The COSO risk framework: A reference for internal control?

Transition from COSO I to COSO II

Annie Bressac
Consultant

COSO II
Enterprise Risk Management – Integrated Framework

Background & objectives
Insights
Underlying principles of COSO-ERM:

- Every entity exists to realize value for its shareholders
- Every entity has to deal with uncertainty
  - The COSO II framework is designed to enable management:
    - To deal effectively with potential future events that create uncertainty
    - To respond in a manner that reduces the likelihood of downside outcomes and increases the upside

The ERM Definition

- Enterprise Risk Management is:
  - A process
  - Effected by an entity’s board of directors, management and other personnel,
  - Applied in strategy setting and across the entity
  - Designed to identify and manage potential events that may affect the entity, and
  - To provide reasonable assurance regarding the achievement of entity objectives.
The ERM Framework

1. **The Enterprise Risk Management framework has eight interrelated components**

2. **Entity objectives can be viewed in the context of four categories**
   - Strategic
   - Operations
   - Reporting
   - Compliance

3. **ERM considers activities at all levels of the organization**

**Internal environment includes:**
- Risk management philosophy and risk culture
- Risk appetite: a high-level view of how much risk the management and the board are willing to accept
- All other aspects of how the organization’s actions may affect its risk culture

**Objective Setting**
- Is applied when management considers risks strategy in the setting of objectives
- Objectives are set with regard to the risk appetite
- A level of variation is accepted for objectives (risk tolerance)
The ERM Framework

**Event identification:**
- Identify those incidents, occurring internally or externally, that could affect strategy and achievement of objectives
- Addresses how internal and external factors combine and interact to influence the entity’s risk profile
- Distinguishes risk and opportunity

**Risk assessment:**
- Allows an entity to understand the extent to which potential events might impact objectives
- Assesses risks:
  - from two perspectives: likelihood and impact
  - on both an inherent and residual basis
- Employs a combination of both qualitative and quantitative risk assessment methodologies

**Risk response:**
- Identifies and evaluates possible responses to risk: avoiding, accepting, reducing, sharing
- Evaluates options in relation to entity’s risk appetite
- Selects and executes response based on evaluation of the portfolio of risks and responses

**Control activities:**
- Policies and procedures that help ensure that risk responses are carried out
- Occur throughout the organization, at all levels and in all functions
- Include application controls and general information technology controls
The ERM Framework

**Information & Communication:**
- Management identifies, captures, and communicates pertinent information in a form and timeframe that enables people to carry out their responsibilities.
- Communication occurs in a broader sense, flowing down, across, and up the organization.

**Monitoring:**
- Monitors the ongoing effectiveness of the other enterprise risk management components through:
  - Ongoing monitoring activities
  - Separate evaluations
  - A combination of the two

Roles and Responsibilities

**Four broad areas of roles and responsibilities:**
- The Board of Directors is responsible for overseeing management’s design and operation of ERM.
- Management is responsible for the design of an entity’s enterprise risk management framework.
- Risk officers work with managers in establishing and maintaining effective risk management.
- Internal auditors contribute to the ongoing effectiveness of the enterprise risk management.
COSO ERM: A reference for internal control?

Transition from COSO I to COSO II

- COSO II doesn’t replace COSO I which remains as a stand-alone internal control framework.
- COSO ERM incorporates the IC framework: A strong system of internal control is essential to effective enterprise risk management.
- COSO ERM expands and elaborates on elements of internal control as set out in COSO Internal Control Framework.
Transition from COSO I to COSO II

Value and utility of COSO ERM

COSO ERM brings to all the « control stakeholders »:

- A definition of risk management
- A vocabulary, concepts and principles shared by all the parties involved
- Criteria to evaluate the effectiveness of risk treatment strategies
- Guidelines for entities to improve their risk management system
Value and utility for managers

ERM process improves capacity to build value
- Align strategy with risk appetite
- Enhance risk response decisions
- Reduce the likelihood and/or impact of negative events and therefore operational losses
- Seize opportunities
- Identify and manage multiple and cross-enterprise risks

Value and utility for internal auditors

- Play an important role in monitoring ERM, but
- Do NOT have primary responsibility for its implementation or maintenance.

- Assist management and the board or audit committee in the process by:
  - Monitoring
  - Evaluating
  - Examining
  - Reporting
  - Recommending improvements
**COSO II extends and strengthens the evolution initiated by COSO I**

- **Bring together risk culture and control culture**

- **Strengthen the link between internal control, risks, and achievement of objectives:**
  - Pertinence and legitimacy of internal control considering its added value to an effective risk control
  - Relevance of the controls implemented to the previous identification and assessment of risks