

COSO ERM Framework Overview

Enterprise Risk Management—Integrating with Strategy and Performance clarifies the importance of enterprise risk management in strategic planning and embedding it throughout an organization—because risk influences and aligns strategy and performance across all departments and functions.

ENTERPRISE RISK MANAGEMENT



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.






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.

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.

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.

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.

COSO ERM Framework Overview

| COSO ERM COMPONENTS | ERM Principles |
|--|---|
|  Governance & Culture | <ol style="list-style-type: none"> 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. Establishes Operating Structures—The organization establishes operating structures in the pursuit of strategy and business objectives. Defines Desired Culture—The organization defines the desired behaviors that characterize the entity’s desired culture. Demonstrates Commitment to Core Values—The organization demonstrates a commitment to the entity’s core values. Attracts, Develops, and Retains Capable Individuals—The organization is committed to building human capital in alignment with the strategy and business objectives. |
|  Strategy & Objective-Setting | <ol style="list-style-type: none"> Analyzes Business Context—The organization considers potential effects of business context on risk profile. Defines Risk Appetite—The organization defines risk appetite in the context of creating, preserving, and realizing value. Evaluates Alternative Strategies—The organization evaluates alternative strategies and potential impact on risk profile. Formulates Business Objectives—The organization considers risk while establishing the business objectives at various levels that align and support strategy. |
|  Performance | <ol style="list-style-type: none"> Identifies Risk—The organization identifies risk that impacts the performance of strategy and business objectives. Assesses Severity of Risk—The organization assesses the severity of risk. Prioritizes Risks—The organization prioritizes risks as a basis for selecting responses to risks. Implements Risk Responses—The organization identifies and selects risk responses. Develops Portfolio View—The organization develops and evaluates a portfolio view of risk. |
|  Review & Revision | <ol style="list-style-type: none"> Assesses Substantial Change—The organization identifies and assesses changes that may substantially affect strategy and business objectives. Reviews Risk and Performance—The organization reviews entity performance and considers risk. Pursues Improvement in Enterprise Risk Management—The organization pursues improvement of enterprise risk management. |
|  Information, Communication, & Reporting | <ol style="list-style-type: none"> Leverages Information Systems—The organization leverages the entity’s information and technology systems to support enterprise risk management. Communicates Risk Information—The organization uses communication channels to support enterprise risk management. Reports on Risk, Culture, and Performance—The organization reports on risk, culture, and performance at multiple levels and across the entity. |

COSO ERM Framework Overview

Enterprise risk management is as much about understanding the implications from the strategy and the possibility of strategy not aligning as it is about managing risks to set objectives. The figure below illustrates these considerations in the context of mission, vision, core values, and as a driver of an entity's overall direction and performance.

