

COSO Enterprise Risk Management 2017

Risk management Components



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

Five components of ERM Framework 2017

ENTERPRISE RISK MANAGEMENT



Governance & Culture



Strategy & Objective-Setting



Performance



Review & Revision



Information, Communication, & Reporting

COSO ERM Components and principles

GOVERNANCE AND CULTURE

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.

2. Establishes Operating Structures —

The organization establishes operating structures in the pursuit of strategy and business objectives.

3. Defines Desired Culture —

The organization defines the desired behaviors that characterize the entity's desired culture.

4. Demonstrates Commitment to Core Values —

The organization demonstrates a commitment to the entity's core values.

5. Attracts, Develops, and Retains Capable Individuals —

The organization is committed to building human capital in alignment with the strategy and business objectives.



STRATEGY AND OBJECTIVE-SETTING

6. Analyzes Business Context —

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

7. Defines Risk Appetite —

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

8. Evaluates Alternative Strategies —

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

9. Formulates Business Objectives —

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



PERFORMANCE

10. Identifies Risk —

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

11. Assesses Severity of Risk —

The organization assesses the severity of risk.

12. Prioritizes Risks —

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

13. Implements Risk Responses —

The organization identifies and selects risk responses.

14. Develops Portfolio View —

The organization develops and evaluates a portfolio view of risk.

REVIEW AND REVISION

15. Assesses Substantial Change —

The organization identifies and assesses changes that may substantially affect strategy and business objectives.

16. Reviews Risk and Performance —

The organization reviews entity performance and considers risk.

17. Pursues Improvement in Enterprise Risk Management —

The organization pursues improvement of enterprise risk management.

INFORMATION, COMMUNICATION, AND REPORTING

18. Leverages Information Systems —

The organization leverages the entity's information and technology systems to support enterprise risk management.

19. Communicates Risk Information —

The organization uses communication channels to support enterprise risk management.

20. Reports on Risk, Culture, and Performance —

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

