
D. Setting risk capacity.

Answer (D) is correct.

REQUIRED: The item not a reason for considering risk appetite.

DISCUSSION: Risk appetite consists of the types and amount of risk the entity is willing to accept in pursuit of value. Among other things, risk appetite should be considered in
1. Aligning with development of strategy.
2. Aligning with business objectives.
3. Prioritizing risks.
4. Implementing risk responses.

Risk capacity is the maximum amount of risk an entity is able to assume. Management considers risk capacity in setting risk appetite.

Answer (A) is incorrect. Management considers risk appetite when evaluating strategic options. Answer (B) is incorrect. Management considers risk appetite when setting objectives. Answer (C) is incorrect. Management considers risk appetite when implementing risk responses.

13. Which of the following components are supporting aspects of the COSO ERM framework?

A. Governance and culture; review and revision.
B. Performance; review and revision.
C. Governance and culture; information, communication, and reporting.
D. Strategy and objective-setting; performance.

Answer (C) is correct.

REQUIRED: The components that are supporting aspects of the COSO ERM framework.

DISCUSSION: The supporting aspect components of the COSO ERM framework are (1) governance and culture and (2) information, communication, and reporting. Answer (A) is incorrect. Review and revision is a common process component of the COSO ERM framework. Answer (B) is incorrect. Performance and review and revision are common process components of the COSO ERM framework. Answer (D) is incorrect. Strategy and objective-setting and performance are common process components of the COSO ERM framework.

14. The components of enterprise risk management (ERM) should be present and functioning. What does “present” mean?

I. Components exist in the design of ERM.
II. Components exist in the implementation of ERM.
III. Components continue to operate to achieve strategy and business objectives.

A. I only.
B. II only.
C. I and II.
D. I, II, and III.

Answer (C) is correct.

REQUIRED: The meaning of “present” in the phrase “present and functioning.”

DISCUSSION: The components and principles of ERM, and their related controls, should be present and functioning to help the entity achieve its strategy and business objective. “Present” means such components, principles, and controls exist in the design and implementation of ERM.

Answer (A) is incorrect. The components also should exist in the implementation of ERM. Answer (B) is incorrect. The components also should exist in the design of ERM. Answer (D) is incorrect. “Functioning” means the components, principles, and controls continue to operate to achieve strategy and business objectives.
15. Inherent risk is

A. A potential event that may affect the achievement of strategy and business objectives.
B. A risk response.
C. The risk after management takes action to alter its severity.
D. The risk when management has not taken action to reduce the impact or likelihood of an adverse event.

Answer (D) is correct.

**REQUIRED:** The definition of inherent risk.

**DISCUSSION:** Inherent risk is the risk when management does not act to alter its severity. Severity commonly is measured as a combination of impact and likelihood.

Answer (A) is incorrect. A risk event is a potential event that may affect the entity adversely. Answer (B) is incorrect. A risk response is an action taken to bring identified risks within the entity's risk appetite. Answer (C) is incorrect. The risk remaining after management takes action to alter its severity is actual residual risk.

16. Which risk response reflects a change from acceptance to sharing?

A. An insurance policy on a manufacturing plant was not renewed.
B. Management purchased insurance on previously uninsured property.
C. Management sold a manufacturing plant.
D. After employees stole numerous inventory items, management implemented mandatory background checks on all employees.

Answer (B) is correct.

**REQUIRED:** The risk response reflecting a change from acceptance to sharing.

**DISCUSSION:** The categories of risk responses under the COSO ERM model are avoidance, acceptance, reduction, pursuit, and sharing. If management does not insure a building, the response is acceptance. Acceptance is appropriate when the risk to strategy and business objectives is within the risk appetite. However, once management purchases insurance, the risk is shared with an outside party.

Answer (A) is incorrect. Not renewing insurance is a change from risk sharing to risk acceptance. Answer (C) is incorrect. Selling property avoids all the risks of ownership. Answer (D) is incorrect. Management originally accepted the risk of employee theft by not implementing pre-hire investigations. Conducting background checks on all employees reduces the risk of theft.

17. Enterprise risk management

A. Guarantees achievement of organizational objectives.
B. Requires establishment of risk and control activities by internal auditors.
C. Involves the identification of events with negative impacts on organizational objectives.
D. Includes selection of the best risk response for the organization.

Answer (C) is correct.

**REQUIRED:** The definition of ERM.

**DISCUSSION:** Enterprise risk management (ERM) is defined as the culture, capabilities, and practices, integrated with strategy setting and performance, that organizations rely on to manage risk in creating, preserving, and realizing value.

Answer (A) is incorrect. Risk management processes cannot guarantee achievement of objectives. Answer (B) is incorrect. Involvement of internal auditors in establishing control activities impairs their independence and objectivity. Answer (D) is incorrect. ERM selects not the best risk response but the risk response within the organization’s risk appetite and performance tolerance.

18. According to COSO’s ERM framework, which view of risk is fully integrated?

A. Portfolio view.
B. Risk view.
C. Risk profile view.
D. Risk category view.

Answer (A) is correct.

**REQUIRED:** The fully integrated view of risk.

**DISCUSSION:** A portfolio view is fully integrated. It is a composite view of the risks related to entity-wide strategy and business objectives and their effect on entity performance.

Answer (B) is incorrect. A risk view is minimally integrated. Risks are identified and assessed. Answer (C) is incorrect. A risk profile view is partially integrated. It is a composite view of the types, severity, and interdependencies of risks related to a specific strategy or business objective and their effect on performance. Answer (D) is incorrect. A risk category results from limited integration. The risks identified and assessed in the risk view (minimal integration) are categorized.
19. An entity determined that its variable interest rate on borrowing will increase significantly in the near future. Consequently, the entity hedged its variable rate by locking in a fixed rate for the relevant period. According to COSO, this decision is which type of response to risk?

A. Reduction.
B. Acceptance.
C. Sharing.
D. Avoidance.

Answer (C) is correct.

REQUIRED: The type of risk response.

DISCUSSION: Sharing reduces the risk by transferring a portion of the risk to another party. By entering into a hedging transaction, the entity transferred a portion of the risk to the party that offered the fixed rate.

Answer (A) is incorrect. Reduction lowers the risk so that it is within the target residual risk profile and the risk appetite. Answer (B) is incorrect. Acceptance takes no action to alter the risk. Answer (D) is incorrect. Avoidance ends exposure to the risk. Not borrowing is the avoidance response.

20. An entity defines its risk appetite in which component of the COSO ERM framework?

A. Performance.
B. Strategy and objective-setting.
C. Governance and culture.
D. Control environment.

Answer (B) is correct.

REQUIRED: The component of the COSO ERM framework in which risk appetite is defined.

DISCUSSION: The entity defines risk appetite in the strategy and objective-setting component of ERM. In defining risk appetite, the entity considers its mission, vision, culture, prior strategies, and risk capacity.

Answer (A) is incorrect. Although the risk appetite concept is applied in the performance component, it is defined in the strategy and objective-setting component. Answer (C) is incorrect. The entity defines its risk appetite in the strategy and objective-setting component of ERM. The governance and culture component is the basis for all of the components. Answer (D) is incorrect. The control environment is a component of the COSO internal control framework, not the ERM framework.