Management's Responsibility for Internal Control and Enterprise Risk Management

Mark T. Hobbs, CPA
The Hobbs Group, P.A.

TheHobbsGroup
CERTIFIED PUBLIC ACCOUNTANTS & CONSULTANTS, PA

History of COSO

- COSO was formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, an independent private-sector initiative which studied the causal factors that lead to fraudulent financial reporting. It also developed recommendations of public companies and their independent auditors, for the SEC and other regulators, and for educational institutions.
- The Treadway Commission studied the financial information reporting system over the period from October 1985 to September 1987 and issued a report of findings and recommendations in October 1987 titled *Report of the National Commission on Fraudulent Financial Reporting*[1]. As a result of this initial report, the Committee of Sponsoring Organizations (COSO) was formed and it retained Coopers & Lybrand, a major CPA firm, to study the issues and author a report regarding an integrated framework of internal control.

Major Concepts of COSO Framework

- The COSO framework involves several key concepts:
  - Internal control is a *process*. It is a means to an end, not an end in itself.
  - Internal control is affected by *people*. It's not merely policy, manuals, and forms, but people at every level of an organization.
  - Internal control can be expected to provide only *reasonable assurance*, not absolute assurance, to an entity's management and board.
  - Internal control is geared to the achievement of *objectives* in one or more separate but overlapping categories.

Response to Financial Crisis

- Through the recent years there has been an increasing concern and focus on risk management, and it became clear that there needed to be a **robust framework** to effectively identify, assess, and manage
- In 2001, post Enron COSO initiated a project, and engaged PricewaterhouseCoopers, to develop a framework that would be readily usable by managements to evaluate and improve their organizations' enterprise risk management.
- This Enterprise Risk Management – Integrated Framework expands on internal control, providing a more extensive focus on the broader subject of enterprise risk management.

Enterprise Risk Management

Enterprise Risk Management Encompasses:

- *Aligning risk appetite/tolerance and strategy*- Management considers the entity's risk appetite/tolerance in evaluating strategic alternatives, setting related objectives, and developing mechanisms to manage related risks.

- *Enhancing risk response decisions*- Enterprise risk management provides the rigor to identify and select among alternative risk responses- risk avoidance, reduction, sharing, and acceptance.

- *Reducing operational surprises and losses*- Entities gain enhanced capability to identify potential events and establish responses, reducing surprises and associated costs or losses.

Enterprise Risk Management, Cont'd

- *Identifying and managing multiple and cross enterprise risks*- Every enterprise faces a myriad of risks affecting different parts of the organization, and enterprise risk management facilitates effective response to the interrelated impacts, and integrated responses to multiple risks.

- *Seizing opportunities*- By considering a full range of potential events, management is positioned to identify value of ERM and proactively realize opportunities.

- *Improving deployment of capital*- Obtaining robust information allows management to effectively assess overall capital needs and enhance capital allocation.

Events: Risks and Opportunities

- Events can have negative impact, positive impact, or both.
- Negative Impacts = Risks which can prevent value creation/losses to entity
- Positive Impacts = offsetting to negative impacts or represent opportunities
  - Management channels opportunities back to its strategy or objective-setting processes, formulating plans to seize the opportunities.

Enterprise Risk Management Defined

GOAL – Achieve Entity's Objectives

Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

Enterprise Risk Management

It is:

- A process, ongoing and flowing through an entity
- Effected by people at every level of an organization
- Applied in strategy setting
- Applied across the enterprise, at every level and unit, and includes taking an entity-level portfolio view of risk

Enterprise Risk Management, Cont'd

- Designed to identify potential events that, if they occur, will affect the entity and to manage risk within its risk appetite/tolerance
- Able to provide reasonable assurance (not absolute assurance) to an entity's management and board of directors
- Geared to achievement of objectives in one or more separate but overlapping categories

Achievement of Objectives

- This framework is geared to achieving an entity's objectives, set forth in four categories:
  - Strategic – high-level goals, aligned with and supporting its mission
  - Operations – effective and efficient use of its resources (Abuse – Yellow Book)
  - Reporting – reliability of reporting (Financial/General ledger/Program-Related)
  - Compliance – compliance with applicable laws and regulations

Components of Enterprise Risk Management

- Enterprise risk management consists of eight interrelated components:
  - Internal Environment – The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite/tolerance, integrity and ethical values, and the environment in which they operate.
  - Objective setting – Objectives must exist before management can identify potential events affecting their achievement. ERM ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite/tolerance.

- Event Identification – Internal and external events affecting achievement of an entity's objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management's strategy or objective-setting processes.

- Risk Assessment – Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a continuing basis

Components of Enterprise Risk Management, Cont'd

- Risk Response – Management selects risk responses – avoiding, accepting, reducing, or sharing risk – developing a set of actions to align risks with the entity's risk tolerances and risk appetite.

- Control Activities – Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.

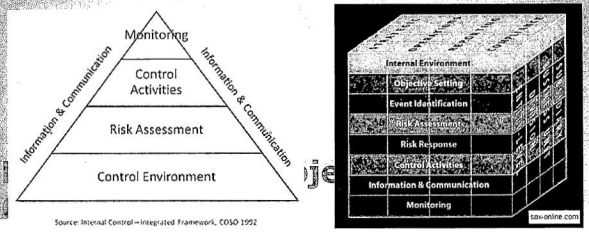
Components of Enterprise Risk Management, Cont'd

- Information and Communication – Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and up the entity.

- Monitoring – The entirety of enterprise risk management is monitored and modifications made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.

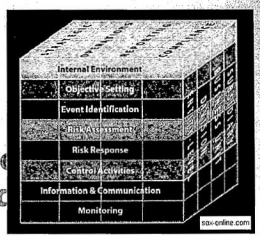
Components of Enterprise Risk Management, Cont'd

- There is a direct relationship between objectives, which are what an entity strives to achieve, and enterprise risk management components, which represent what is needed to achieve them. The relationship is depicted in a three-dimensional matrix, in the form of a cube:



- The four objectives categories – strategic, operations, reporting, and compliance – are represented by the vertical columns, the eight components by horizontal rows, and an entity's units by the third dimension. This depiction portrays the ability to focus on the entirety of an entity's enterprise risk management, or by objectives category, component, entity unit, or any subset thereof.

Source: Internal Control—Integrated Framework, COSO 1992



- Figuring out whether an entity's ERM is "effective" is a judgment resulting from an assessment of whether the eight components are present and functioning effectively.
  - For this to happen there can be no material weaknesses, and risk needs to have been brought within the entity's risk appetite/tolerance.
- When ERM is determined to be effective in each of the four categories of objectives, respectively, the board of directors and management have reasonable assurance that they understand the extent to which the entity's strategic and operations objectives are being achieved, and that the entity's reporting is reliable and applicable laws and regulations are being complied with.

Effectivess

- Limitations result from:
  - The realities that human judgment in decision making can be faulty
  - Decisions on responding to risk and establishing controls need to consider the relative costs and benefits
  - Breakdowns can occur because of human failures such as simple errors or mistakes
  - Controls can be circumvented by collusion of two or more people, and management has the ability to override enterprise risk management decisions.
  - [Not Absolute] Assurance

Limitations

- Everyone in an entity has some responsibility for enterprise risk management. The chief executive officer is ultimately responsible and should assume ownership.
  - Other manager support the entity's risk management philosophy, promote compliance with its risk appetite/tolerance, and manage risks within their spheres of responsibility consistent with risk tolerances.

Roles and Responsibilities

Use of this Presentation

- Board of Directors – The board should discuss with senior management the state of the entity's ERM and provide oversight as needed. The board should ensure it is apprised of the most significant risks, along with actions management is taking and how it is ensuring effective ERM. The board should consider seeking input from internal auditors, external auditors, and others.
- Senior Management – An initial assessment should determine where there is a need for, and how to proceed with, a broader, more in-depth evaluation.

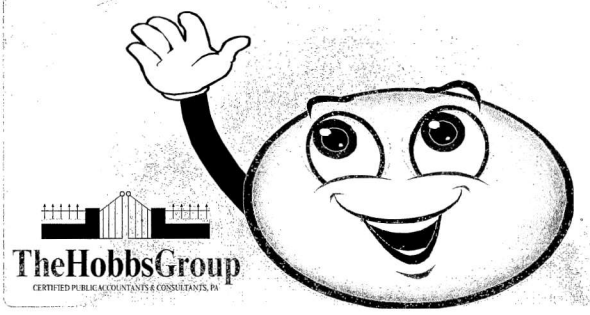
Use of This Presentation, Cont'd

- Other Entity Personnel – Managers and other personnel should consider how they are conducting their responsibilities in light of this framework and discuss with more senior personnel ideas for strengthening ERM. Internal auditors should consider the breadth of their focus on ERM.
- Regulators – This framework can promote a shared view of ERM, including what it can do and its limitations. Regulators may refer to this framework in establishing expectations, whether by rule or guidance or in conducting examinations, for entities they oversee.

Use of This Presentation, Cont'd

- Professional Organizations – Rule-making and other professional organizations providing guidance on financial management, auditing, and related topics should consider their standards and guidance in light of this framework. To the extent diversity in concepts and terminology is eliminated, all parties benefit.
- Educators – This framework might be the subject of academic research and analysis, to see where future enhancements can be made.

Questions or Comments



TheHobbsGroup
CERTIFIED PUBLIC ACCOUNTANTS & CONSULTANTS, PA