Internal Audit’s Evolving Role In Enterprise Risk Management

Dr. Mary Sheets
University Of Central Oklahoma
February 21, 2013
msheets@uco.edu

Enterprise risk management defined

- COSO (2004): “… a process, effected by an entity’s BOD, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, to provide reasonable assurance regarding the achievement of entity objectives.”
Expansion of ERM’s objectives

- Standard and Poor’s (2007): “We now propose to introduce (ERM) analysis into the corporate credit ratings process globally as a forward-looking, structured framework to evaluate management as a principal component in determining the overall business profile. […] ERM provides management with information to optimize earnings – and ultimately the firm’s value – while staying in a well-defined risk tolerance. […] ERM also provides a new and clear language for transferring information about management’s intentions and capabilities, which are critical to credit evaluation.”

ERM’S evolution

- Over the years, ERM has evolved from a technical process to improve decision making and management control to a strategic tool.
- ERM is now more fluidly defined
- It can vary in its technical complexity, cultural significance, and level of embeddedness
COSO’s 8 elements

ERM Criticisms

- The model is too simplistic and not in line with organization realities
- So many approaches, it’s hard to tell what ERM is and becomes in practice
- Indicative of good management, sometimes
- Rooted in internal control, which tends to emphasize regulatory compliance and external accountability
Three companies and ERM

- Cicero – telecommunications – CRO is a former internal auditor – ERM relates primarily to BOD
- Phoedrus – oil and gas – viewed as “regulatory compliance” with the IA leading
- Virgilio – multinational technology – ERM fully integrated in all other risk management activities, including budget

IA’s roles in risk management when the organization has ERM

- Giving assurance on risk management processes
- Giving assurance that risks are correctly evaluated
- Evaluating risk management processes
- Evaluating the reporting of key risks
- Reviewing the management of key risks
Internal audit roles with safeguards – consulting activities

- Facilitating identification and evaluation of risks
- Coaching management in responding to risks
- Coordinating ERM activities
- Maintaining and developing the ERM framework
- Championing the establishment of ERM.

Roles IA should not perform

- Setting the risk appetite
- Imposing risk management processes
- Being the sole source for management’s assurance that risks are effectively managed
- Making decisions on risk responses
- Implementing risk responses on management’s behalf

**Safeguards for IA**

- Management is responsible for risk management
- IA’s functions should be documented in the internal audit charter
- IA cannot manage risks on management’s behalf
- IA can provide advice, challenge, and support to management’s decision making, but cannot make decisions
- IA cannot give objective assurance on any part of the ERM framework for which it is responsible
- Any work beyond assurance should be recognized as a consulting engagement

**COSO’s “Practical Approaches for Getting Started” with risk management**

- Concerned about ad-hoc, informal efforts
- Recommended an incremental approach to organizing risk management
- Focus initially on a small number of top risks
Questions for risk assessment

- What are your primary business objectives/strategies?
- What are the key components of enabling your business strategy or objectives?
- What internal factors or events could impede or derail each of these key components?
- What types of catastrophic risks does the organization face? How prepared is the organization to handle them, if they occur?

Near-Miss Management Systems

- Near-miss systems can contribute to improving company profitability and reducing the frequency and severity of both major industrial accidents and failures in other types of businesses.
Catastrophic events & near-misses

- Catastrophe: any unplanned event or accident that results in significant business losses.
- Near-miss: most important indicator of major accidents.
- Characteristics:
  - Frequency.
  - Actual damage.
  - Maximum potential damage.

Concept of near misses

- Industrial: an opportunity to improve environmental health and safety practice based on a condition or incident with potential for more serious consequences
- Financial: an event, a sequence of events, or an observation of unusual occurrences that possess the potential for improving a system’s operability by reducing the risk of upsets, some of which could eventually cause serious damage
- US DOE: A case where no barrier or only one barrier prevented an event from having a reportable consequence
Barings Bank failure (1995)

- Began with Nick Leeson’s attempt to cover up the mistake of his employee – a £20,000 near-miss
- Everyone overlooked continued problems
- The one auditor noticed a £50M problem, but discounted its potential for a bad outcome
BP Texas City Refinery Explosion (March 2005)

- The disaster killed 15 people and injured more than 150; the BP Independent Safety Review Panel conducted an investigation
- BP had emphasized personal safety but not process safety
- Improving personal safety statistics, plus lack of understanding of process problems, gave BP’s management a false sense of security

Findings - Very significant near-misses

- Trailers were in an unsafe location, too close to a unit handling very hazardous materials
- Key equipment in the unit had serious existing malfunctions— it should have never been started
- The same equipment had a history of abnormal start-ups
- The blow down drum was never connected to a stack
- In the 10 years before the accident, the unit had 4 serious releases of flammable material
- Process safety audit reports from 1998, 2001, and 2004 contained a significant number of overdue, high priority, process safety recommendations
Near-miss management process

- Identification – an individual recognizes a situation or condition to be a “near-miss.”
- Company must have (1) a clear definition of a “near-miss” and (2) the means to ensure that every employee knows the definition at all times

Near-miss management process

- Disclosure (reporting). Once identified, the near-miss must be disclosed, preferably in writing.
- Prioritization: Each organization should have its own criteria, which include frequency, actual damage, and maximum potential damage of worst-case scenarios,
Near-miss management process

- Distribution: Getting the information to the people who will analyze the cause of the incident.
- Identification of causes: Identification of both direct and root causes of a near-miss.

Near-miss management process

- Solution identification: This process should seek a solution for every identified cause.
- Dissemination: Solutions should be communicated to the people who will execute them; the executors should not be the same people who participated in the solution identification process.
- Resolution: Follow-up procedure to determine that the solutions are implemented. When the changes are complete, the reporters should be informed of the results.
Near-miss management process

- To get the full benefit of lessons and corrective actions, all eight steps must be performed fully and completely. For example, it is important to find all possible causes and all possible solutions.
- The logic flow of these steps applies to any size or type of organization.

Critical elements of risk-related decision-making

- Probability neglect – people tend to focus on the consequences rather than the probability of the occurrence of an outcome
- Consequence neglect – Sometimes people neglect the magnitude of outcomes
- Statistical neglect – People use rules of thumb (heuristics), which will introduce systematic biases in their decisions. People should subjectively assess small probabilities and continuously update them.
- Solution neglect – choosing an optimal solution is impossible when one does not consider all the solutions.
- External risk neglect – in making decisions, individuals or groups often consider the cost/benefit only for themselves, without including externalities, sometimes leading to significant outcomes for others.