The COSO Risk Framework: A reference for internal control ?

Transition from COSO I to COSO II

ENTERPRISE RISK MGMT INTEGRATED FRAMEWORK (COSO II)

UNIVERSITA' degli STUDI di ROMA TOR VERGATA

COURSE OF BUSINESS AUDITING
UNIVERSITY OF ROME TOR VERGATA

NOVEMBER 2022

PROF FABIO ACCARDI

COSO II
Enterprise Risk Management – Integrated Framework 2004

- Underlying principles of COSO-ERM:

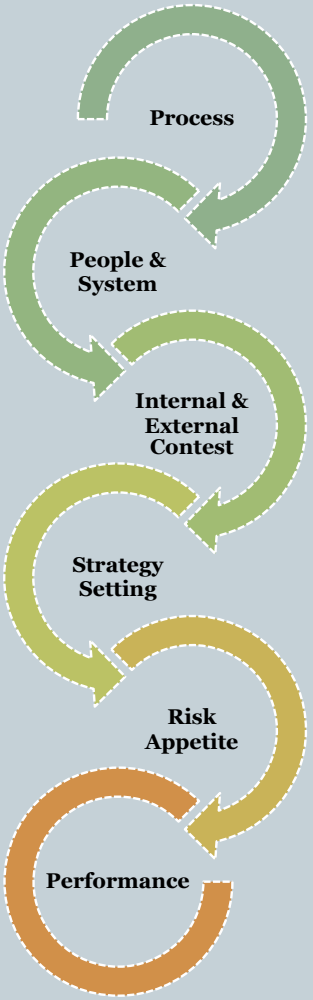
Every entity exists to realize value for its shareholders

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**
- (continuous series of interactive actions pervading the entire company)
- **effected by an entity's board of directors, management and other personnel**
- (ERM implementation concerns all company actors)
- **applied in strategy setting and across the enterprise**
- (the knowledge of risks makes it possible to choose among the strategic alternatives those that are most suited to the corporate risk appetite)
- **designed to identify potential events that may affect the entity**
- (in the process of identifying possible events we must distinguish the opportunities from risks, and on these concentrate the risk management)
- **and manage risk to be within its risk appetite**
- (the acceptable risk represents the amount of risk that a company is willing to run to pursue value creation. The definition of acceptable risk influences the strategic choices and the allocation of resources)
- **to provide reasonable assurance regarding the achievement of entity objectives**
- (ERM helps in pursuing the objectives, but can not give the security of their achievement)

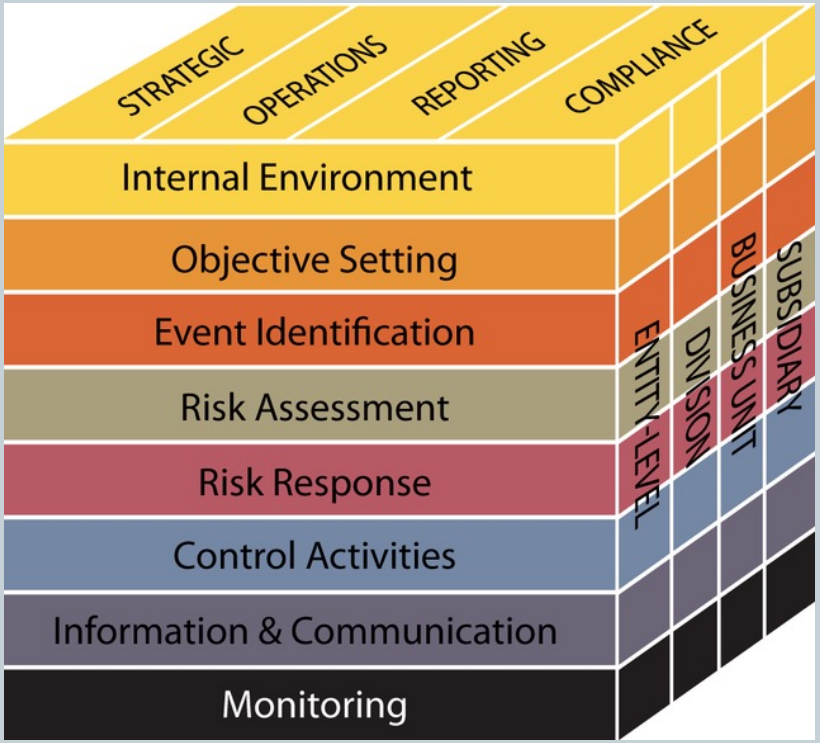


The ERM Framework

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



ERM: Relationship between COMPONENTS, objectives and ORGANIZATION levels

- The 8 components of the ERM apply to each objectives category and to the entity as a whole and to its different levels / processes / functions.

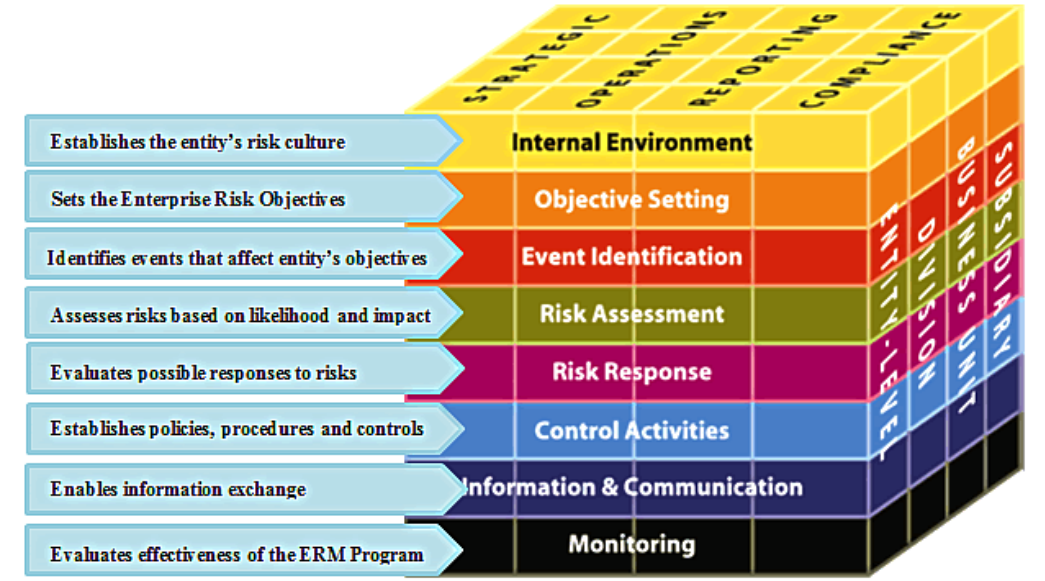
- **STRATEGIC**
- Aligned with the company mission, strategic objectives are declined and contextualized in the other 3 categories of objectives;

- **OPERATING**
- Effective and efficient use of resources

- **REPORTING**
- Reliability of internal and external information

- **COMPLIANCE**
- compliance with laws and regulations

“ERM 2004” 8 components



“ERM 2004” 8 COMPONENTS

Internal environment

It embodies the essential identity of an organization and determines the ways in which the risk is to be tackled. Therefore, it can be considered as the very foundation of the other components of the Enterprise Risk Management. The internal environment is affected/influenced by factors such as the philosophy of risk management, the level of acceptable risk, the supervision of the Board, the integrity, ethical values, competence, the modalities of the delegation of powers and responsibilities, training staff

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

The definition of objectives is a prerequisite for an effective event identification, risk assessment and risk response. The strategic objectives are the foundation in order to define the operational objectives, reporting, and compliance. In choosing targets, companies must make sure to align themselves to acceptable risk, fixed by the companies themselves, that are determined according to the levels of risk tolerance

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)

Event identification

Management must identify events that may affect the company. If they compromise the achievement of the objectives, they represent risks that require evaluation and determination of response measures. If they have a positive impact, they represent opportunities worth pursuing in redefining strategies. The events are influenced by internal and external factors, and their identification involves the application of structured techniques

Event identification

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

4 – Valutazione dei Rischi

Risk assessment measures the repercussions of a potential event on the achievement of objectives in terms of likelihood and impact, through qualitative and/or quantitative techniques. The evaluation regards the individual event categories of potential events interconnected with the various levels of the company. Risks can be assessed in terms of inherent risk (i.e., independent from the existing control system) and in terms of residual risk, which considers the effects on the probability and/or impact of the activated risk responses

Risk assessment :

- Allows an entity to understand the extent to which potential events might impact objectives
- Assesses risks: 1) from two perspectives: likelihood and impact; 2) on both an inherent and residual basis
- Employs a combination of both qualitative and quantitative risk assessment methodologies

“ERM 2004” 8 COMPONENTS

Risk Response

Based on the risk assessment, management must select the most appropriate responses to the risk (e.g., avoiding the risk, reducing it, sharing it, accepting it). The choice depends on several factors: cost/benefit analysis; desired effects on the probability/ impact; capacity to reduce risk within the limits of tolerance. The risk mitigation strategy should allow bringing the overall level of residual risk within the limits of acceptability set by top management

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

Control activities are the application of policies and procedures to ensure the implementation of directives to address the risks that may affect the achievement of the objectives. Control activities are implemented at all levels of the organization, and may consist of approvals, authorizations, verifications, reconciliations, review of operational performance, protection of company assets, separation of duties

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

Information and Communication

The company should identify, collect, and disseminate relevant information to enable everyone to fulfill their responsibilities. They must take the form of implemented information systems that deal with both internal and external information for the risk management and decision making. Effective communication flow must be ensured through the entire organization: top-down (e.g., communication objectives); bottom-up (significant reports);
transversal (i.e., management processes); third parties.

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

Monitoring fulfils the function of assessing in real time the presence and operation of the components of the control and risk management system. It is carried out through continuous supervision, by the operating management, or through specific testing and evaluation systems. The monitoring scope and frequency depends on the risk assessment and effectiveness of continuous oversight

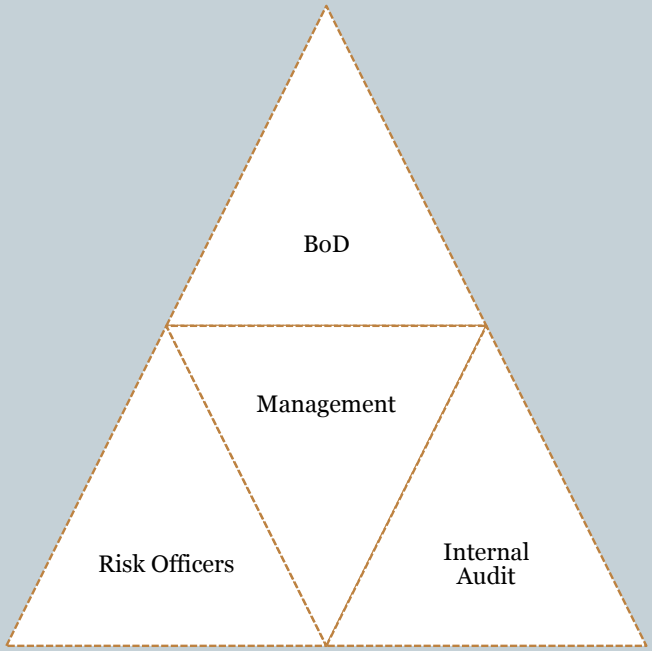
Monitoring :

- 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:

1. The Board of Directors is responsible for overseeing management's design and operation of ERM
2. Management is responsible for the design of an entity's enterprise risk management framework
3. Risk officers work with managers in establishing and maintaining effective risk management
4. Internal auditors contribute to the ongoing effectiveness of the enterprise risk management

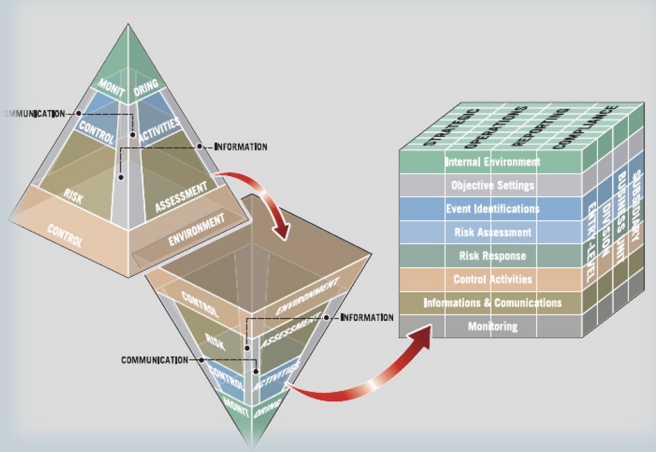


Relationships between COSO I and ERM

COSO (2004) was first published in 2004 and it represents an evolution with respect to the framework of COSO (1992). The ERM model, formalized subsequently with respect to COSO Report I, has intended not to replace the previous framework but to incorporate it in order to systematically satisfy both internal control and company risk management needs. The principal aspects in which we can summarize the transition from COSO (1992) to COSO (2004) are:

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 (by bringing together risk culture and control culture; by strengthening the link between internal control, risks, and achievement of objectives through: i. pertinence and legitimacy of internal control considering its added value to an effective risk control; ii. relevance of the controls implemented to the previous identification and assessment of risks)

Relationships between COSO I and ERM



ERM incorporates its predecessor, the CoSo Report, but reverses its logic:

THE FOCUS IS NO LONGER ON CONTROL
BUT ON RISK
SINCE CONTROL IS A MEANS

Adequacy of internal controls depends on thier ability to maintain risk within the risk appetite

Breakdown and expansion of the internal control and risk management process through 3 additional components, specific for risk management

Greater connection between internal control systems and risk management and business strategy

Evaluation of risks and opportunities in holistic terms, appreciating the correlation between events

Introduction of the concepts of risk appetite, acceptability of risk and risk tolerance

COSO II extends and strengthens the evolution initiated by COSO I

Bring together risk culture and control culture

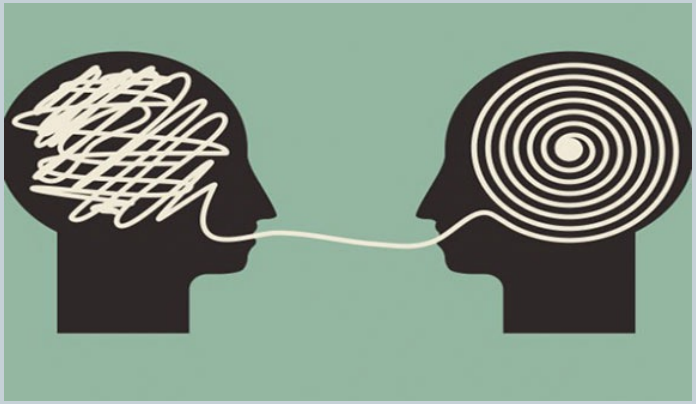
Strengthen the link between internal control, risks, and achievement of objectives:

1. Pertinence and legitimacy of internal control considering its added value to an effective risk control
2. Relevance of the controls implemented to the previous identification and assessment of risks

Value and utility of COSO ERM

COSO ERM brings to all the « control stakeholders:

1. A definition of risk management
2. A vocabulary, concepts and principles shared by all the parties involved
3. Criteria to evaluate the effectiveness of risk treatment strategies
4. Guidelines for entities to improve their risk management system



Value and utility for managers

ERM process improves capacity to build value

1. Align strategy with risk appetite
2. Enhance risk response decisions
3. Reduce the likelihood and/or impact of negative events and therefore operational losses
4. Seize opportunities
5. Identify and manage multiple and cross- enterprise risks

Value and utility for internal auditors

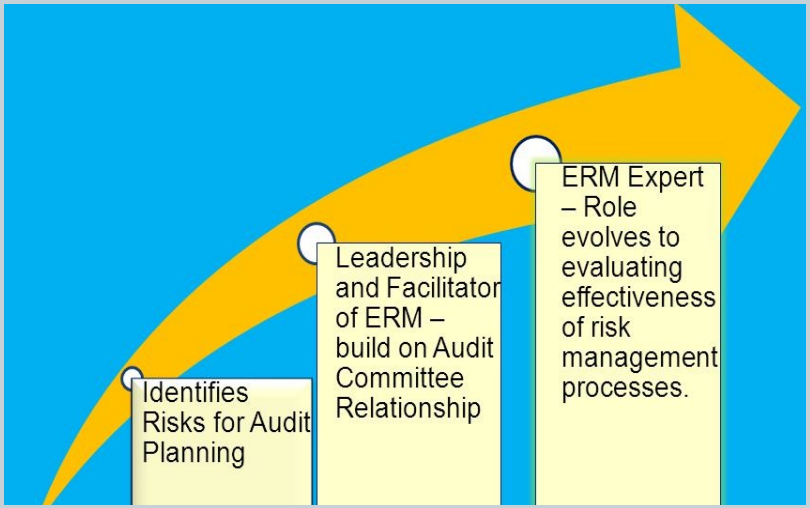
Play an important role in monitoring ERM, but

Do NOT have primary responsibility for its implementation or maintenance

Assist management and the board or audit

committee in the process by:

1. Monitoring
2. Evaluating
3. Examining
4. Reporting
5. Recommending improvements



ERM Maturity level

The difference between entities can outline different priorities and place emphasis on the objectives of ERM, and this can influence the way the framework operates in terms of components (COSO, 2004)

The eight components will not function identically in every entity. Application in small and mid-size entities, for example, may be less formal and less structured. Nonetheless, small entities still can have effective enterprise risk management, as long as each of the components is present and functioning properly