Lecture 2.08

ENTERPRISE RISK MANAGEMENT (ERM)

The business and economic environment is often unpredictable with significant technology evolution, rapidly shifting customer behavior, global influences, and fierce competition—all factors that stress strategic planning and the need to maximize operational capabilities to survive and thrive. All this creates uncertainty, which provides both risk and opportunity, and management must determine how to balance those risks and opportunities in alignment with the objectives of the entity. As you can imagine, this can be an extremely daunting task without an organized ERM approach to help keep up with the pace of change facing entities today.

To respond to the need for this organized approach, COSO developed an ERM framework in 2004 updated it in 2017 to complement the internal control framework previously discussed. COSO’s ERM framework is designed to be applied by all types and sizes of entities to strategically identify events that may affect the entity and to manage those risks in accordance with the entity’s risk appetite, to provide reasonable assurance of achieving the entity’s objectives. As updated in 2017, due to the increasing complexity of business risks, the accelerated rate of emerging new risks, and the demand for better risk reporting, the framework, retitled Enterprise Risk Management—Integrating with Strategy & Performance, dives deeper to redefine risk in relation to strategy and performance and focuses on the need to embed ERM proactively throughout the entity.

Benefits

COSO touts several benefits to implementing its ERM framework:

- Promotes identification and management of entity-wide risks.
- Increases identification of opportunities by examining the pros and cons of possibilities.
- Reduces costs of negative surprises and maximizes positive outcomes.
- Manages performance risks to reduce disruption and increase opportunity.
- Prioritizes and maximizes allocation of resources.
- Enhances entity resilience—the ability to anticipate and respond to change.

Components & Principles Overview

COSO’s new ERM framework has 5 components (COPe RR) and 20 different associated principles as outlined below.

Governance & Culture

1. Exercises board risk oversight
2. Establishes operating structures
3. Defines desired culture
4. Demonstrates commitment to core values
5. Attracts, develops, and retains capable individuals

**Strategy & Objective Setting**
6. Analyzes business context
7. Defines risk appetite
8. Evaluates alternative strategies
9. Formulates business objectives

**Performance**
10. Identifies risks
11. Assesses severity of risks
12. Prioritizes risks
13. Implements risk responses
14. Develops portfolio view

**Review & Revision**
15. Assesses substantial change
16. Reviews risk and performance
17. Pursues improvement in ERM

**Information, Communication & Reporting**
18. Leverages information systems
19. Communicates risk information
20. Reports on risk, culture, and performance

**Governance & Culture**
The first of the five components of the COSO ERM Framework is *Governance and Culture*. It sets the overall tone for the organization, addressing such issues as mission, vision, and core values. Governance encompasses the establishment of oversight responsibilities for ERM and the entity's tone. Culture refers to the ethical mindset, standards of acceptable behavior, and understanding the entity's risk.

**Principle 1: Exercises Board Risk Oversight**
“The board of directors provides oversight of the strategy and carries out governance responsibilities to support management in achieving strategy and business objectives.”

The board's oversight role supports the creation of value in an entity and prevents its decline. The framework catalogs risk oversight responsibilities for boards. These responsibilities include overseeing governance and culture; strategy and objective-setting; performance; information, communications and reporting; and the reevaluation and improvement of practices to enrich entity performance. The board's risk oversight role includes, but is not limited to:
- Cultivating investor and stakeholder relations
- Authorizing management pay and incentives
- Reevaluating, questioning, and agreeing with management on:
  - Suggested strategy and target risk appetite
Coordination of strategy and business objectives with the entity's mission, vision, and values

Major decisions including mergers, acquisitions, capital allocations, funding, and dividend-related decisions

Reactions to substantial fluctuations in entity performance or the risk portfolio

Treatment of instances of deviation from values

Management is responsible for managing risks to the entity. To evaluate management's performance, a board generally would determine the answers to the following questions, among others. The answers may illustrate the entity's actual mindset for risk taking as opposed to what appears in documentation.

- Can all levels of management—not just senior management—articulate how risk is considered in the selection of strategy or business decisions?
- Can all levels of management clearly articulate the entity's target risk appetite and how it might influence a specific decision?
- How does the culture promote or retard responsible risk taking?
- How does management monitor the risk culture and how it changes? What changes have occurred?
- As changes occur, how does management ensure a suitable and prompt response?

Principle 2: Establishes operating structures
“The organization establishes operating structures in the pursuit of strategy and business objectives.”

Principle 3: Defines desired culture
“The organization defines the desired behaviors that characterize the entity's desired culture.”

Principle 4: Demonstrates commitment to core values
“The organization demonstrates a commitment to the entity's core values.”

Principle 5: Attracts, develops, and retains capable individuals
“The organization is committed to building human capital in alignment with the strategy and business objectives.”

Principles 2 through 5 represent the internal environment, which sets the tone for the organization. It establishes a basis for the analysis of risk, incorporating management’s philosophy, the entity's risk appetite, and the values that are important to the entity, such as integrity and ethical values.

The internal environment is exhibited in a variety of ways, both formal and informal. Some of the more formal components will include the entity's mission statement and its code of conduct. These should be evident in all aspects of the entity and should be incorporated into the entity's culture. A well-designed mission statement may address some or all of the following:

- The moral or ethical position of the entity and its desired public image
- The key strategic influence for the entity's operations
- A description of the entity's products or services, target market, and geographical domain
- Expectations in relation to growth and profitability

The informal aspect of the internal environment is probably the most important. It is comprised of the actual behavior of members of management and others who might be seen as influential within the organization. Whenever the behavior of such individuals is in conflict with the entity's
mission statement or core values, or its formal policies and procedures, individuals both inside the organization and outside of it will assign more significance to the behavior.

One significant aspect of management and executive behavior is the relationship established with employees. Management should exhibit a willingness to tolerate mistakes, listen, and learn.

**Strategy & Objective Setting**

The second component of the COSO ERM Framework is *Strategy & Objective Setting*. It represents the entity's process for strategic planning. The entity determines its risk appetite, aligns it with its strategy, and develops business objectives to execute the strategy. This process serves as a basis for recognizing, evaluating, and responding to risk.

**Principle 6: Analyzes Business Context**

“The organization considers potential effects of business context on risk profile.”

Business context refers to the environment in which the business operates. ERM involves considering a full range of potential events, enabling management to identify and take advantage of opportunities. Also see principle 10.

**Principle 7: Defines Risk Appetite**

“The organization defines risk appetite in the context of creating, preserving, and realizing value.”

It is important for management to consider what level of risk is acceptable when evaluating alternatives, establishing goals, and developing policies, procedures, and other mechanisms to manage risks. For example, an entity should consider its risk appetite when determining its policy regarding the amount of information that must be obtained about a potential customer and how much must be verified independently before extending credit in order to avoid selling to someone who is not likely to pay.

**Principle 8: Evaluates Alternative Strategies**

“The organization evaluates alternative strategies and potential impact on risk profile.”

Strategy is about developing a plan of action to achieve the entity's objectives. In evaluating alternative strategies, the entity must first align potential business strategies with the entity's mission, vision, and core values, and then determine the impact of those strategies with respect to the entity's risk profile (i.e. risk appetite). COSO's ERM framework provides 3 types of risks to consider in this process:

- **Risks to a chosen strategy** and the performance of that strategy—These are factors an entity should address when choosing a strategy, such as customer demand, supply, competition, and technology infrastructure.
- **Risks that the strategy chosen will not align with the mission, vision, and values**—Even if a strategy is successful, a misaligned strategy increases the risk that the entity will not achieve its mission and vision, or its values will be compromised. While some entities have been reluctant to truly embrace their mission, vision, and values, they have been shown to be extremely important to risk management and resilience in times of change.
- **Risks of, or from, the chosen strategy**—Every choice has some downsides. The risks of the strategy that is chosen should be considered and aligned with the risk appetite of the entity. The board and management should determine how the strategy will steer the entity in setting objectives and whether resources will be allocated efficiently.
Note: It's important to realize that ERM is as much about understanding all the risks as it is about managing them to enhance the performance of the entity.

**Principle 9: Formulates Business Objectives**

“The organization considers risk while establishing the business objectives at various levels that align and support strategy.”

While an entity’s mission describes what it would like to accomplish, it does not set out a specific plan for accomplishing the mission. Management translates the mission into goals or objectives that support the mission and take into account the entity’s risk appetite. The *department manager* would be the best person to devise and execute the risk procedures for a particular department, as they are the most able to identify risky events within that department.

There are four types of business objectives to establish:

- **Setting objectives** begins at the top with *strategic objectives*, which establish a unifying theme for the entity and direct actions and decisions. While strategic objectives set the direction for the entity, objectives related to *operations, reporting, and compliance* provide the mechanisms for meeting those objectives. To be most effective, objectives should be set at each level and, when appropriate, in each of the three categories. A division manager, for example, should know what outputs their division is expected to provide, to whom, to what specifications, and on what timetable so that the manager can make the decisions that will accomplish those objectives.

- The strategic objectives may relate to the quality and other characteristics of the outputs and how the division will be operated. In order to achieve the strategic objective as to quality, the division manager will need the appropriate raw materials, qualified laborers, and the equipment or other resources necessary to convert those inputs into the desired outputs. *Operational objectives*, as a result, may be set to address the acquisition of raw materials, the screening and assignment of laborers, the acquisition and maintenance of equipment and support, and the process for completing the outputs.

- **Reporting objectives** would be established to determine how the division is progressing toward meeting the operational objectives and, ultimately, the strategic objectives. The manager will need to devise a means of determining if the needs of the customer are being met. This may involve obtaining feedback from a subsequent department as to the quality and amount of output that is being transferred. It may involve obtaining feedback from the work force as to the quality of the raw materials that are being provided or from supervision regarding the efficiency of the labor. Achievement of reporting objectives may require sophisticated reports that provide a large amount of information manipulated in a variety of ways. The most effective information is often limited in scope to one or very few parameters, does not require a great deal of effort to accumulate and report on a timely basis, and can be simply understood.

- **Compliance objectives** make certain that the division operates within appropriate guidelines, including both regulatory requirements and internal company policies. This includes making certain that employees are not working against the better interests of the employing entity. At the same time, they must be designed so that an employee does not violate requirements externally imposed in a misguided attempt to help the entity.
**Performance**

The third component of COSO’s ERM Framework is *Performance*. It represents the process of actually identifying, evaluating, and responding to risks. The risks should be prioritized by severity with regard to the entity’s risk appetite. The entity then chooses the appropriate responses, while keeping an overall view of the amount of risk assumed. Results are reported to the appropriate stakeholders.

**Principle 10: Identifies Risks**

“The organization identifies risk that impacts the performance of strategy and business objectives.”

The occurrence or nonoccurrence of certain events (i.e., risks) will determine whether or not the entity will achieve its objectives. Thus, risk identification involves determining what those events may be and how to distinguish between those events that representing opportunities, which should be encouraged and exploited, and those representing threats, which should be dealt with in accordance with the entity’s risk appetite.

- **Opportunities must be exploited** in order to gain a competitive advantage, sustain one, or prevent a competitor from obtaining one. As such, opportunities should be considered in developing the strategic and other objectives of the entity. A plan might be established, and resources might be set aside, to take advantage of an opportunity in case it arises. Of course, the amount of effort going into the design of the plan and the resources set aside to take advantage of the opportunity will be a function of the likelihood that the event will occur, which is analogous to risk assessment, and the benefit that will be derived from it, which will be a factor in determining the appropriate response.

- Likewise, **risks must be prepared for** so that the entity does not lose a competitive advantage or allow a competitor to gain one. As a result, adverse events are considered in the entity’s risk management process. The entity will consider the likelihood that an event will occur, the magnitude of the effect of the event, and the amount the effect will be influenced by actions of the entity in determining an appropriate response.

Event identification is primarily the identification and monitoring of the sources of information that pertain to areas of risk for the entity. Since resources are limited, the entity must be discreet in deciding which sources of information will be monitored. One approach, an aspect of risk assessment, is to determine the resources that are critical to achieving the objectives of the entity. The entity might then be able to identify the types of events that would affect that resource and might be able to seek out sources of information that would help the entity estimate the likelihood of the event and alert the entity of its occurrence, or imminent occurrence, on a timely basis. There are various techniques for identifying relevant events for ERM:

- **Event inventories** are detailed lists of the types of events the entity may be subject to due to the industry it is in, its geographic location, or other characteristics of its operations.
- **Internal analysis**, often done as part of routine business planning, may consist of discussions at meetings, or formal processes that are conducted on a routine basis. They utilize information that is developed internally as well as that obtained from external sources including customers, suppliers, and business relationships, as well as from the news, governmental reports, and other general sources.
- **Escalation or threshold triggers**, which involves the establishment of benchmarks or other criteria against which experiences can be compared to identify those that may require attention. These may be routine, such as reports on delinquent accounts receivable that will trigger collection procedures or monitoring devices that warn of factory temperatures exceeding certain limits.
- **Facilitated workshops or interviews** may be conducted for the specific purpose of learning of event indicators. They may involve staff, outside consultants, or experts in
various fields. An auditor, for example, is required to conduct a brainstorming session with key staff to identify fraud risk factors. This enables the auditor to use the combined knowledge and experience of all participants to identify signs of fraud. Similarly, a meeting with factory staff may be useful in identifying signs of an unsafe condition, thereby preventing an undesirable event in the form of an accident.

- **Process flow analysis** involves the consideration of all components of a process including its inputs, tasks, responsibilities, and outputs. The factors affecting each aspect of the process can be considered to identify events that may be relevant, such as a potential scarcity of a resource used as a raw material in the process.

- **Leading event indicators** involves identifying data that is indicative of a pending event, such as an increase in consumer spending, which may correlate with possible increases in future interest rates.

- **Loss event data methodologies** are collections of information regarding past losses that may have been incurred by the entity or others to identify causes or trends. In anticipating allocating a new contract among different manufacturing plants, analyzing returned goods may identify that certain plants are delivering defective parts and the company can avoid a loss by not awarding the contract inappropriately. **Black swan analysis** involves evaluating the occurrence of events that had a negative effect and were unanticipated or viewed as highly unlikely.

ERM also identifies categories of events, including:

- **Internal** factors such as infrastructure, personnel, processes, and technology
- **External** factors such as economy, natural environment, politics, social factors, and technology

Three broad approaches might be employed to identify events that may have an adverse effect on an entity. These approaches are not mutually exclusive and an entity should apply all in its risk assessment at all levels of the organization. These three approaches can be described as a balance sheet approach, a process approach, and an event identification approach.

- **Under the balance sheet approach**, the entity should identify the resources within its control and determine which ones might be vulnerable and the degree of vulnerability. Most any assets might be misappropriated, for example, but the likelihood of misappropriation and the damage the entity would sustain upon misappropriation will be important factors in evaluating risk.
  
  - Assets essential to the achievement of the entity's objectives, such as raw materials; exclusive information, formulae, or processes; and customer lists, for example, might be so essential to the entity that they will require protection regardless of their cost or the likelihood of their misappropriation. Other assets might not be essential to the entity but might be used by employees or general consumers in their everyday lives. These might include cash, supplies, and other assets like certain inventories. The risk evaluation must take into account that these assets are particularly susceptible to misappropriation or other misuse.

  - When applying the balance sheet approach, it is important to consider assets owned by the entity, its intellectual property, and its human resources. It is also important to consider all of the individuals who are in position to create events that will affect the entity. This might include employees with access to, or custody of, assets. As discussed earlier, threats may come from internal sources, including employees, officers, and directors. They may also come from external sources, including competitors and potential competitors, customers, and con artists.
• The **process approach** involves evaluating the processes that are used to achieve the entity's objectives. At the entity level, this might include the process for establishing objectives and allocating resources. All processes, at all levels, should be considered. This will include the process for determining when a raw material or supply should be purchased, the process for providing a service or manufacturing a component of inventory, the process for obtaining supplies, and the process for recording a transaction. The evaluation of risk under this approach includes the consideration of various possibilities. For each possibility, the entity must consider the likelihood that the possibility will become a reality and its consequences. Examples might include the risk that a process will not be performed, that it will not be performed on a timely basis, or that it will not be performed correctly. Consequences may range from being negligible to very significant. Neglecting to perform a process properly may result in defective inventory, a work stoppage, or product liability.

• The **event identification approach** incorporates many of the principles already discussed. One of the most difficult aspects of this approach is limiting the number of areas in which sources for information are sought. This might be accomplished when viewing the entity from the standpoint of competition. In *Contemporary Strategy Analysis*, Robert Grant discusses Michael Porter's Five Forces of Competition. These include customers, suppliers, competitors, potential entrants into the market, and substitutes. The entity should seek to identify events that might affect any of these five forces.
  
  o In the case of **customers**, increases or decreases in the demand for their products or services may affect the demand for the entity's products or services. **Economic events** may make it easier or more difficult for customers to pay for the entity's products or services on a timely basis. **Changes in customers' needs** may make certain features of the entity's products or services more or less valuable to customers. Other types of events may create new customers, such as a change in an industry's manufacturing process that makes the entity's products or services valuable to entities that had no previous use for them.

  o When an entity is evaluating events that may affect suppliers, it must consider all of its suppliers, including suppliers of human resources, financial resources, and physical resources. Events including changes in school enrollments or graduation rates, failing or emerging industries, and shifts in population may affect the supply of human resources. **Economic and social events**, as well as events affecting other entities seeking the same human resources, may affect the compensation and benefits required to attract or retain the appropriate human resources.

  o **Economic events may affect the availability and the cost of capital.** The entity's access to financial resources will also be affected by the availability of investment alternatives. The availability of physical resources may be affected by events related to weather or other natural phenomena. In addition, increases or decreases in the demand for the goods and services of an entity's suppliers will affect the cost and availability of those goods and services to the entity.

  o **Events that affect competitors** also affect the entity. Innovations that result in changes to their processes may provide them with a competitive advantage or eliminate one held by the entity. When operating in a finite market, events that create an advantage to competitors generally result in a disadvantage to the entity. As competitors devote more resources to marketing, they may improve their access to customers and reduce the entity's market share. More resources
devoted to recruiting may increase access to human resources, decreasing those available to the entity. When events affect competitors’ sales volumes, it affects their demand for raw materials, which will affect the price and availability of those raw materials to the entity.

- Events that change the cost of entry into the market will encourage or discourage potential competitors. Events might include those related to the cost of capital, access to customers or suppliers, or the ability to emulate or improve processes. Obviously, events that lower the cost of entry into the market will increase competition, while events that increase it may decrease competition and, at a minimum, will slow down increases in it.

- Substitutes affect the entity in two ways. They are in competition for the attention of suppliers as well as for the attention of customers. Substitutes include those who might use the same resources that are used by the entity. Events that increase or decrease their need for common resources will affect the price and availability of those resources to the entity. In addition, the extent to which events will cause customers to see other products or services as substitutes for those of the entity will increase or decrease demand for the entity’s products or services.

**Principle 11: Assesses Severity of Risk**

“The organization assesses the severity of risks.”

Management must evaluate the extent of potential effects of identified events on the ability of the entity to achieve its objectives. The likelihood of the occurrence of each identified risk is measured as well as the potential effect on the entity if the event were to occur. Here’s three approaches used to quantify risk:

- **Benchmarking**, which compares expected outcomes to common measures.
- **Probabilistic models**, which develop expected values using probabilities of possible outcomes (quantifying risk).
- **Nonprobabilistic models**, which use subjective assumptions to measure possible outcomes (qualitative, but not quantitative).

**Principles 12. Prioritizes Risks**

“The organization prioritizes risks as a basis for selecting responses to risks.”

Once management has identified and assessed the severity of the risks that may affect the entity’s ability to achieve its objectives, it can decide how to prioritize the risks so that management can effectively assess capital needs and allocate capital where it is most needed or will be most productive.

**Principle 13. Risk Response**

“The organization identifies and selects risk responses.”

When deciding on an appropriate risk response, the entity must consider inherent risk and residual risk.

- **Inherent risk** is the risk to the entity if no action is taken.
- **Residual risk** is the risk to the entity that would remain if action were taken and controls are taken into account.
The *reduction in risk*—basically the difference between an event’s inherent risk and its residual risk—*can be compared to the cost of taking action to determine if action is appropriate*. This type of analysis is also useful in deciding among alternative actions when more than one risk response is available.

Among the **alternative responses to risks** are the decisions to *avoid* a risk, *mitigate* the risk, *share* the risk, or simply *accept* the risk. For example, if there is not sufficient verifiable information about a potential customer, the company can avoid risk by not extending credit, reduce it by limiting the amount of credit extended, share it by entering into an agreement with a third party, such as a bonding company or a guarantor, or accept it by extending credit.

- **Acceptance** of a risk indicates that the entity would take no action and simply allow the event to occur. This would be appropriate when the entity believes that inherent risk is already at an acceptable level or that the cost of taking action would exceed the reduction in risk that would result from the action anticipated.

- If the inherent risk is above an acceptable level, an entity might next seek to share that risk. **Sharing** the risk might involve the use of insurance or fidelity bonds, entering into an arrangement with another entity to share the risk, or outsourcing an activity. Outsourcing may be considered an example of sharing risk or avoiding it. In addition, the risks being “avoided” by the outsourcing entity are taken into account and incorporated in the cost of the product or service being outsourced.

- An entity that cannot find a cost-efficient manner of sharing the risk may decide to reduce it. **Reducing** the risk may require a change in the internal environment or may be accomplished through control activities, which can often reduce risk to an acceptable level. An entity may reduce the risk of inventory misappropriation, for example, by keeping it in a more secure location. It may also minimize losses through early detection. This could be accomplished if the entity maintains a perpetual inventory system and conducts regular and frequent counts. Such a system may be costly, and the costs should be compared to the anticipated reduction in risk to determine whether such control activities would be cost effective.

- When risk cannot be reduced to an acceptable level, **avoidance** may be the best alternative. This may require an entity to change an internal process, eliminate a line of business or product, stop using a particular raw material or buying from a specific supplier, or discontinue selling to a particular customer. An entity may determine that it does not have the ability to monitor receivables efficiently and the cost of reducing losses to an acceptable level would be prohibitive. As a result, the entity may decide to make all sales for cash, checks, and debit or credit cards and discontinue accepting sales on open account.

**Principle 14. Risk Portfolio**

“The organization develops and evaluates a portfolio view of risk.”

ERM is designed to help management evaluate the interrelated impacts of decisions and deal with multiple risks. One risk may combine with other risks or offset other risks. Management must be careful when developing policies and procedures that are designed to affect one issue as, due to the integrated nature of business, it increases a different risk. For example, if we decide not to sell to the customer on credit, we also risk losing the customer to a competitor and adversely affecting the enthusiasm of the sales person who worked to bring the customer in.
**Review & Revision**
The fourth component of the COSO ERM Framework is Review & Revision. It represents the process of evaluating how well ERM components perform over time and refining the components as conditions change, as necessary.

**Principle 15: Assesses substantial change**
“The organization identifies and assesses changes that may substantially affect strategy and business objectives.”

**Principle 16: Reviews risk and performance**
“The organization reviews entity performance and considers risk.”

**Principle 17: Pursues improvement in ERM**
“The organization pursues improvement of enterprise risk management.”

Risk assessment is an ongoing process, not a “one-time” activity. The entire ERM system must be monitored so that changes can be made on a timely basis. Monitoring may be through ongoing management activities or as part of a separate evaluation of the entity's ERM process.

**Information, Communication & Reporting**
The last of the five COSO ERM Framework components is Information, Communication & Reporting. It represents the ongoing exchange of internal and external information up and down as well as across the entity.

**Principle 18: Leverages information and technology**
“The organization leverages the entity's information and technology systems to support enterprise risk management.”

**Principle 19: Communicates risk information**
“The organization uses communication channels to support enterprise risk management.”

**Principle 20: Reports on risk, culture, and performance**
“The organization reports on risk, culture, and performance at multiple levels and across the entity.”

People must have relevant information to carry out their responsibilities. As a result, the entity must have a means of identifying what information is pertinent from all of its internal and external sources.

Relevant information may be financial or nonfinancial and may be quantitative or qualitative in nature. It may also be formal or informal, such as that derived from conversations with customers or suppliers. It can potentially come from such a wide range of sources that it becomes very important for an entity to determine what sources are reliable as well as what information is relevant.
Once identified, relevant information must be captured, processed, and communicated to those who can benefit from it. It must be put into a form that is usable and must be provided on a timely basis so that decisions can be made to prevent losses.

Communication must include parties to whom it is relevant. It is most effective when lines of communication move in all directions within and around an organization. There should be communication at all levels, including upward and downward communication. Likewise, relevant information should be communicated with customers or suppliers to enhance the entity's ability to meet the needs of customers and have its needs met by suppliers.

**Inherent Limitations of ERM**

Applying ERM may enhance an entity's opportunity to be successful, but it does not ensure it. Regardless of how well a system is designed, implemented, and operated, there are certain inherent limitations on ERM:

- The future, by its nature, cannot be predicted with certainty.
- Some events are beyond management’s control and, due to the need to allocate scarce resources, the entity will not necessarily be able to pursue all objectives to the extent desired.
- No system process, regardless of how well designed and managed, will necessarily always accomplish what it is intended to accomplish (i.e., there is no absolute assurance).

As is true of most systems, ERM can provide reasonable, but not absolute assurance that objectives will be met. Some of the reasons that this is the case include:

- Decisions made in designing, implementing, and operating a system are often largely depending on human judgment, which is not perfect.
- Systems can suffer breakdowns due to changes in personnel, technology, or the failure of any component of the system.
- Systems can be overcome by dishonest individuals through collusion, which negates effective segregation of duties.
- Decisions in design, implementation, and monitoring always require an analysis of costs versus benefits because entities do not have unlimited resources.
- Effective controls are often subject to management override.
Lecture 2.09

13. Which of the following activities would the COSO Enterprise Risk Management framework consider part of the governance and culture component?
   a. Demonstrating commitment to core values
   b. Formulating business objectives
   c. Defining risk appetite
   d. Leveraging information and technology

14. A manufacturing firm identified that it would have difficulty sourcing raw materials locally, so it decided to relocate its production facilities. According to COSO, this decision represents which of the following responses to the risk?
   a. Risk reduction
   b. Prospect theory
   c. Risk sharing
   d. Risk acceptance

15. Each of the following is a limitation of enterprise risk management (ERM), except:
   a. ERM deals with risk, which relates to the future and is inherently uncertain.
   b. ERM operates at different levels with respect to different objectives.
   c. ERM can provide absolute assurance with respect to objective categories.
   d. ERM is as effective as the people responsible for its functioning.

16. According to COSO, under which of the following components of enterprise risk management does the practice of prioritizing risks fall?
   a. Information, Communication & Reporting
   b. Strategy & Objective Setting
   c. Performance
   d. Review & Revision
13. (a) Demonstrating commitment to core values is a principle that COSO classifies under the Governance & Culture component. Answer (b) is incorrect because formulating business objectives is a principle that COSO classifies under the Strategy & Objective Setting component. Answer (c) is incorrect because defining the risk appetite is a principle that COSO classifies under the Strategy & Objective Setting component. Answer (d) is incorrect because Leveraging information and technology is a principle that COSO classifies under the Information, Communication & Reporting component.

14. (a) By moving its production facility, the entity improves its access to raw materials. This reduces the risk that raw materials will not be obtainable, which would represent a risk to the achievement of the entity's objective. Answer (b) is incorrect because prospect theory is not an ERM component. Answer (c) is incorrect because risk sharing would involve taking action, such as entering into a joint venture, so that other entities share losses if the risk materializes. Answer (d) is incorrect because risk acceptance would involve taking no action to mitigate the risk.

15. (c) ERM cannot provide absolute assurance with respect to objective categories since it deals with future actions which are inherently uncertain and is dependent on people who may commit errors or may not share in the entity's ethical values. It is instead designed to provide reasonable, not absolute assurance, as to the achievement of the entity's objectives.

16. (c) According to COSO's enterprise risk management framework, the prioritization of risk is a practice that occurs within the Performance component. Answer (a) is incorrect because Information, Communication & Reporting relates to how the entity obtains and develops information and how it is disseminated. Answer (b) is incorrect because the Strategy & Objective Setting component represents the entity's process for strategic planning, where the entity determines its risk appetite, aligns it with its strategy, and develops business objectives to execute the strategy. Answer (d) is incorrect because Review & Revision represents the process of evaluating how well ERM components perform over time and refining the components as conditions change.