Practical Enterprise Risk Management: 
A Building Block Approach for Implementing COSO 2004

Brian Ballou
Associate Professor
Department of Accountancy
Miami University

Dan Heitger
Assistant Professor
Department of Accountancy
Miami University

October 2004

Biographies:
Brian Ballou is an associate professor of accounting at Miami University. His teaching and research emphasis is on enterprise risk management, risk-based assurance, and performance measurement (513-529-6213; balloubj@muohio.edu).

Dan L. Heitger is an assistant professor of accounting at Miami University. His teaching and research emphasis is on new product development, activity cost estimations, incentive systems, and performance measurement (513-529-6208; heitgedl@muohio.edu).
EXECUTIVE SUMMARY: As a result of the highly-publicized business failures, scandals, and frauds over the past several years, there has been a series of laws, regulations, and listing standards calling for strengthened corporate governance and risk management involving top management. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued its framework for enterprise-wide risk management (ERM) in September 2004 to address this need. The goal of the framework is to enable organizations to standardize ERM so that organizations can more easily benchmark, establish best practices, and enable more meaningful dialogue about this critically important business issue. One concern regarding the COSO ERM framework is that its overreaching nature can appear overwhelming for some organizations, particularly those that are fairly small in size or that have not previously established an ERM culture. This article presents a building block approach to implementing the COSO ERM framework that is accessible to organizations, regardless of their size or previous experience in risk management. Further, the process offered here enables organizations to evolve ERM as they establish a risk culture and offers better opportunities for efficient and effective allocation of resources when conducting ERM activities.
Introduction

Managing risk is an important and sometimes overlooked aspect of running an organization, even in the wake of the unprecedented level of business failures and financial reporting scandals over the past several years. The responsibility of overseeing risk management falls on the Board of Directors, while the ownership responsibility for enterprise risk management falls on the CEO and senior executives. In Mary Pat McCarthy and Timothy Flynn’s 2004 book, *Risk from the CEO and Board Perspective*, Hewlett-Packard board member Jay Keyworth states, “In my years at HP and in talking to other board members from large Fortune 50 companies, I find that people thought that actually becoming familiar with the business itself and the details of the business, and particularly the half-dozen major areas of potential risk the company faces, was not really a board responsibility.” This quote suggests that boards might not have taken responsibility for risk management to the extent that stakeholders expect.

The need for enterprise risk management is even more important given today’s business environment. Organizations today face unprecedented challenges competing in an increasingly global, volatile, and regulated business environment. Further, meeting customer needs, managing complex supply chains utilizing strategic alliance partners, and ensuring effective and efficient business process performance internally is increasingly more difficult, even with the presence of more sophisticated, real-time information systems. Added to these pressures are the threats to an organization’s reputation from (1) perceptions of improper (or a lack of) social responsibility created from an ever-strengthening perception by the public of the role of
organizations in improving the communities and environments in which they operate and (2) external reporting based on distrust created by frauds and restatements continually appearing over the past five years.

Because of the variety and complexity of risks that organizations need to address and the unique challenges faced by individual organizations, there has to-date not been a standardized framework for approaching enterprise risk management that organizations can use to establish benchmarks and best practices. To address this void, the Committee of Sponsoring Organizations (COSO) of the Treadway Commission developed an enterprise risk management (ERM) framework, which was released in September 2004. COSO includes representatives from the IMA (managerial accountants), AICPA (CPAs), AAA (academia), FEI (financial executives), and IIA (internal auditors) and developed the framework with the help of PricewaterhouseCoopers LLP (to order a complete copy of the framework, go to www.coso.org).

COSO’s framework includes the following definition of ERM:

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

Exhibit 1 lays out the steps of COSO’s ERM framework. Exhibit 2 illustrates the four categories of risk and levels of the organization to which the framework should be applied. Further descriptions of the steps of the process, the types of risks, and levels of application of the framework will be described within the context of implementing the framework in a practical manner. Please note that this article is based on the framework’s contents such that the actual document can be utilized to gain additional insights on model components described herein.

-----------Insert Exhibits 1 and 2 About Here-----------
The COSO ERM framework can be quite intimidating upon first review. The report consists of two volumes—one that presents the framework and one with helpful guidance for implementing the framework. One of the drawbacks associated with introducing a comprehensive framework, such as the COSO ERM, is that it requires a significant investment in time and resources to fully implement within an organization. Further complicating this challenge is that effective ERM requires ownership by executives, careful oversight by directors, and a cultural shift at most organizations before the process can reach its full potential. Thus, initial implementation of the framework is perhaps the biggest obstacle to its ultimate success.

In this article, a practical implementation of COSO’s ERM framework is offered that enables organizations to gain comfort with utilization of an entity-wide portfolio approach to risk management, including an allowance for the culture shift needed for an ERM framework to achieve its potential. This practical implementation encompasses the entire framework utilizing a building block approach. The approach consists of (1) implementing the ERM framework across each component but only on a limited basis, and (2) placing initial emphasis on entity-wide risks across all four risk categories (see Exhibit 2). The ERM framework can be expanded, including an eventual cascading of the framework throughout other levels of the organization as senior management become comfortable with the culture being created and are able to shift the ownership structure for risk management throughout the organization.

Benefits and Challenges from a Building Block Approach to ERM

There are several benefits associated with utilizing a building block approach to implementing the COSO ERM framework. These benefits include:

- *Size Does Not Matter*—All organizations can benefit from enterprise risk management to some degree. COSO argues that its ERM framework can be applicable for small
companies, as long as each component is present and functioning properly, even though it might be less formal and less structured. However, by using a formalized building block approach in which the framework is applied on a limited basis and only entity-wide risks are included during initial implementation, smaller organizations can benefit from having a structured, formal ERM process that can be expanded over time only to the extent that doing so makes sense for the organization.

- **Culture Shifts Take Time**—Shifting employees’ attitudes about risk management to include monitoring, measuring, and controlling certain risks, while sharing, avoiding, and accepting other risks will not effectively occur in a short period of time. Once a risk management culture has been developed within an organization, these processes can be incorporated efficiently into day-to-day operations. However, initially many employees view ERM as the latest corporate trend that distracts from running the business. By evolving an ERM framework over time, employees see executives and directors shifting their emphasis and are more likely motivated to incorporate the philosophy at their level to be more in tune with top management’s view of the organization.

- **Better Allocation of Resources**—Implementing an effective ERM will consume significant resources. No organization has excess resources lying around waiting to be utilized to incorporate a new framework for managing risk. However, by utilizing a building block ERM approach consisting of first understanding entity-wide risks, executives and directors can decide which components of ERM need more/less resources for effective and efficient risk management at the other levels of the organization. For example certain business units can be identified as having more significant risk concerns
for the organization overall, while other units that are more mature but excellent sources of cash flow might be identified as needing less resources for effective ERM.

There also are several pitfalls to avoid when using a building block approach to ERM that can occur if an organization is not careful to emphasize the cultural shift when implementing the framework. Two of the more important challenges include:

- **Oversimplifying the Framework**—One challenge associated with implementing a practical ERM framework that evolves over time is that the initial framework is too simplified for establishing an effective understanding of entity-wide risks to the extent that effective management decisions can occur. Thus, organizations need to invest time and resources to the extent necessary to implement an effective ERM framework sufficient to create a risk management culture and establish a foundation for managing risks not only at the entity-level, but at other levels of the organization as the framework evolves.

- **Skeptical Perceptions Associated with Implementing a Framework**—Often, when an organization opts to slowly roll out new initiatives, skeptics within the organization will assume that there is an ulterior motive behind them. For example, if the first version of an ERM framework emphasizes ownership of risk management within pockets of the organization without a corresponding emphasis on a risk management culture, employees and other stakeholders might view such a movement as the C-Level distancing itself from risk management but creating a scapegoat should risk management problems occur at a later time. Further, analysts might view a skeletal risk management framework as being solely a signal that an organization is following trends to meet shareholder expectations.
The Building Block Approach for Implementing COSO’s ERM Framework

The remainder of the article describes a practical ERM framework that is designed to help achieve the benefits and avoid the pitfalls associated with COSO’s framework utilizing a building block approach. This framework, which is presented in Exhibit 3, incorporates all steps of the COSO ERM framework such that risk owners and other employees within the organization can compare risk management initiatives with those of other organizations and have more meaningful discussions with members of other organizations also implementing ERM frameworks. The key difference is that the building block approach provides organizations with the time to gain comfort with utilizing a formal ERM framework such that C-Level managers, with oversight by directors, can make informed decisions on how best to develop a more intricate framework that cascades throughout the organization. As the last step under monitoring, organizations are encouraged to continue to expand their ERM frameworks at a rate and in directions that make the most sense based on individual experiences with the prior year’s framework. The following sections further discuss the recommendations in Exhibit 3.

--------Insert Exhibit 3 About Here--------

Internal Environment

There are many components to an organization’s internal environment that should be addressed as an organization develops its ERM framework. However, there are several elements that are critical for laying the foundation for ERM that should be addressed at a minimum, including establishment of a risk management philosophy, culture, and organizational structure. The COSO report includes many categories under internal environment, some of which have been re-classified under the three components mentioned herein. Many organizations might argue that a risk culture currently exists based on the subcategories mentioned in Exhibit 3.
However, the cultural items mentioned will serve to create a risk culture only if a risk management philosophy and organizational structure also are in place.

Two necessary conditions for an internal environment to facilitate an effective risk culture is an awareness of the risk appetites (i.e., the degree of risk that an organization is willing to accept) of key stakeholders and a philosophical commitment to align the organization’s risk appetite embedded in its strategic objectives, strategies, and other initiatives with those of the key stakeholders. An emphasis on aligning risk appetites is not likely to occur unless the risk management organizational structure includes some level of responsibility of ERM for all C-Level employees and directors. Although the authority and responsibility for ERM should lie with a committee and chief officer (e.g., a risk committee and a chief risk officer), directors and executives should take a direct interest in receiving reports and engaging in discussion on achieved risk levels and their alignment with stakeholder risk appetites.

**Objective Setting**

For objective setting, an organization needs to specify its strategic objectives and the key strategies for achieving those objectives. As part of this process, the organization should define its risk appetite, ensuring that the risk appetite is aligned with its objectives and strategies. Not included in the COSO ERM Framework but highly recommended in this article is to ensure that the risk appetite of the organization also is aligned with risk appetites of key stakeholders, most notably shareholders, key employees, and external entities involved in the supply chain (suppliers, customers, etc.). By attempting to align risk appetites to the extent possible, dialogue between the organization and its shareholders can be open and transparent because risk/return preferences should be fairly well agreed upon by all parties.
**Event Identification**

Identifying risk events that could impact an organization is a very important step in developing an ERM framework. Because of the potential for forgetting risks, organizations need to carefully create risk categories and consider various ways that such risks can be realized. While the four risk categories in COSO’s ERM clearly are universal to most organizations, examples of each type of risk are offered to demonstrate the types of risks that likely affect most organizations to varying degrees (see the examples of each risk in Exhibit 2). Another important consideration when considering the impact of risk events is thinking through risk interdependencies. In other words, are the risk events isolated or are they part of a chain reaction or do they result in ripple effects, etc.? Organizations are encouraged to utilize holistic, systems-type thinking to develop a deep understanding of the full impact of risk impacts. This knowledge will be useful during the next phase of the framework. Also, organizations should consider the methodologies and techniques that might be used to assess and measure risk management at this stage to better understand the resources required to complete the ERM framework (note that the COSO ERM framework document provides examples of various methodologies and techniques).

**Risk Assessment**

The risk assessment stage is where the rubber meets the road in an ERM framework. Here, organizations first estimate probabilities/frequencies and cost impacts of risk events. By first having carefully considered the source of events and interdependencies with other risk events, organizations are in a better position to make these estimates. Also, estimates can be made utilizing various approaches. A point estimate (i.e., expected) probability or cost can be used. Some organizations prefer to use relevant ranges. Others use various scenarios (e.g., best
case, worst case, etc.). There is no right answer; rather, organizations should use an approach that is agreeable and most consistent with other components of the framework, such as risk appetite, etc. Exhibit 4, Parts A and B, provides an example of various risks that an organization faces relative to its risk appetite, and Panel A of Exhibit 5 shows how organizations can plot risks—the examples in the exhibit represent point estimates and only general categories (high and low) for illustrative purposes. The diagonal line represents risk appetite, the points at which an organization would prefer its risks to lie, which differs across organizations.

---------Insert Exhibits 4 and 5 About Here----

**Risk Response**

Other than risk appetite, determining risk response is the most important decision exercise that organizations make in developing an ERM framework. Because risk events by definition are uncertain, deciding whether to accept or avoid a risk-related activity can have significant consequences for an organization. Further, by choosing to share or reduce a risk, the organization is committing to expending resources to purchase an insurance premium, enter into a strategic alliance, and/or implement control activities. Organizations should be careful to consider the impact of risk responses for a given risk on other risks. Upon determining risk responses, plots for accepted risks remain while plots for avoided risks are removed from the risk plot. Risks that are shared or reduced are impacted based on the effectiveness of the mechanism employed.

**Control Activities**

Organizations that decide to reduce risks need to identify control activities that can be used to effectively reduce risks or the costs associated with the risks. Note that control activities under the COSO ERM expand beyond what have traditionally been considered control activities
under the notion of internal control. Basically, a control activity consists of any initiative or activity that reduces the probability/frequency of a risk or reduces the associated cost impact.

The next aspect of control activities is determining all costs associated with premiums, alliances, and control activities. However, organizations must be careful to consider that the impact of share and reduce activities likely does not eliminate the risk in question. Rather, the activities likely reduce probabilities/frequencies of risk (preventive), cost impacts (detective), or both (preventive and detective). An effective way to understand that residual risks remain is to adjust the risk plots with arrows representing the reduction of risk from the associated share or reduction activity. Thus, the adjusted risk costs consist of the costs of the premium, alliance, or control activity plus the residual probability/frequency multiplied by the residual cost impact.

See Part C of Exhibit 4 and Panel B of Exhibit 5 to see how risk responses and control activities impact inherent risk plots.

**Information and Communication**

Even a building block ERM framework needs effective information systems and communication channels to be effective. At a minimum, information systems should be able to track actual information to inform the organization about actual event occurrences, including those avoided, and actual costs of premiums, alliances, and control activities so that a comparison of costs of actual risk events to estimates can be performed as part of monitoring. Further, organizations need to ensure that timely reporting of ERM occurs at all levels actively involved in managing the framework, most notably the responsible party for ERM (e.g., CRO). In particular, the effectiveness of the ERM framework at managing risk events and the actual costs associated with the events should be reported. Perhaps most importantly, the responsible party should provide updates on ERM effectiveness and costs to senior executives and directors.
Monitoring

Monitoring is important for a building block ERM approach because at this point the organization makes decisions regarding how to expand its ERM framework throughout the organization. By performing separate risk assessments of actual events and costs to estimates, the organization can refine its risk assessment and response decision making process such that some degree of internal standardization can occur. Further, as C-Level employees and directors gain comfort with the ERM framework, a solid risk philosophy and culture can be developed that will enable more effective internal marketing of the benefits of the framework as it is expanded throughout other levels of the organization (e.g., divisions, business units, subsidiaries).

Conclusion

This article is designed to augment COSO’s 2004 ERM framework so that organizations of all sizes, cultures, and risk experiences can successfully implement an ERM framework without being overwhelmed by the overreaching goal of the complete framework. By taking a building block approach to ERM, organizations can decide how to best evolve its framework, including the activities within each component of the framework and the extent that it is applied throughout the organization. The key aspects to this building block approach are to start by (1) considering entity-wide risks, followed by cascading the framework throughout the organization over time, and (2) including all phases of the COSO framework but limiting those phases to the most basic elements needed to construct a solid foundation that can be evolved over time. Accordingly, we encourage all C-level managers and directors to obtain and read a copy of the full report so that an understanding of the endgame of the ERM framework can be established. With an effectively developed and carefully implemented ERM framework, most organizations
should improve the probability of achieving objectives, which is the underlying goal of the process.
Exhibit 1
The COSO 2004 ERM Framework

Internal Environment

Objective Setting

Event Identification

Risk Assessment

Risk Response

Control Activities

Information and Communication

Monitoring

Note: Arrows identify the phases of the ERM Framework that are sequential by design
(Adapted from COSO’s Enterprise Risk Management Framework, www.coso.org)
### Exhibit 2
Categories of Risk and Organizational Levels of ERM

Panel A: Four Categories of Risk in COSO ERM Framework (Along with Examples of each Risk):

<table>
<thead>
<tr>
<th>Category</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic</td>
<td>Governance, Strategic Objectives, Business Model, External Forces, etc.</td>
</tr>
<tr>
<td>Operations</td>
<td>Business Processes, Upstream Value Chain, Downstream Value Chain, Financial, etc.</td>
</tr>
<tr>
<td>Reporting</td>
<td>Information Technology, Financial, Internal, Intellectual Property, Reputation, etc.</td>
</tr>
<tr>
<td>Compliance</td>
<td>Securities and Exchange Commission, Environmental, Legal, Contractual, etc.</td>
</tr>
</tbody>
</table>

Panel B: Organizational Levels of ERM (Along with Application Under Building Block Approach):

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entity-Level</td>
<td>(Fundamental to the Initial ERM Framework)</td>
</tr>
<tr>
<td>Division Level</td>
<td>(Expand ERM as Needed Over Time)</td>
</tr>
<tr>
<td>Business Unit Level</td>
<td>(Expand ERM as Needed Over Time.)</td>
</tr>
<tr>
<td>Subsidiary Level</td>
<td>(Expand ERM as Needed Over Time.)</td>
</tr>
</tbody>
</table>
Exhibit 3
Components of a Practical ERM Framework

Internal Environment
• Develop a Risk Management Philosophy
  o Take steps to understand the risk appetites of key stakeholder group for the organization
  o Take steps to enable alignment of risk appetites across stakeholders
• Create a Risk Management Culture
  o Emphasize integrity and ethical values in every endeavor
  o Emphasize the role of employee commitment and capability through incentives and measures
  o Design human resource policies and practices to support risk culture
• Design a Risk Management Organizational Structure
  o Responsibility established on some level for all BOD members and senior executives
  o Consider utilization of risk committee beyond audit committee
  o Assignment of authority and responsibility (e.g., CRO)

Objective Setting
• Establish Clear Strategic Objectives and Strategies
  o At entity-wide level
  o At other levels of the organization to the extent that a direct, material impact on entity is reasonably likely
• Determine Entity-Wide Risk Appetite (Tolerance)
  o Align with key stakeholders, strategic objectives and strategies, and alliance partners

Event Identification
• Identify Risk Events
  o Consider factors influencing objectives and strategies
  o Carefully analyze each risk category (i.e., strategic, operational, reporting, and compliance)
• Consider Event Interdependencies (isolated, part of chain reaction, cause ripple effects, etc.)
• Identify measurement issues associated with methodologies or techniques utilized

Risk Assessment
• Select Assessment Technique (e.g., point estimates, probability/loss ranges, best/worse case scenarios, etc.)
• Assess Inherent Probability/Frequency of Risk Events
• Assess Cost Impact of Risk Events (any losses per unit of output multiplied by output until contained)
• Consider plotting the risks on a graph (see Exhibit 5)

Risk Response
• Identify and Select Response for Each Risk (accept risk, avoid risk, share risk, or reduce risk)
• Consider Effects of Risk Response on Other Risks
• Adjust Plots (see Exhibit 5)
  o Accepted risks (estimated risk cost is plot)
  o Avoided risks (remove plots from graph)
  o Shared and reduced risks (alter plots based on control activities step)
Exhibit 3 (Continued)
Components of a Practical ERM Framework

Control Activities
- Shared Risks
  - Assess costs of premiums for insured risks
  - Assess forfeited returns and/or costs to manage alliances
- Reduced Risks
  - Identify control activities needed to reduce risk
  - Assess all costs associated with control activities
- Adjust Plots (see Exhibit 5)
  - Determine extent to which policy, alliance, and control activity reduces inherent probability/frequency estimates (preventative) and/or cost impact estimates (detective)
  - Estimate total risk costs, which are the sum of residual risk costs and premium/alliance/control activity costs

Information and Communication
- Ensure that Information Systems can Measure and Report
  - Actual risk event occurrences (including those associated with avoided activities)
  - Actual costs of premiums (insurance), alliance relationships, and control activities
  - Actual costs of risk events
- Communicate ERM Effectiveness and Costs
  - Ensure proper periodic report of ERM
  - Responsible party (e.g., CRO) accumulates ERM effectiveness and costs
  - Responsible party reports on ERM effectiveness and costs to executives and BOD

Monitoring
- Perform Separate Risk Evaluations
  - Compare actual event occurrences with residual probability/frequency estimates
  - Compare actual costs with risk sharing/reduction and residual cost impact estimates
- Re-Evaluate Risk Assessments
  - Incorporate any changes to risk appetite, objectives, strategies, etc.
  - Identify any events not previously identified
  - Add/Revise estimates for probability/frequency, share/reduce cost, and/or cost impact estimates
- Consider Areas to Expand ERM Framework based on COSO 2004


**Part A: Risk Appetite Assessment**
Assume that a mature organization is controlled by several large retirement funds such that the Board and executives assess its risk appetite at a low enough level such that reasonable rates of return and fairly steady income streams result over time. Further, the organization has a long established brand name for quality and durability in its products, dominates market share for its industry, and operates in an industry with high entry costs. Accordingly, the company sets its risk appetite such that its risk preferences mainly are low probability events with low to moderate cost impacts. The line drawn through the risk plots on Exhibit 5 represent the organization’s risk appetite, and the organization will choose to manage risks so that they are as close to the risk appetite line as possible.

**Part B: Risk Assessments**
Assume that the organization identifies its five most important entity-wide risks. Risk 1 is market share loss from a new entrant, which the organization has assessed as significantly below its risk appetite. Risk 2 is a reduction in product quality associated with the replacement of its aging work force, which is heavily unionized. Risk 3 is a regulatory risk associated with government approval of a new product line being considered that includes use of a chemical that the Environmental Protection Agency (EPA) has targeted for investigation based on its potential for contaminating the atmosphere. Risk 4 is the risk of rising supply chain costs associated with the distribution of finished products from the organization’s plants to authorized dealers and distributors. Risk 5 is the cost associated with worker injuries from the dangerous nature of the production process of the organization’s products. The organization has self-insured in the past but costs and liability exposures have been rapidly increasing over the past several years. The plots in Panel A of Exhibit 5 illustrate how these five risks might be plotted within the ERM framework.

**Part C: Risk Responses**
Assume that the organization wants to manage its risks close to its risk appetite. The organization in this example could choose a different response for each risk. For Risk 1, there is no need to consume resources to manage the risk further, so market share risk is accepted. The organization can choose to reduce the probability and cost impact of Risk 2 by investing in the human resource business process such that a favorable union contract and training programs can be implemented to attract quality employees who will continue the tradition of quality. The organization can choose to avoid Risk 3 by opting not to pursue the new product line until the EPA resolves the issues surrounding the controversial chemical. For Risk 4, an alliance with a distribution company that has a core competency in distribution can help reduce the probability and cost impacts of distribution risks. Finally for Risk 5, since the probability of work-related incidents has proven to be difficult to reduce, the organization can choose to purchase worker compensation insurance to reduce the cost impacts associated with the risks. Note that the responses to Risks 3, 4, and 5 all involve significant costs associated with the control activity (Risk 3), alliance (Risk 4) and policy premium (Risk 5). The key to these decisions is that the risk response costs plus remaining residual risk costs should be less than the risk costs should the risks be accepted. The adjusted plots in Panel 5 of Exhibit 5 illustrate how the risk responses impact the inherent risk assessments.
Panel A: Basic Example of Risk Assessments

Panel B: Basic Example of Risks Adjusted for Responses

Note: The risk appetite and responses are possible choices and not meant to suggest responses that are/are not appropriate