COSO

Committee of Sponsoring Organizations of the Treadway Commission

Thought Leadership in ERM

EMBRACING ENTERPRISE RISK MANAGEMENT

Practical Approaches for Getting Started

By

Mark L. Frigo and **Richard J. Anderson**

Authors

Mark L. Frigo
Director, Strategic Risk Management Lab
Ledger & Quill Alumni Distinguished Professor
Professor of Accountancy

The Center for Strategy, Execution and Valuation
Kellstadt Graduate School of Business
DePaul University

Richard J. Anderson
Clinical Professor
Strategic Risk Management Lab

DePaul University

The Strategic Risk Management Lab in the Center for Strategy, Execution, and Valuation at DePaul University is an engagement platform for thought leaders and the business community to co-create and share leading practices in Strategic Risk Management and Enterprise Risk Management.

COSO Board Members

David L. Landsittel
COSO Chair

Mark S. Beasley
American Accounting Association

Richard F. Chambers
The Institute of Internal Auditors

Marie Hollein
Financial Executives International

Larry E. Rittenberg
COSO Chair - Emeritus

Chuck Landes
American Institute of Certified Public Accountants

Jeff Thomson
Institute of Management Accountants

Preface

This project was commissioned by COSO, which is dedicated to providing thought leadership through the development of comprehensive frameworks and guidance on enterprise risk management, internal control, and fraud deterrence designed to improve organizational performance and governance and to reduce the extent of fraud in organizations. COSO is a private sector initiative, jointly sponsored and funded by the following organizations:

American Accounting Association

American Accounting Association (AAA)

AICPA

American Institute of Certified Public Accountants (AICPA)

fei

Financial Executives International (FEI)

ima

Institute of Management Accountants (IMA)

IIA

The Institute of Internal Auditors (IIA)

COSO
Committee of Sponsoring Organizations
of the Treadway Commission

www.coso.org

Thought Leadership in ERM

EMBRACING ENTERPRISE RISK MANAGEMENT

Practical Approaches for Getting Started

Commissioned by

COSO

Committee of Sponsoring Organizations of the Treadway Commission

January 2011

Copyright © 2011, The Committee of Sponsoring Organizations of the Treadway Commission (COSO).
1 2 3 4 5 6 7 8 9 0 PIP 1 9 8 7 6 5 4 3 2 1 0

All Rights Reserved. No part of this publication may be reproduced, redistributed, transmitted or displayed in any form or by any means without written permission. For information regarding licensing and reprint permissions please contact the American Institute of Certified Public Accountants, licensing and permissions agent for COSO copyrighted materials. Direct all inquiries to copyright@aicpa.org or to AICPA, Attn: Manager, Rights and Permissions, 220 Leigh Farm Rd., Durham, NC 27707. Telephone inquiries may be directed to 888-777-7707.

COSO
www.coso.org

Overview and the Question of "Where to Start?"

The increased interest in and importance of enterprise risk management is being driven by many powerful forces. Most importantly, it is driven by the need for companies to manage risks effectively in order to sustain operations and achieve their business objectives. Other forces also come into play, including rating agency reviews, government regulations, expanded proxy disclosures, and calls by shareholders and governance reform proponents for improving the way risks are managed by organizations.

Any entity that is currently operational has some form of risk management activities in place. However, these risk management activities are often *ad hoc*, informal and uncoordinated. And, they are often focused on operational or compliance-related risks and fail to focus systematically on strategic and emerging risks, which are most likely to affect an organization's success. As a result, they fall short of constituting a complete, robust risk management process as defined by COSO (See definition of ERM below).

In addition, existing risk management activities often lack transparency. Transparency about how enterprise-wide risks are managed is increasingly being sought by directors and senior management, as well as various external parties seeking to understand an organization's risk management activities. What's more, existing risk management processes often are not providing boards and senior management with an enterprise-wide view of risks, especially, emerging risks. Unfortunately, many organizational leaders are struggling with how to begin in their efforts to obtain strategic benefit from a more robust enterprise-wide approach to risk management.

> **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 enterprise, designed to identify potential events that may affect the entity, and manage risk to be within the risk appetite, to provide reasonable assurance regarding the achievement of entity objectives**
>
> *COSO's Enterprise Risk Management – Integrated Framework (2004)*

This leads to the question of "Where do we start?" Answering this question can be a major challenge for organizations where the perceived complexity of ERM or a lack of understanding of its strategic benefits may be barriers. At the same time, organizational pressures to reduce costs may prompt some decision makers to look at risk management as something that can be deferred or viewed as a lower priority, thereby setting the stage for unmanaged risk exposures that could seriously threaten the viability of the organization.

This COSO thought paper describes how an organization can start to move from informal risk management to ERM. We discuss the increasing importance of and focus on ERM and the need for all types of organizations to understand and embrace ERM. And, we examine perceived barriers to starting ERM and working through those barriers.

The approaches described in this document are based on successful practices that organizations have used to develop an incremental, step-by-step methodology to start ERM. While this is not the only way to start an ERM initiative, this incremental approach is designed to be very adaptable and flexible. We suggest specific, tangible actions that organizations can use to get started in this thought paper's three sections:

I. Keys to Success - Overarching themes to provide management with a strong foundation for an effective ERM program as they develop and tailor their specific approach to implementing ERM.

II. Initial Action Steps - Action oriented, "how to" steps to implement an initial ERM effort. These steps support development and implementation of a tailored ERM initiative.

III. Continuing ERM Implementation - Next steps to further develop and broaden the organization's initial ERM effort.

Content Outline

Page

Description

I. Keys to Success

While specific action steps may vary, there are some consistent underlying themes that have proved valuable in successful ERM initiatives. These themes represent "Keys to Success" for organizations that are now starting ERM initiatives and provide a useful foundation for specific actions detailed in Section II. These keys also help directors and management teams address some of the recognized barriers and resistance points to ERM adoption.

Theme 1.

Support from the Top is a Necessity

To successfully manage risk, an ERM initiative must be enterprise wide and viewed as an important and strategic effort. In the aftermath of the financial crisis of 2008, there has been a growing emphasis on the board's responsibilities for overseeing an organization's risk management activities. For example, the corporate governance rules of the New York Stock Exchange require audit committees of listed corporations to discuss the risk assessment and risk management policies of their organizations. More recently, the U.S. Securities and Exchange Commission (SEC) expanded proxy disclosures pertaining to the extent of the board's role in risk oversight. Moreover, credit rating agencies, such as Standard and Poor's (S&P) are also inquiring about enterprise risk management practices as part of their credit rating assessment processes.

Support from the board of directors and senior management is needed to get the right focus, resources and attention for ERM. Although it is not the job of the directors to manage the ERM activities, directors do need to demonstrate clear support for the ERM initiative as well as oversee what management has designed and implemented to manage top risk exposures. Thus, ERM must be enterprise wide, and understood and embraced by its personnel, and driven from the top down through clear and consistent communication and messaging from the board and senior management. It is the board's responsibility to ensure that management is devoting the right attention and resources to ERM and is setting the right tone for ERM. What's more, the board should be comfortable that management has put in place an effective ERM leader who is widely respected across the organization and who has accepted responsibility for overall ERM leadership, resources and support to accomplish the effort.

Top level support for ERM from the board and senior management is also important for establishing the desired "Internal Environment" to foster ERM success (as described in Appendix A, the *Internal Environment* is one of the eight components of COSO's 2004 *Enterprise Risk Management - Integrated Framework)*. This enterprise wide component is fundamental to setting the foundation for ERM and embedding it across the organization. It also sets the stage for further development of other COSO ERM Framework components including the establishment of the tone or the "risk culture" of the organization. S&P and other rating agencies have identified "risk culture" as a key element of ERM and have stressed its importance in their releases.

Theme 2.

Build ERM Using Incremental Steps

One perceived barrier to launching ERM is the perception that ERM is overly complex and requires a major and costly effort to implement. Related to this perception is the belief that an organization must implement all of the components of ERM in one single effort for it to work and bring any tangible value to the organization. Experience suggests otherwise.

In practice, some organizations, especially smaller organizations, have achieved ERM successes by taking an incremental, step-by-step approach to enhancing their risk management capabilities to provide a more enterprise-wide view over time rather than undertaking one massive launch effort. They start with a simple process and build from there using incremental steps rather than trying to make a quantum leap to fully implement a complete ERM process. By doing so, they are able to:

- **Identify and implement key practices to achieve immediate, tangible results.** For example, they may start by completing and sharing with their board for the first time a short list of enterprise wide risks with certain action steps to address the risks identified. This initial step would be followed by a more detailed risk assessment delving deeper into other risks the organization faces.

- **Provide an opportunity to change and further tailor ERM processes**. As the organization and its executives and directors expand their knowledge of ERM, they have the opportunity to make additional requests to broaden or deepen the organization's risk management activities.

- **Facilitate the identification and evaluation of benefits at each step.** This can be an effective way to respond to another possible barrier, the question of "What value do we derive from ERM?" There are two examples to illustrate this point on the next page:

Example Incremental Action Step	Benefit Received
Perform a risk assessment and prepare a short list of the organization's most significant risks	Board and senior management sees and discusses, often for the first time, a consensus view of the organization's most significant risks and how they are managed. This builds a common understanding and focus around these risks.
Identify opportunities to enhance risk management activities related to the significant risks identified	Specific actions are identified to enhance the risk management activities on each significant risk. This results in a better understanding of the organization's practices and how to enhance those practices and enables the identification of specific tangible benefits related to each action.

Theme 3.
Focus Initially on a Small Number of Top Risks

For an organization just starting out with ERM, it might make sense to first identify a small number of critical risks that can be managed, and then evolve from this starting point. For some organizations, such an approach might mean keeping the initial ERM focus on only those strategic risks that are deemed critical to the organization achieving its strategic business objectives. Focusing initially on a smaller, manageable number of key risks would also be beneficial in developing related processes such as monitoring and reporting for those specific risks. This focused approach also keeps the developing ERM processes simple and lends itself to subsequent incremental steps to expand the risk universe and ERM processes.

Another way to keep ERM manageable is to focus initially on a few top risks in just one critical business unit. This limited focus could be used to develop initial risk management processes that can be expanded across the enterprise to other business units. And when dealing with much smaller organizations, it can be useful to start things off by identifying just one critical risk or risk category and building ERM processes around that one risk.

Whichever specific risk approach is utilized, the critical success factor is to focus attention on a manageable number of key risks and then apply the lessons learned to identifying and managing additional critical risks across the enterprise.

Theme 4.
Leverage Existing Resources

Another possible barrier to initiating an ERM process may be the view that significant resources including investments or outside expertise are needed to undertake an ERM project. For example, some directors or senior executives might think that they would need to hire an experienced Chief Risk Officer or make significant investments in new technologies or automated tools. Such a viewpoint could prove to be a significant barrier to smaller organizations, in particular, which might have a strong desire to move ahead with ERM but have limited resources for making it happen.

Many organizations have successfully entered the ERM arena by leveraging their existing risk management resources. Organizations often discover that they have the personnel on their existing staffs, with the knowledge and capabilities relating to risks and risk management that can be effectively used to start. For example, some organizations have used their Chief Audit Executive or their Chief Financial Officer as the catalyst to begin an ERM initiative. In other instances, organizations have appointed a management committee, sometimes headed by their CFO, to bring together a wide array of personnel from across the entity who collectively have sufficient knowledge of the organization's core business model and related risks and risk management practices to get ERM moving. In addition, most organizations start their ERM effort without any specific enabling technology or automated tools other than basic spreadsheets and word-processing capabilities.

Theme 5.
Build on Existing Risk Management Activities

Any organization with current operations has some form of risk management activities or risk related activities already in place. These might include activities such as risk assessments performed by the internal audit, insurance or compliance functions, fraud prevention or detection measures, or certain credit or treasury activities. By leveraging, aligning and subsequently enhancing these existing risk related activities, the organization can achieve immediate and tangible benefits. For example, a company might implement a common set of risk definitions or a common risk framework across the organization. Others have conformed their risk assessment methodologies so that all areas of the organization performing a risk assessment do so using the same methodology.

Although it makes sense to build upon existing risk related activities, it must be done with the recognition that the existing activities probably do not constitute ERM. ERM requires risk management processes that ultimately are applied across the enterprise and represent an entity-wide portfolio view of risk, which is often missing from these existing functions.

Theme 6.
Embed ERM into the Business Fabric of the Organization

As articulated in COSO's ERM definition, enterprise risk management is a process that is applied across the organization. It is a management process, ultimately owned by the chief executive officer and involves people at every level of the organization. The comprehensive nature of the ERM process and its pervasiveness across the organization and its people provides the basis for its effectiveness.

ERM cannot be viewed or implemented as a stand-alone staff function or unit outside of the organization's core business processes. In some companies and industries, such as large banks, it is common to see a dedicated enterprise risk management unit to support the overall ERM effort including establishing ERM policies and practices for their business units. However, because ERM is a process, organizations may or may not decide that they need dedicated, stand-alone support for their ERM activities.

Whether a risk management unit exists or not, a key to success is linking or embedding the ERM process into its core business processes and structures of the organization. Some organizations, for example, have expanded their strategic plans and budgeting processes to include the identification and discussion of the risks related to their plans and budgets.

Theme 7.
Provide Ongoing ERM Updates and Continuing Education for Directors and Senior Management

ERM practices, processes and information continue to evolve. Thus, it is important for directors and senior executives to ensure that they are receiving appropriate updates, new releases and continuing education on ERM, including information about regulatory requirements and best practices. This information provides the opportunity for directors and senior management to update their risk management processes as they become aware of new or developing practices. This ongoing improvement process is particularly important with the increased focus on ERM by regulators, rating agencies, and the SEC.

II. Initial Action Steps and Objectives

Building off the "Keys to Success," this section of the thought paper details an initial action plan and steps to support development of a tailored ERM initiative. The plan reflects some simple, basic steps for implementing ERM, including the key step of performing an initial risk assessment. In Appendix B – "Where to Start: Draft Action Plan for an ERM Initiative" – we have included an example action plan, which can be further adapted for use by organizations. And in Appendix C – "Frequently Asked ERM Questions" – we have included responses to some common questions related to ERM that directors and senior management should find useful.

Step 1.
Seek Board and Senior Management Leadership, Involvement and Oversight

The board of directors and senior management set the tone for the organization's risk culture. Their involvement, leadership and oversight are essential for the success of any ERM effort.

A recent COSO thought paper, ***Effective Enterprise Risk Management: The Role of the Board of Directors***, notes that;

> "An entity's board of directors plays a critical role in overseeing an enterprise-wide approach to risk management. Because management is accountable to the board of directors, the board's focus on effective oversight is critical to setting the tone and culture towards effective risk management through strategy setting, formulating high level objectives, and approving broad-based resource allocations."[1]

The board and senior management should agree on their initial objectives regarding ERM, its benefits and their expectations for successful ERM. At a high level, there should be clear agreement and alignment of the board's and senior management's expectations, timing and expected results. This should include agreement on the resources to be made available and targets dates for the effort. The board should also consider the timing and level of status reporting that will be required to effectively monitor and oversee the ERM effort.

[1] Download COSO's *Effective Enterprise Risk Management: The Role of the Board of Directors* thought paper from COSO's website (www.coso.org).

This is also an appropriate time to lay the groundwork for the organization's risk culture including how to best communicate a desire for more effective risk management. This initial communication may be focused at senior level executives to emphasize the importance of the initial ERM effort and the critical nature of these activities. Subsequent communications can be directed at describing the ERM effort in more general terms for a broader audience across the organization.

Step 2.

Select a Strong Leader to Drive the ERM Initiative

Finding a leader to head the initial ERM project is also critical for success. Management should identify a leader with the right attributes (see box below) to head the ERM effort. This person does not need to be a "CRO" (Chief Risk Officer). Often, it is best to initially use existing resources, for example the Chief Audit Executive or Chief Financial Officer, for this role to get ERM started. This leader will not necessarily be the person to head ERM long term, but the person to get the initiative started and to take responsibility for moving the organization's ERM activities to the next level.

It is critical that the risk leader have sufficient stature and be at an appropriate senior management level in the organization to have a rich strategic perspective of the organization and its risks and to be viewed as a peer by other members of senior management. Embedding ERM into the business fabric of the organization is necessary. Having a risk leader who can be viewed as a peer by members of senior management is vital for the success of the ERM initiative.

Attributes of Effective Leaders of Enterprise Risk Management

- Broad knowledge of the business and its core strategies
- Strong relationships with directors and executive management
- Strong communication and facilitation skills
- Knowledge of the organization's risks
- Broad acceptance and credibility across the organization

Step 3.

Establish a Management Risk Committee or Working Group

To provide strong backing for its ERM effort, an organization should consider creating a senior-level Risk Management Committee or Working Group as the vehicle through which the designated risk leader can implement the ERM initiative.

While the use of a committee or working group in addition to the risk leader can be viewed as optional, these committees have been used by risk leaders as an effective means to engage the right people across the organization to ensure success of their ERM efforts.

Ideally, such committees or working groups would include "C-suite" level executives as well as key business unit leaders to ensure that the organization's ERM efforts are firmly embedded within the organization's core business activities. Engaging senior executives at this level also ensures ERM receives appropriate attention and support and it can be very useful in building and communicating the risk culture across the organization. And it provides top executives with the opportunity to share their insights about the types of risks that could impede the organization's ability to achieve its business objectives, which will be important information during the initial risk assessment.

Typically, the organization's ERM leader, as described in step 2 above, would head this committee and use it as a principle forum for implementation of ERM. Alternatively, an organization could create a committee and use the committee solely for the purpose of implementing ERM. With this approach, a risk leader or Chief Risk Officer could then be named at a later point as the organization matures its ERM processes and decides it needs a dedicated leader.

Step 4.

Conduct the Initial Enterprise-wide Risk Assessment & Develop an Action Plan

In many ways, this step is the heart of the initial ERM process. The focus here is to gain an understanding of and agreement on the organization's top risks and how they are managed. The assessment is a top-down look at the risks that could potentially be most significant to the organization and its ability to achieve its business objectives. While any organization faces many risks, the starting point is to get a manageable list of what are collectively seen as the most significant risks. Here, members of the risk committee or working group can be most helpful by sharing their views or identifying people in the organization who should be involved in the risk assessment.

While there is no one best way to conduct a risk assessment, many organizations start by obtaining a top-down view of the most important risk exposures from key executives across the organization. This is typically accomplished by starting with a discussion of the organization's business strategy and its components and then identifying the principal risks that would impede its ability to achieve its strategic objectives. An alternative is to discuss the strategies and risks of each of its major business units. To aid in these discussions, some organizations prepare a list of major risk categories, such as operational, financial, legal, market and then discuss exposures to that risk category for the business overall or each significant business unit.

It is often simplest and most effective for an organization to conduct this initial, top-down risk assessment with a handful of key business-unit leaders and members of the "C-suite." More individuals across and further within the organization can be added later as the risk assessment process matures. This data gathering could be accomplished through interviews, surveys, facilitated discussion groups or committee meetings. (See Appendix D to this paper for some examples of questions to consider for this initial risk assessment.)

The organization should then consider prioritizing or ranking the risks identified. This step could be accomplished by a simple ranking of the perceived level of inherent risk or by a more detailed assessment of the probability and impact of each risk. Consider using a basic scale of high, medium and low for each inherent risk as a starting point rather than quantification or modeling. Again, during this initial assessment, many organizations find good discussion and simple classifications helpful.

As a result of some of the large and unexpected risks that have manifested themselves lately, some organizations are now expanding their impact and probability assessments to include other factors. Examples of these new factors include assessing the velocity of a risk or the level of preparedness of the organization for that risk. For an example of an expanded risk assessment, see the Example Strategic Risk Profile following Step 6.

Whatever specific approach is taken, the information gathered should be compiled into an initial list with a manageable number of risks or potential risk events. As the organization matures its ERM processes, it can probe into finer levels of detail on other risks or, with enhanced knowledge of risk management activities, evolve its risk assessment from inherent risks to residual risks. Keep in mind, however, that focusing on too much detail or too many risks in the early stages of ERM adoption can impede progress on the broader ERM effort.

The organization also needs to assess its risk responses related to identified risks and develop action plans to address any gaps that are beyond those acceptable. Typically, action plans stemming from the initial risk assessment would identify gaps in the existing risk management processes related to the risks identified and detail specific ways to address those gaps.

The initial risk assessment exercise is also a time to initiate discussions about the organization's risk appetite relative to the risks identified. Some executives find it difficult to articulate, much less discuss, their organization's risk appetite. To overcome this challenge, consider focusing initially on qualitative or narrative descriptions of the risk appetite, (e.g. the organization may have zero tolerance for anything related to customer or employee safety). Management can facilitate the discussion of the risk appetite by identifying types of activities or products that they will or will not undertake because of the perceived risks. Alternatively, they may discuss how risk aggressive or conservative they want to be compared to their peers or competitors.

Step 5.
Inventory the Existing Risk Management Practices

During the risk assessment process, the organization should also be taking an inventory of its current risk management practices to determine areas of strength to build upon and areas of weakness to address. This inventory becomes valuable information for management to assist in enhancing the risk management processes.

First, it enables the organization to identify gaps in its current risk management processes relative to its most important and significant risks as they are identified. Oftentimes risk management activities are focused on existing operations and compliance risks, as opposed to significant external, emerging or strategic risks. As new risks are identified in the risk assessment process, the knowledge gained from a comprehensive inventory of existing risk management activities will help the organization assess the connections between existing risk management processes and the most critical enterprise level risks so that management can determine if there are any gaps in how they are managing the most important risks. Further, it assists the organization in mapping risks to underlying objectives.

Second, the inventory forms a baseline for the organization as it continues to develop and enhance its ERM processes. It helps management demonstrate progress and the benefits of ERM by serving as a point of comparison as the processes mature.

A **Risk Management Alignment Guide**, such as the example depicted below, can help facilitate compiling and documenting a high level inventory of the organization's risk management activities. The guide can be developed in two steps. First, management would list the top risks in the **Risk Category** column, which would be identified during its initial risk assessment as described on the prior page. Next, management would ensure that they have pinpointed an owner of the risk, articulated some form of risk appetite relevant to that risk, and have considered what existing processes are in place to monitor the risk over time, if any.

The last three columns would include information about any needed actions required to strengthen risk oversight and pinpoint management and board oversight related to the risk. In practice, organizations have found the completion of the column on the **Risk Owner** to be a useful exercise to ensure that they have a risk owner identified and acknowledged for each major risk. The **Risk Management Alignment Guide**, once completed, also serves as a concise and useful way to communicate the organization's overall risk management practices at a high level for the board and senior management.

Risk Management Alignment Guide Example

Risk Category	Risk Owners(s)	Risk Appetite Metrics	Monitoring	Action Plans	Company Oversight	Board Oversight
Reputation Risk	CEO	Policy including specific metrics approved xx/xx/xx	Corporate Communications	Approved & Updated xx/xx/xx	Executive Committee	Full Board
Operations Risk	COO	Daily operations metrics in place in all operating divisions	Operations Management daily monitoring and reporting	Plans in place for each trigger point	Risk Management Internal Audit	Risk Committee
Information Technology Risk	CTO	Policies including daily performance metrics in place for security, back-up and recovery	Daily monitoring against established performance standards	Contingency and back-up plans in place and periodically tested	Operating Committee Internal Audit	Audit Committee Full Board
Risk 4						

Step 6.
Develop Your Initial Risk Reporting

The organization next needs to develop its initial approach to risk reporting including its communication processes, target audiences, and reporting formats. Organizations should start by keeping things simple, clear and concise. Make it a point, however, that regardless of what specific reporting format employed, the reporting must reflect clearly the relative importance or significance of each risk. To this end, many organizations use simple lists, with their top risks listed in rank order. Others use colors or graphics along with their ranking to help focus attention on the most significant of the risks being reported. Also consider what status reporting and tracking you need to monitor progress on your action plans in order to address gaps in risk processes or risk responses identified during the ERM implementation.

The following example of a **Strategic Risk Profile** (see next page) includes three major strategic risk categories in the rows of the table (*Operations, Reputation, and Information Technology*) and four possible risk factors in the columns of table (*Likelihood, Impact, Velocity and Readiness*). The strategic risks are then listed in order of their overall priority and the red, yellow, and green readiness symbols help readers focus on risks that are most critical (e.g. those highlighted in red).

This example of a **Strategic Risk Profile** is presented for illustrative purposes only. Organizations should test various risk-reporting formats, approaches and risk factors in addition to talking with directors and executives about the level of detail needed and formats they find most useful.

Example Strategic Risk Profile

Strategic Risk	Description of Risk	Likelihood	Impact	Velocity	Readiness	Priority
Operations Risk	Supply Chain Disruptions; Product Liability Events	Low	High	High	🔴	1
Reputation Risk	Damage to reputation caused by company actions and/or partner actions	Medium	High	High	🟡	2
Information Technology Risk	Liability to achieve objectives because of failures of enabling technology	Medium	High	High	🟢	3
Risk 4					⚪	4
Risk 5					⚪	5

Step 7.
Develop the Next Phase of Action Plans & Ongoing Communications

The implementation of ERM is an evolutionary process that takes time to develop. In the spirit of continual improvement, once the initial ERM action plan has been completed, the working group or risk leader should conduct a critical assessment of the accomplishments to date and develop a series of action plans for the next stage of implementation. Following the incremental approach, the leader should identify next steps in the ERM roll-out that will foster additional enhancements and afford tangible benefits as a result.

The completion of the initial ERM action plan is also an opportune time for the risk leader and the ERM working group to convey the status and benefits achieved to the board of directors and senior management. The risk leader should also consider what types of ongoing education offerings and communications should be deployed across the organization to continue to strengthen the organization's risk culture and ERM capabilities.

III. Continuing ERM Implementation

The intent of this paper is to provide a simple illustration of ways to launch ERM. It represents a beginning, not an end point. An organization following this incremental approach to achieving ERM benefits will have taken a significant first step toward ERM and have a much better understanding of where it is headed and what needs to be accomplished next.

To lay the groundwork for ERM success, an organization should first establish its initial ERM process as an ongoing and important element that will assist in achieving business objectives. Given the evolutionary nature of ERM and the dynamic nature of risk, the ERM process must be ongoing and not viewed as a one-time event. The initial risk assessment process will need periodic updating and the organization will need to be attuned to the need to identify new and emerging risks. A solid foundation for risk management should be established and nurtured. Ongoing communications from directors and senior management will serve to reinforce and nurture the risk management culture.

Once ERM is off the ground, the organization can look for additional ways to expand the implementation of ERM across the organization. It should also be aware that, while tangible risk processes may have been implemented during this initial phase of ERM deployment, the processes may likely fall short of a complete ERM process and need to be enhanced. Accordingly, the organization's risk management leaders need to continue to drive further development and maturity of the risk management processes. They need to pursue levels of risk management maturity that reflect the components of the COSO's *Enterprise Risk Management - Integrated Framework*.

As the organization considers next steps, it should also evaluate the need for further developing and broadening the organization's risk culture and practices. Here is a working list of activities to consider that will strengthen an organization's risk culture and practices:

- A program of continuing ERM education for directors and executives
- ERM education and training for business-unit management
- Policies and action plans to embed ERM processes into the organization's functional units such as procurement, IT, or supply chain units
- Continuing communications across the organization on risk and risk management processes and expectations
- Development and communication of a risk management philosophy for the organization
- Identification of targeted benefits to be achieved by the next step of ERM deployment
- Development of board and corporate policies and practices for ERM
- Further discussion and articulation of a risk appetite for the organization and /or significant business units, including quantification
- Establishment of clear linkage between strategic planning and risk management
- Integration of risk management processes into an organization's annual planning and budgeting processes
- Expansion of the risk assessment process to include assessments of both inherent and residual levels of risk
- Exploration of the need for a dedicated Chief Risk Officer or ERM functional unit

The specific next steps to be taken should be implemented by continuing the incremental approach, taking small, tangible steps rather than attempting to implement the complete ERM framework. The primary objective is to keep the momentum moving and to continue to evolve, expand and deepen the organization's ERM capabilities.

Summary

Boards of directors and senior management need to challenge critically their organization's risk management practices and take the opportunity to enhance their processes and improve their ability to meet their organizations' objectives.

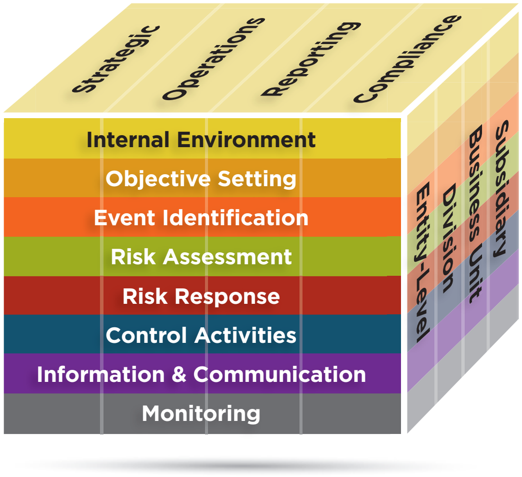
The concepts, techniques, and tools outlined in this thought paper, coupled with COSO's *Enterprise Risk Management - Integrated Framework* and other COSO thought papers, are intended to provide a strong foundation and effective starting point for pursuit of ERM benefits. Collectively, these resources provide a robust source of information and knowledge of ERM practices and processes.

The ideas and recommendations presented in this paper are neither intended to be, nor are they, the only way to enter the ERM arena. Ultimately, every organization must develop its own approach to ERM, one that best suits its particular culture and circumstances.

Above all, keep in mind the benefits of taking small, incremental steps on the path toward full ERM rather than attempting to implement the complete ERM framework all at once. The goal is to keep the momentum for ERM that will continue to expand and deepen the organization's ERM capabilities on a continual basis.

Appendix A – COSO's *Enterprise Risk Management – Integrated Framework*

Components of Enterprise Risk Management – Enterprise risk management consists of eight interrelated components. These components are derived from the way management runs a business and are integrated with the management process.



For more detailed information on enterprise risk management, the COSO *Enterprise Risk Management - Integrated Framework*, and related practices and activities, see the following COSO publications, available through the COSO website at **COSO.org/guidance**.

- *Enterprise Risk Management - Integrated Framework*
- *Effective Enterprise Risk Oversight: The Role of the Board of Directors*
- *Strengthening Enterprise Risk Management for Strategic Advantage*

Appendix B – Where to Start: Draft Action Plan for an ERM Initiative

Outlined below is an initial high-level draft of an action plan for ERM. This draft plan highlights key events and actions that organizations should consider in starting an ERM initiative. The draft is not intended to be viewed as a complete plan; furthermore, it requires careful tailoring and expansion prior to use. However, we believe it reflects useful information and is a practical draft plan as a basis to start.

1. Seek Board and Senior Management Involvement and Oversight

a. Set an agenda item for the board and executive management to discuss ERM and its benefits
b. Agree on high-level objectives and expectations regarding risk management
c. Understand the process to communicate and set the tone and expectations of ERM for the organization
d. Agree on a high-level approach, resources and target dates for the initial ERM effort

2. Identify and position a leader to drive the ERM Initiative

a. Identify a person with the right attributes to serve as the risk management leader
   i. Does not have to be a CRO (Chief Risk Officer)
   ii. Use existing resources
b. Set objectives and expectations for the leader
c. Allocate appropriate resources to enable success

3. Establish a Management Working Group

a. Establish a management working group to support the risk leader and drive the effort across the organization
b. Have the right, key people in the group
   i. Sufficient stature
   ii. "C-suite" representation
   iii. Business unit management
c. Look at using cross-functional teams
d. Agree on objectives for the working group
   i. Build ERM using incremental steps
   ii. Define some sought-after benefit to evaluate each step
   iii. Establish reporting process for management and the board

4. Conduct an Initial Enterprise-wide Risk Assessment and Action Plan

a. Focus on identifying the organization's most significant risks
b. Look for risks at the strategic level
c. Consider risk factors beyond just probability and impact, e.g.
   i. Velocity of risk
   ii. Preparedness
   iii. Other factors
d. For the most significant risks;
   i. Assess exposure to the risk
   ii. Assess adequacy of existing risk mitigation or monitoring
   iii. Identify opportunities to enhance mitigation or monitoring activities

e. Develop action plans to enhance risk management practices related to the risk identified
   i. Identify actions to implement the opportunities identified above
   ii. Establish target dates and responsibilities
   iii. Develop process to monitor and track implementation

5. Inventory the Existing Risk Management Practices

a. Identify and inventory existing practices
b. Identify gaps and opportunities
   i. Consider initial completion of the Risk Management Alignment Guide
c. Develop specific action steps to close gaps
d. Produce and implement action plans to close gaps and manage risks

6. Develop Initial Risk Reporting

a. Assess adequacy and effectiveness of existing risk reporting
b. Develop new reporting formats
   i. Consider extensive use of graphics and colors
   ii. Consider developing a risk "dashboard" for the board
c. Develop process for periodic reporting of emerging risks
d. Assess effectiveness of new reporting with stakeholders and revise as appropriate

7. Develop the Next Phase of Action Plans and Ongoing Communications

a. Conduct a critical assessment of the accomplishments of the working group
b. Revisit the risk process inventory and identify next processes for enhancement
c. Identify tangible steps for a new action plan including benefits sought and target dates
   i. Review with executive management and the board
d. Implement with appropriate resources and support
e. Schedule sessions for updating or further educating directors and executive management
f. Assess progress and benefits of ERM initiative against objectives and communicate to target audiences
g. Continue organization-wide communication process to build risk culture

Appendix C – Frequently Asked ERM Questions

- ***"Do I need to appoint a Chief Risk Officer?"***

No, COSO has observed that many organizations have started ERM using existing staff and appointing one of their key, senior-level personnel as the leader of the initiative. For example, some organizations have used their Chief Audit Executive or their CFO to begin the process. Regardless of title, the person selected to lead the ERM initiative must have the stature, authority and senior management leadership skills to be a true leader for ERM. Some organizations then develop their ERM processes to a point that they believe a dedicated Chief Risk Officer is needed. However, organizations don't have to create a CRO position in order to get started, nor does a more mature ERM process necessarily require a dedicated CRO.

- ***"Do I need to form a functional ERM unit?"***

No, many organizations have started ERM using management committees, working groups or existing personnel. Working groups or committees can take the lead in developing the organization's initial approach to ERM or to conduct an initial risk assessment as part of their existing duties. For smaller organizations, in particular, a separate risk management unit may not be necessary. Again, ERM as defined by COSO is a process not a functional unit. Whether a functional risk unit is needed ultimately depends on the complexity of the organization and the breadth and depth of its ERM processes.

- ***"What's wrong with just continuing my current, informal risk activities? Don't they constitute ERM?'***

While you want to leverage existing, informal risk management activities, these activities often lack both transparency and an enterprise-wide view or application. Accordingly, they are unable to address risk in a portfolio manner, including aggregation of risk. In addition, existing, informal risk activities are more likely to be performed on an *ad hoc* basis and done separately; therefore, these informal risk activities lack the consistency of approach and communications required by ERM processes. Thus, an organization's current, informal risk processes probably do not constitute true ERM. Increasingly, boards and other stakeholders, including rating agencies and regulators, are looking for ERM processes that are transparent, systematic and repeatable and that produce an enterprise-wide view.

- ***"What role does the board play in ERM?"***

The board is ultimately responsible for overseeing the ERM process, which is typically driven by management. The board's oversight responsibilities often involve using various board committees to oversee risks related to their areas of responsibility. In the end, effective engagement, involvement, and communications with the board is critical to ERM success. More specific guidance for boards is contained in the COSO thought paper, *Effective Enterprise Risk Oversight: The Role of the Board of Directors*.

- ***"Do I have to implement the complete COSO Enterprise Risk Management - Integrated Framework to conduct ERM activities?"***

COSO's *Enterprise Risk Management - Integrated Framework* notes that an entity may find it useful to discuss sub-sets of one or more of its objective categories to facilitate communications on a narrower topic. This approach can help an entity build its understanding of ERM and risk components on a step by step or incremental basis, staying within the context of the COSO ERM Framework. As noted in this paper, many organizations are taking a step-by-step approach to ERM to facilitate building their understanding and experience with components of ERM. While this "starting small" approach to ERM adoption has significant merit, care must be taken to maintain momentum.

If an organization loses momentum and only implements a few initial ERM steps, it will fall short of having an adequate ERM process. See Appendix A for additional information about the COSO *Enterprise Risk Management - Integrated Framework*.

- ***"Do I need to use quantitative models and metrics in starting ERM?"***

The use of quantitative models and metrics may ultimately be useful in a more robust ERM environment, but they are not needed to launch an ERM effort. What's more, some types of risks, strategic or emerging risks, for example, may not lend themselves to quantification at all.

Many organizations start their ERM process by simply listing or identifying what management and the board believe to be their top risks and then reviewing how those risks are managed and monitored. Depending on the size and complexity of the organization, quantitative modeling may, in the long run, prove helpful and even necessary to address certain types of risks, such as some financial and market risks. However, the quantification of all risks is not a goal. Management and the board need to first develop a solid understanding of ERM processes, approaches, and tools and then ensure that the organization's risk processes and tools are appropriate for the nature and scope of their specific risks and risk profile.

Appendix D – Risk Assessment Questions

Outlined below are some example questions that could be used in an interview with a senior executive or director during the risk assessment process. These questions are representative of the types of questions that could be asked to help identify the organization's most significant strategic or emerging risks.

- What are your primary business objectives or 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 events external to the organization could impede or derail each of the key components?

- What are the three most significant risk events that concern you regarding the organization's ability to achieve business objectives?

- Where should the organization enhance its risk management processes to have maximum benefit and impact on its ability to achieve business objectives?

- What types of catastrophic risks does the organization face? How prepared is the organization to handle them, if they occur?

- Can you identify any significant risks or exposures to third-parties (vendors, service providers, alliance partners etc) that concern you?

- What financial market risks do you believe are or will be significant?

- What current or developing legal/regulatory/governmental events or risks might be significant to the success of the business?

- Are you concerned about any emerging risks or events? If so, what are they?

- What risks are competitors identifying in their regulatory reports that we have not been addressing in our risk analysis?

About COSO

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a voluntary private-sector organization comprised of the following organizations dedicated to guiding executive management and governance participants towards the establishment of more effective, efficient, and ethical business operations on a global basis. It sponsors and disseminates frameworks and guidance based on in-depth research, analysis, and best practices.

COSO, 2011

American Accounting Association   AICPA®   fei   ima®   IIA®

About the Authors

Mark L. Frigo
Director, Strategic Risk Management Lab
Ledger & Quill Alumni Distinguished Professor of Strategy and Leadership
Professor of Accountancy

Richard J. Anderson
Clinical Professor
Strategic Risk Management Lab

The Center for Strategy, Execution and Valuation
Kellstadt Graduate School of Business
DePaul University

DEPAUL UNIVERSITY

The Strategic Risk Management Lab in the Center for Strategy, Execution, and Valuation at DePaul University is an engagement platform for thought leaders and the business community to co-create and share leading practices in Strategic Risk Management and Enterprise Risk Management

Thought Leadership in ERM

COSO

Committee of Sponsoring Organizations
of the Treadway Commission

www.coso.org

Thought Leadership in ERM

EMBRACING ENTERPRISE RISK MANAGEMENT

Practical Approaches for Getting Started

COSO

Committee of Sponsoring Organizations of the Treadway Commission

www.coso.org