COSO

Committee of Sponsoring Organizations of the Treadway Commission

Thought Leadership in ERM

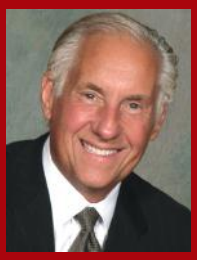
CREATING AND PROTECTING VALUE

UNDERSTANDING AND IMPLEMENTING ENTERPRISE RISK MANAGEMENT

By

Richard J. Anderson | Mark L. Frigo

Authors



Richard J. Anderson, MBA, CPA
Clinical Professor
Strategic Risk Management Lab

Dr. Mark L. Frigo, PhD, CPA, CMA, CGMA
Distinguished Professor Emeritus
Co-founder and Director Emeritus

Strategy, Execution and Valuation Initiative & Strategic Risk Management Lab
Kellstadt Graduate School of Business
Driehaus College of Business - School of Accountancy & MIS
DePaul University

Acknowledgements

We would like to recognize the COSO Board: Paul J. Sobel (Chair), Richard F. Chambers (IIA), Bob Dohrer (AICPA), Daniel C. Murdock (FEI), Douglas F. Prawitt (AAA), Jeffery C. Thompson (IMA) and Mark Beasley (North Carolina State University), Paul Walker (St. John's University) and Frank Martens (Pacific Risk Services) for their comments in helping us develop this thought leadership paper and to Ray Whittington and Dean Misty Johanson at DePaul University for their support of our work.

COSO Board Members

Preface

This project was commissioned by the Committee of Sponsoring Organizations of the Treadway Commission (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 (AAA)

American Institute of CPAs (AICPA)

Financial Executives International (FEI)

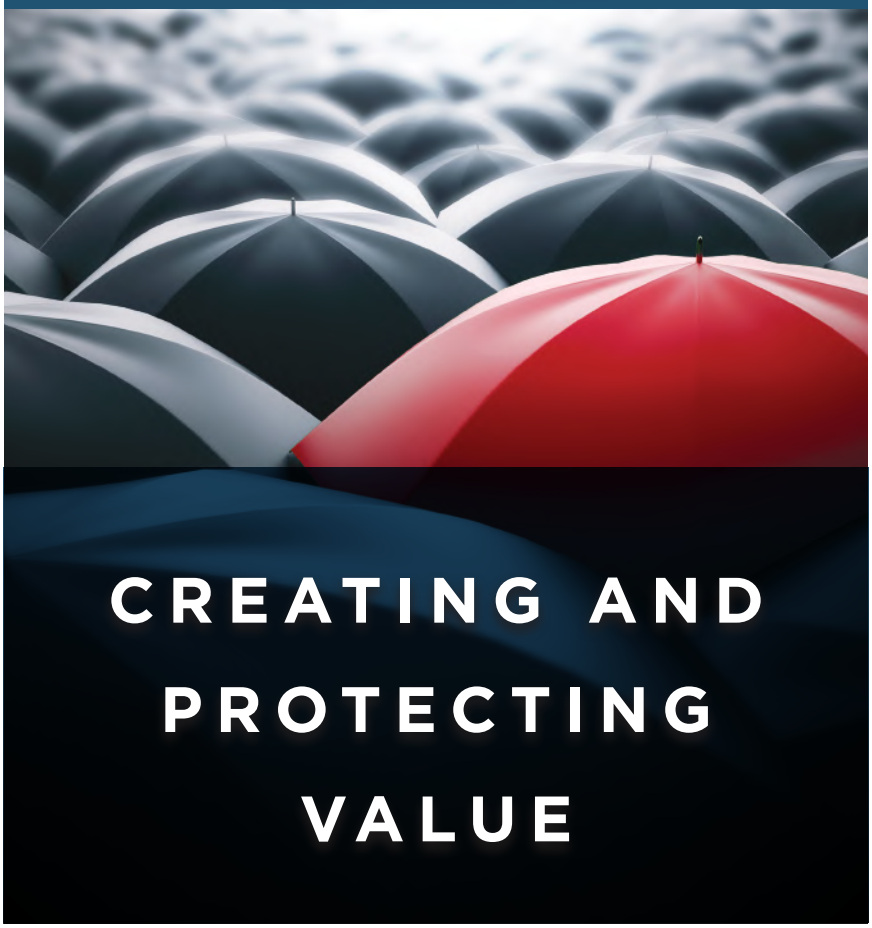
The Institute of Management Accountants (IMA)

The Institute of Internal Auditors (IIA)

COSO
Committee of Sponsoring Organizations of the Treadway Commission

coso.org

Thought Leadership in ERM



CREATING AND PROTECTING VALUE

UNDERSTANDING AND IMPLEMENTING ENTERPRISE RISK MANAGEMENT

Research Commissioned by

COSO

Committee of Sponsoring Organizations of the Treadway Commission

January 2020

1234567890 PIP 198765432

Design and production: Sergio Analco.

Contents

INTRODUCTION

Over the past few decades, enterprise risk management ("ERM") has been receiving increased attention by boards and executives and has undergone a continuing evolution in its development and uses. Along the way, lessons have been learned and ERM has been better understood regarding its benefits, objectives, and role in the organization. This COSO thought paper takes advantage of lessons learned and new guidance on enterprise risk management published by COSO to provide directors and executives with a better understanding of the role of enterprise risk management in creating and preserving value and its relationship to the key strategies of the organization. While not a detailed implementation guide, this paper includes overall guidance and an outline of succinct tangible steps that can used to implement an effective ERM program.

This thought paper outlines and provides clarity on the role and value of enterprise risk management to help directors and executives answer several key questions including:

"What is the real value of enterprise risk management?"

"What is its role and objectives?

"What are practical steps that can be taken to implement enterprise risk management?

The approach and steps contained in this thought paper are based on successful practices that organizations have used to take an incremental, step-by-step approach to implementing enterprise risk management. While this is not the only way to implement ERM, this incremental approach is designed to be very adaptable and flexible. The approach provides practical steps that can help take conceptual ideas of strategy and risk and actualize them through a series of basic steps. The thought paper is structured in four sections;

I. Background and Overview of the Updated COSO ERM Guidance

Background on the updated COSO ERM guidance and discussions on the role of ERM in enhancing performance and the relationship between strategy, risk, and performance.

II. Keys to Success in Getting Started

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.

III. Initial Action Steps

Action oriented, "how to" steps to implement an initial ERM effort including a basic methodology and related frameworks to assist in the identification of key strategies and their related risks.

IV. Continuing ERM Implementation

Next steps to further develop and broaden the organization's initial ERM initiative.

Those four sections are further supported by appendices, which include a draft action plan for ERM and frequently asked ERM questions.

I. BACKGROUND AND OVERVIEW OF THE UPDATED COSO ERM GUIDANCE

In June of 2017, the COSO board published new guidance on enterprise risk management entitled "*Enterprise Risk Management – Integrating with Strategy and Performance,*" (the "Framework"). The Framework updated COSO's previous ERM guidance, which was published in 2004, entitled *"Enterprise Risk Management – Integrated Framework."* The 2004 guidance presented a comprehensive framework and detailed guidance on ERM as it was starting to receive strong focus by organizations and boards. The 2004 ERM guidance was an important milestone in the advancement of ERM.

Since the publication of the 2004 ERM guidance, there has been a continued evolution of the concepts and practices of risk management while simultaneously the dynamic nature of risk has also evolved. It was becoming increasingly clear that in today's risk environment, improved risk management processes are needed to ensure that organizations are successful. In addition, the nature and role of ERM was being better understood and clarified particularly in the understanding that the role of ERM was not just that of a separate staff function but was integral to how an organization creates and preserves value.

In response to the risk environment and evolved thinking on ERM, in June of 2017, COSO published its updated ERM Framework. The updated guidance makes some very important distinctions and clarifications about both the role and objective of ERM as well as the need for its integration in the organization's strategy-setting process. It explains and makes explicit the relationship between strategy and risk, and discusses how improved risk management practices can contribute to improving performance and helping the organization create and enhance value.

While these concepts were also included in the 2004 ERM guidance, the updated Framework makes them much more explicit and clear, creating a simplified structure for ERM. The new guidance is also principles-based, which provides a comprehensive structure that can be used for both developing and assessing an ERM process.

Components of Enterprise Risk Management

The COSO ERM framework consists of five interrelated components of enterprise risk management as shown in Figure 1 Risk Management Components. The figure illustrates these components and their relationship with the entity's mission, vision, and core values. It depicts the flow of an organization's business model, ultimately resulting in enhanced value. The ribbons in the figure represent the components and show how they flow through an organization, integrated with all aspects of strategy and performance.

COSO's 2017 Framework, *Enterprise Risk Management – Integrating with Strategy and Performance*, defines enterprise risk management as:

The culture, capabilities, and practices, integrated with strategy-setting and performance that organizations rely on to manage risk in creating, preserving, and realizing value.

Figure 1. Risk Management Components

Source: COSO ERM Framework, 2017

Clarifying the Role of ERM in Creating and Protecting Value

An organization's board plays a key role in ERM. A primary oversight role of the board is helping the organization create and protect value. It executes this role through oversight of strategy and the ongoing performance of the organization in executing its chosen strategies. Through effective oversight, boards become aware of the growing complexities of risk in the environments they operate in. Risk complexities today have necessitated increased attention to risk management activities. In some cases, however, organizations have operated their risk management activities as detached, separate staff functions, simply focused on the objective of assessing risks on a stand-alone basis.

The 2017 Framework clearly positions ERM as an activity whose role and objective are helping the organization to create and protect value. It accomplishes this by helping the board and management make better informed decisions that enable them to effectively manage those risks that could impair their ability to achieve their strategies and business objectives. The overall objective of ERM is accordingly, enhanced performance of the organization. It is not a separate activity with its own objectives but an integral part of the organization's strategy setting and performance processes. This is one of the key lessons learned since 2004, and it is important to the understanding and proper positioning of an ERM effort.

A graphic representation of the positioning of ERM is in Figure 2 below. The risk management activities related to strategy are represented by the circle that sits in the middle of the value-chain between the mission, vision, and core values of the organization and its enhanced performance. Figure 2 also illustrates the relationship between ERM and the organization's mission, vision, and core values. The wrong mission and vision will create risks as will misguided values. This figure then helps demonstrate that ERM is not an end point but an integral part of the processes by which an organization develops and executes its strategies to achieve its mission and vision.

Figure 2. COSO 2017 ERM Framework Strategy

Source: COSO ERM Framework, 2017

The Relationship between Strategy and Risk

One of the key responsibilities of a board is the oversight of the strategies of the organization. This oversight role extends from the development of strategy through the assessment of the organization's performance in executing those strategies. Events may occur that could impact the ability of the organization to achieve its strategies and business objectives, however, those events are the risks that the organization faces. All strategies have embedded risks. The clarification of that relationship between strategy and risk, and their effect on overall performance, is one of the key points clarified by the updated COSO Framework.

The Framework also discusses two additional types of risk related to strategies: namely, (i) the risks that the strategy may not align with the organization's mission, vision, and core values and (ii) the implications from the strategy chosen. For example, an incentive compensation strategy that is focused on short term cash incentives may not align with the organization's long term, sustainable growth objective. The implication of a large stock buyback program may similarly be the inability to adequately invest in needed R&D.

Board guidance published in South Africa offers a quick, useful way to think about the relationship between the board and strategy, risk, performance, sustainability, and value creation. See Example 1 below. The board is responsible for the oversight of the organization's strategies and their related risks. While it may delegate day-to-day responsibilities to management, it retains ultimate responsibility for oversight seeing that management is achieving the strategy and business objectives. Example 1 also introduces the concept of sustainability, the need for the organization to focus on value creation for the long term not just short-term maximization.

EXAMPLE 1

The Relationship between Strategy, Risk, Performance and Value Creation

"The governing body should appreciate that the organization's core purpose, its risks and opportunities, strategy, business model, performance, and sustainable development are all inseparable elements of the value creation process."

That simple statement and principle encapsulates the thought process underlying the updated COSO guidance namely the importance of linking and aligning strategy, risk, performance, and sustainability to create value and ensure the long-term success of the organization.

Source:
"King IV Report of Corporate Governance for South Africa 2016"
The Institute of Directors in Southern Africa, 2016, Page 40.

Linking the relationship between strategy and risk is beneficial to evaluating which risks are most critical to the organization. There are various levels of severity and impact of risks. ERM helps not only identify risks but also assesses which risks are significant enough to impair the organization's ability to achieve its objectives. Those are the events and risks related to the core strategies that the organization's ERM activities must identify and manage to be successful.

ERM helps organizations identify, assess and manage the risks to their strategies. It is a practical way to create and protect value and should be an integral part of the strategy selection process. Understanding the role of ERM is key to avoiding a common mistake many organizations make. ERM is not a separate, stand-alone function but is embedded in the fabric of how the organization sets and monitors its strategies and helps enhance the overall performance of the organization. It also answers a question that some ask, which is "*What is the real value of ERM*?" If you attempt to answer that question with a separate, not aligned ERM activity, the answer is often unclear. If ERM is understood and positioned as described by COSO, however, the answer becomes clear; its benefit is improved decision making and ultimately improved performance of the organization as it strives to meet its mission and achieve its strategies and business objectives.

Understanding and supporting these objectives for ERM are critical for boards and managements to both help improve their organizations and to understand the benefit and return for an investment in ERM.

EXAMPLE 2

What ERM is

- An ongoing/continuous process
- A way to help create and preserve value
- Includes practices that management puts in place to manage risks
- A process that can be used by organizations of any size
- An aid to making better decisions

What ERM is not

- A separate activity, not coordinated or integrated with strategy setting activities
- A separate staff function or department
- A "to-do" or checklist
- Applicable only to large, public companies
- Simply a listing or inventory of risks
- A solely quantitative exercise

The Benefits of Integrated Enterprise Risk Management

As noted, one of the "lessons learned" during the evolution of ERM was the need to integrate it into the organization's existing processes including strategy setting, governance, performance management and internal control. Separate, "silo-ed" ERM functions, can seldom, if ever, deliver the level of benefits of an ERM function that is fully integrated into the core businesses processes of the organization. Bob Hirth, former chair of COSO put it this way, "*Rather than heaping on ERM as a separate and new item, we are suggesting it dovetail in and enhance what is already occurring.*"[1] That integration of ERM is critical to not only the success of an ERM initiative but key to obtaining the real benefits of an investment in ERM. Those benefits include:

- Increase the range of opportunities by considering both the positive and negative aspects of risk
- Increase positive outcomes and advantages while reducing negative surprises
- Respond more proactively to risks versus reactive responses
- Enhance ability to identify and manage entity-wide risks
- Reduce performance variability
- Improve resource deployment
- Hold richer and more robust conversations and dialog among management and the board about risks

Another way to look at the benefit and value of ERM is its contribution to better decision making. Boards and management are constantly faced with decisions ranging from strategy decisions to day-to-day decisions. An ERM process provides additional risk information related to the strategies to enable them to make better informed decisions to create and protect value.

EXAMPLE 3

"Integrate" ERM in the Organization

What does it mean to "integrate" ERM in the organization? The key concept underlying integration is to add the ERM activities to existing activities rather than creating separate and entirely new processes and practices. For example, most organizations already have some kind of budgeting or performance planning process. A first step in integrating ERM may simply be to add one page to the existing budgeting process for each business unit to articulate: first, what events are they concerned with that may impair their ability to achieve their budget/business plan objectives, and second, describe what activities they will undertake to monitor and manage those possible events.

Using the 2017 COSO ERM Framework

Any ERM effort must fit the governance structure and culture of a specific organization. The 2017 ERM Framework recognizes this need and facilitates tailoring as it is not a checklist or to-do list of specific actions, but rather it is comprised of a set of five interrelated components that are built off 20 foundational principles (see Appendix A – *COSO Updated Framework and Principles*). This principles-based Framework provides organizations a structure under which they can develop and tailor specific risk management actions and practices that best fit their organization. The principles also provide organizations with an inventory of principles that they can use to identify additional areas to focus on as they evolve their ERM practices and a reference to assess the completeness of their ERM processes.

[1] Interview with Richard J. Anderson, November 2016

II. KEYS TO SUCCESS

As an organization considers implementing or enhancing their ERM activities, it is important to establish a strong conceptual foundation that provides the base to begin the ERM work. Experience has shown that there are some consistent underlying themes that have proven valuable in successful ERM initiatives. These themes represent "Keys to Success" for organizations implementing or enhancing their ERM initiatives. Outlined below are some overarching themes that can form the basis for this foundation. These "Keys to Success" can aid directors and management to avoid recognized barriers and resistance points as they are implementing their ERM efforts.

Theme 1.

Start at the top; board and management support is necessary

Support from the board and senior management is probably the single most important success factor for any ERM initiative. The board and management not only set the strategy of the organization, but they also set the "tone at the top" and define the desired culture of the organization. The tone and priority given to an ERM initiative by the board and management will quickly and visibly determine its success.

This important board and management engagement and support is described in more detail in the Governance and Culture component of the revised COSO ERM framework (see Principle 3: Defines Desired Culture in COSO's 2017 *Enterprise Risk Management – Integrating with Strategy and Performance*). That component of the Framework notes, "An entity's culture influences how the organization applies this Framework: how it identifies risk, what types of risk it accepts and how it manages risk." Establishing a "risk aware" culture across the organization is critical and will determine whether ERM is viewed as a separate compliance driven initiative or viewed as a process to help the organization enhance its value. Starting from the top, for an ERM initiative to be successful, the board and management must clearly embrace the objectives of enterprise risk management and set the tone that it is an integral part of how the organization achieves its mission and its business objectives. Also, as the board and senior management have the best "enterprise view" of the organization they are critical to the success and effectiveness of any ERM initiative.

The board must also demonstrate clear support for ERM as an important strategy and governance process and provide clear direction and oversight to management's ERM undertakings. It is the board's responsibility to see that management is devoting the right level of attention, resources and priority to ERM and that actions are being taken to integrate ERM with the appropriate functions and processes across the organization. Failure to do that can result in separate, lower level staff functions who do not have an appropriate support or voice and as a result, the organization will not realize fully the benefits of ERM.

Further, the board should see that an effective ERM leader is in place who is widely respected across the organization, knowledgeable about its businesses and strategies, and given the resources and support to accomplish the ERM effort. That leader should also be at a level in the organization that affords them access to the board and management and involvement in key strategy setting and planning activities.

Appendix C – *Frequently Asked ERM Questions* includes responses to some common questions related to ERM that directors and senior management should find useful.

Theme 2.

The role and objective of ERM must be understood and communicated

The 2017 Framework makes explicit the role and objective of ERM as helping the organization enhance value. This clarity is beneficial in helping people understand the real benefit and value of an investment in ERM and avoiding misunderstandings about its role and objective. As ERM was receiving increased attention from regulators, rating agencies, and financial reporting agencies, it led some organizations to view ERM as a regulatory or compliance driven activity. Likewise, some viewed ERM as a simple exercise in risk identification. The Framework brings needed clarity in explicitly describing the role and objective of ERM as helping the board and management make better decisions and enhancing the value of the organization. This role and objective needs to be understood fully by directors and management. They can then correctly position any ERM initiative.

That clarity of the role and objective of ERM is also useful in building a culture where all members of the organization understand that managing risk is a part of their day-to-day responsibilities. Education and communications concerning the role and objective of ERM are needed and they become the enablers to help establish and build the desired risk culture. These communications should be widespread across the organization and iterative. They should articulate not only the role and objective of ERM but the priority that management places on this activity as being an important process helping the organization achieve its mission, vision, and core values. The communications should also be simple and straight forward so that people can understand how this activity relates to them personally.

Theme 3.
ERM must be integrated into the fabric and culture of the organization

As noted above, one of the clear "lessons learned" during the evolution of ERM is that successful ERM activities must be integrated into the organization's culture and core strategy-setting and performance processes. Integration with those core business processes is necessary to achieve the real benefit of ERM and it also is helpful in avoiding the misconception that ERM is just a separate compliance or regulatory driven staff function. In the early years of ERM, unfortunately, some organizations did not have this clarity and understanding, and undertook ERM activities that were not aligned with strategy and not integrated with the business. Therefore, they struggled to understand the benefit they were receiving for their investment.

The importance of culture is also reflected in Principle 3 of the revised COSO ERM framework which states, "The organization defines the desired behaviors that characterize the entity's desired culture." That principle also notes that, "It is up to the board of directors and management to define the desired culture of the entity as a whole and of the individuals within it."

EXAMPLE 4

Fitting ERM with the Culture of the Organization

At a transportation company, the internal audit function became the catalyst for not only developing the company's ERM process but ensuring that it fit the culture of the organization. Internal audit designed the ERM process and activities to fit the culture and management style of the organization. For example, the organization does not have a CRO or dedicated risk staff as that may be perceived as adding bureaucracy in an organization that prides itself on running "lean." However, they do have a robust, consistent risk management methodology, terminology, and reporting processes that are executed by their Management Risk Committee. Management has accepted and embraced the ERM process and has integrated ERM within the annual business planning cycle. In addition, the Board is engaged and values an ERM program with a solid footing that underpins all their enterprise activities.

Particularly for organizations just starting an ERM initiative, integrating with existing processes also provides a simpler path for initiating ERM than creating an entire separate process and function. Organizations already have processes in place for establishing their strategies and implementing them in their lines of business. They also typically have a performance measurement or budget process to assess their performance. Integrating enterprise risk management activities into these existing processes is not only simpler but reinforces the concept that the risk activities are related to and focused on the performance and value of the organization. In particular, as the ERM process is directly linked to the organization's planning and strategy development processes, integrating ERM with those specific processes makes good sense and is necessary. Integration with these existing processes also is more likely to be lower cost than creating complete stand-alone functions. As the risk management activities are also broadened into and across the business activities, they also help build and evolve the culture to include risk awareness at all levels of the organization.

EXAMPLE 5

The Integration of Strategic Planning and ERM

A good example of the integration of strategic planning and ERM is found in a US-based global manufacturing company. This organization has integrated its strategic planning group into its enterprise risk management effort. The head of their strategic planning function is a member of an executive risk committee, where each executive risk owner prepares a risk map of the risk(s) that they are responsible for. The strategic planning group then reviews the risk maps and considers the risks as they relate to the organization's strategic plan. The risk maps are updated prior to updating the organization's strategic plan so that the risks can be considered as management and the strategic planning group update the strategic plan.

The integration of the enterprise risk management activities also helps organizations avoid a "siloed" risk management environment where separate parts of the organization are undertaking independent risk related activities. Following the financial crisis of the prior decade, several studies pointed out that organizational silos were detrimental to the ability of some organizations to see and respond to the developing turmoil. The integration can also foster an environment and culture of knowledge and data sharing across the organization.

Theme 4.

The starting point is to focus initially on the organization's top strategies and business objectives

The starting point for enterprise risk management is to specifically and carefully identify the key strategies and business objectives of the organization. Depending on when the ERM initiative is started, this can be conducted during the strategy setting process or done by analyzing existing strategies. ERM does not start by simply attempting to identify risks, but it starts with a thorough analysis of the organization's key strategies and business objectives. Following the updated Framework, the organization is trying to identify those events that might impair its ability to achieve its strategies and business objectives. Accordingly, there first must be a clear understanding of the key strategies and business objectives before one can assess the events that could impair those strategies. The sequence is critical and, again, reinforces the objective of ERM as helping the organization be successful with its chosen strategies. Put another way, in approaching ERM, the organization needs to be "strategy-centric" not "risk-centric."

Theme 5.

The key risks are those events and outcomes related to the key strategies

The key risks that ERM is focused on are those events, and the resultant outcomes, that could impair the organization's ability to implement its specific strategies identified above. All organizations face a multitude of risks of various levels of likelihood and impact, some large and others smaller. While smaller risks can cause problems for an organization, various studies have shown that the biggest losses of value for organizations are from strategic risks, those risks and events related to key strategic decisions. The linkage of ERM with strategy provides a lens that enables the organization to identify, within its total population of risks, those risks that are most significant to its success. This "lens" can be especially useful in large organizations who by their nature face a multitude of various kinds and sizes of possible risks. Linking risk to strategies will enable directors and management to focus on a smaller number of more critical risks, those which are most worthy of their time and attention.

EXAMPLE 6

The Significance of Risk in Two Organizations

Two different companies have operations outside of the US. These activities present each organization with foreign exchange exposure and risk. One organization's activities outside the US are limited and the organization does not plan to significantly expand those activities. Its level of foreign exchange exposure is minimal and is managed and hedged within its Treasury function. The other organization has implemented a plan to significantly expand its overseas activities, including in countries with a history of volatile foreign exchange rates. That strategy and exposure to rate movements is potentially large enough to impact the financial condition of the organization. As a result, a much more robust risk management process is needed regarding the performance of this strategy including ongoing monitoring of its foreign exchange exposure and results and reporting to the board and management.

Theme 6.

Start with simple actions and build incrementally

One misconception and barrier to beginning an ERM initiative is the perception that ERM is overly complex and requires a major and costly effort to implement. Related to this misconception is the belief that an organization must implement fully all the components of ERM in one single effort to bring tangible value to the organization. Experience suggests otherwise.

In practice, some organizations, especially smaller organizations, have achieved ERM success by taking an incremental, step-by-step approach to implementing or enhancing their risk management activities rather than one massive undertaking. They start with simple risk management processes and actions and build from there using incremental steps rather than attempting to make a quantum leap to implement fully a complete ERM process.

Approaching ERM in this manner also means that supporting ERM processes such as reporting, data gathering and analysis, and the use of technology can be introduced at the right time corresponding to the maturity level of the ERM practices and the knowledge levels of the key stakeholders. Building incrementally also allows organizations to:

- Bring the board and management up a learning curve about ERM. Directors and members of management typically have varying levels of understanding of ERM and its objectives and processes. For ERM success, these individuals need a consistent level of understanding about ERM and how it will benefit the organization. Taking incremental steps provides an opportunity to educate the directors and management at each step and help them progress up a learning curve about ERM. Experience has shown that organizations that undertake ERM initiatives with directors and management who do not understand fully what is being proposed are not likely to be successful. To put it another way, as the board and management move up their own learning curve about ERM, they will then drive the organization's ERM processes to more mature levels.

- Provide the ability to change and further tailor ERM processes. A successful ERM initiative must be tailored to the governance structure and culture of the organization. An incremental approach affords the directors and management the ability to assess at each step exactly how best to tailor ERM activities as the process evolves and matures. They then are in a better position to make additional requests to broaden or deepen the organization's risk management activities and to ensure that the activities being deployed are right for their specific organization.

- Facilitate the identification and evaluation of the benefit at each stage of development. A possible barrier for ERM is the question of "*What benefits are we receiving from our ERM activities*?" Building incrementally provides an opportunity to assess and demonstrate the benefit of each step or action. For example, an initial action may be to complete and share with the board for the first time a concise summary of the key risks related to their core business strategies and the actions that management is taking to address the risks identified. Example 7 shows three examples to illustrate this point:

EXAMPLE 7
ERM Actions and Their Related Benefits

Incremental Action Step	Benefit Received
Perform an assessment of the key risks related to the core strategies of the organization and prepare a report to the board showing the strategies and related risks.	Board and senior management see and discuss, often for the first time, a consensus view of the risks related to their core business strategies. This builds a common understanding and tangibly demonstrates the relationship between strategies and risks.
Prepare a strategy map reflecting the organization's business objectives, the related business strategies and risks and the existing risk management activities of the organization. Use the strategy map to identify gaps in the existing ERM activities.	The strategy map and analysis will provide transparency to existing risk management activities and provide management and the board a starting point for discussions on the risk management activities and opportunities to enhance those activities.
Different business units and staff functions within an organization may be using different definitions or terminology related to risks. Develop a common taxonomy or definitions of risks that would be used consistently by all units across the organization.	A common risk language will facilitate enterprise wide assessments and reporting of risks and risk activities. It also can provide consistency in how units assess and report on risk and the sharing of risk related information and data It facilitates the establishment of an enterprise risk culture.

Theme 7.
Leverage existing resources and risk management activities

One misconception and barrier to beginning an ERM initiative is the perception that ERM is overly complex and requires a major and costly effort to implement. Related to this misconception is the belief that an organization must implement fully all the components of ERM in one single effort to bring tangible value to the organization. Experience suggests otherwise.

Any organization will typically have some forms of risk management activities or risk related processes in place. These activities are frequently informal or unstructured or not aligned across the organization. Many organizations have successfully entered the ERM arena by leveraging existing resources with knowledge and capabilities related to their core strategies, risks, and risk management. For example, some organizations have used their head of Strategic Planning or their Chief Audit Executive as the catalyst to start their ERM effort. Also, with increasing frequency, organizations form a management-level risk 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 strategies and the related risks to get ERM moving. When forming these management risk committees, it is critical to involve line business leaders, not just staff personnel, to obtain the knowledge of strategies and business objectives.

Using existing resources and activities helps avoid the potential barrier to initiating ERM that is the view that an ERM process requires significant new resources such as investments or outside resources to undertake the ERM process. 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. In addition, most organizations start their ERM efforts without investments in any specific enabling technology or data support. These enablers may come later as the ERM processes mature but are not necessarily required to get started.

III. INITIAL ACTION STEPS

This section describes action oriented, "how-to" steps to implement an initial ERM effort including a basic methodology, process, and related frameworks to assist in the identification of key strategies and their related risks. These steps build from the "Keys to Success" above and describe some simple steps that can serve as the basis for a tailored action plan to implement an ERM initiative. To further assist organizations in implementing ERM, we include, in Appendix B — *Where to Start: Draft Action Plan for an ERM Initiative* — an initial, draft high-level action plan. The draft action plan highlights eight key events and actions that organizations should consider when starting an ERM effort. The draft plan is not intended to be used as a complete action plan but rather as a starting point that would be tailored and expanded prior to use. The Appendix B draft action plan adds details to the action plan steps summarized in this section and reflects useful information which is a practical basis for developing an organization-specific action plan.

Step 1.
Seek Board and Senior Management involvement and oversight

This step would involve setting an agenda item for the board and executive management to discuss ERM which could include the following topics:

- Establishing that the overall objective of ERM is to enhance the performance of the organization, not just to identify risks.
- Discussing how ERM helps in achieving the organization's strategies and business objectives.
- Stating and discussing the need to integrate ERM with the organization's strategy and performance processes.
- Identifying the expected benefits from an integrated ERM approach.
- Discussing how ERM would change the culture of the organization.

It would also include agreeing on high-level objectives and expectations regarding a risk management initiative. It would also include understanding the process to communicate and set the tone and expectations of ERM for the organization and agreeing on a high-level approach, resources, and target dates for the initial ERM effort.

Conducting education and discussion sessions with the board and senior management to clarify the role and benefits of ERM and its relationship to strategy setting and performance measurement can set the stage for a successful ERM implementation. Consider circulating the Executive Summary to the 2017 Framework[2], as well as this COSO thought paper, and consider where/who in the organization should be responsible for the ERM initiative. Since responsibility for strategy is with the board, oversight of the top risks should also remain with the board. While the full board is responsible for overseeing the top risks of the organization, the full board may determine that it is more practical for one of its board committees to understand, review, and approve the process management has in place to identify, assess, and manage risks. One approach is the possible delegation of the ERM process review to a board committee such as audit committee, risk committee, or strategic planning committee. Where the oversight responsibility for ERM is placed is an organization by organization decision.

Step 2.
Identify and position a leader to drive the ERM initiative

Identify a person with the right attributes to serve as leader of the risk management initiative. Critical attributes would include an in-depth knowledge of the organization's overall strategies and business objectives, an appropriate level and stature within the company, ability to acquire appropriate resources, and the appropriate authority to execute their responsibilities.

It is also critical that the ERM leader have direct access to the top of the organization, ideally to the CEO and be an integral player in the strategic planning process. If they are too low in the organization hierarchy or have no input or involvement with strategic planning, the ERM process will likely not be value adding.

[2] The Executive Summary to the ERM Framework is available for free download at coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

Identifying a leader for the ERM effort doesn't mean the company needs to appoint a "Chief Risk Officer." Sometimes, it is best to use existing resources, for example the Head of Strategy, Chief Internal Auditor, or Chief Financial Officer to get ERM launched. Given the need to link ERM to strategy, the organization's head of strategic planning may be an excellent candidate to lead the ERM initiative. Regardless of the position of the ERM leader, that person needs to be involved in the organization's strategic planning process or at least an observer of the process to ensure that the ERM and strategic planning processes are integrated fully. The risk leader is not necessarily the person to head risk management long-term, but the person with the deep understanding of the organization's business and strategies to get the initiative started, build momentum and take the ERM initiative to the next level.

Step 3.

Establish a management working group

Establish an executive level management working group to support the risk leader and drive the effort across the organization. Such a working group helps in both communicating the ERM effort and in obtaining broader buy-in for the process. Quite often, these working groups evolve into a standing management-level risk committee.

The initial objective of the working group should be to determine next steps and action plans. Here it is important to get the "right people" involved to ensure success. The group may include executive level personnel not just staff, and business leaders who know the strategies and can consider how to embed the ERM processes in the businesses. The committee's actions should result in tangible benefits.

The working group should start by developing the objectives and expected benefits from an ERM initiative. This can include considerations of the current and expected culture as it relates to risk management. The working group also needs to understand and discuss the need for ERM to be integrated and linked into the strategy setting and performance measurement processes of the organization. It may be helpful for the working group to spend time reviewing and understanding the updated Framework to ensure that participants have the appropriate understanding of the objectives and benefits of ERM.

EXAMPLE 8

Initial Objectives for a Management Working Group

A major financial institution formed a Management Risk Steering Committee as a first step in aligning its various risk management activities. The committee included senior level business executives as well as senior executives from its various risk and control units. The committee began its activities by developing a set of four overall objectives for the committee. These objectives were:

- Agree on a common risk management concept for various functions across the Company who deal with risk ("risk management functions")
- Maintain the independence/objectivity of each risk management function
- Rationalize and harmonize approaches to risk across the Company
- Increase information sharing across the risk management functions

The committee then developed specific actions and plans under each objective. In particular, the committee was focused on increasing the sharing of risk related information across the organization. These four objectives were subsequently achieved, and the committee then developed a second set of more granular risk related objectives to continue to mature their risk management processes.

Step 4.

Inventory the existing Risk Management Practices of the organization.

Identify and inventory existing risk management practices, whether formal or informal, and ensure they are aligned and coordinated. During this step, the working group should undertake an effort or project to identify and catalog those existing practices. This effort can be accomplished in various ways, including through facilitated sessions of the working group, by surveying business units, or by involving personnel from various risk or control units who may have this knowledge, such as internal audit staff.

After these existing practices have been cataloged, the working group can consider how those practices fit or align with the organization's strategy setting and performance review process. This will allow them to identify gaps and opportunities to further integrate the organization's strategy and risk processes. Often, this step highlights a lack of common risk language across the organization. Various units may be defining or describing risks differently, which may present the working group with the opportunity to develop and communicate a set of common risk definitions or "risk language" across the organization. A common risk language or taxonomy is not only helpful but in fact is necessary to communicate and establish consistent risk processes across the organization.

EXAMPLE 9

Taking Inventory of Risk Management Activities and Integrating Risk Management into the Decision-Making Processes

The CFO of a global manufacturing company realized that the organization had separate, detached risk management activities across the company. Risks such as financial, employee safety, operational, IT security, and legal were being handled as separate "silos" without any consistent reporting. The CFO assigned a risk leader to inventory their existing risk management practices and develop an enterprise risk management process. One result of the inventory process was that the company realized that they were not identifying and addressing risks related to their key strategies. They added risk processes related to their strategies including the use of scenario analysis to help the company test strategies for resilience and relevance. In addition, they began a process to subject possible business projects to a systematic risk and opportunity assessment as part of preparing the business case before final decisions are made about a possible project.

Step 5.

Conduct an initial assessment of key strategies and related strategic risks

Understand the organization's key strategies and the related risks and how they are managed. This involves first identifying the organization's key business objectives that enable those strategies, then the Strategic Risks related to the strategies. "Strategic Risks" as used in this paper refers to those events and risks that could impair the organization's ability to achieve its strategies and business objectives. This is consistent with the ERM Framework, which refers to risks as "one or more potential events that may affect the achievement of objectives." These are the risks that are most significant to the long-term success of the organization. Other risks may hurt or cause a loss of some value, but these are the risks where the organization could lose significant value. The organization should also strive to identify external and emerging risks that could impact the organization and its strategies.

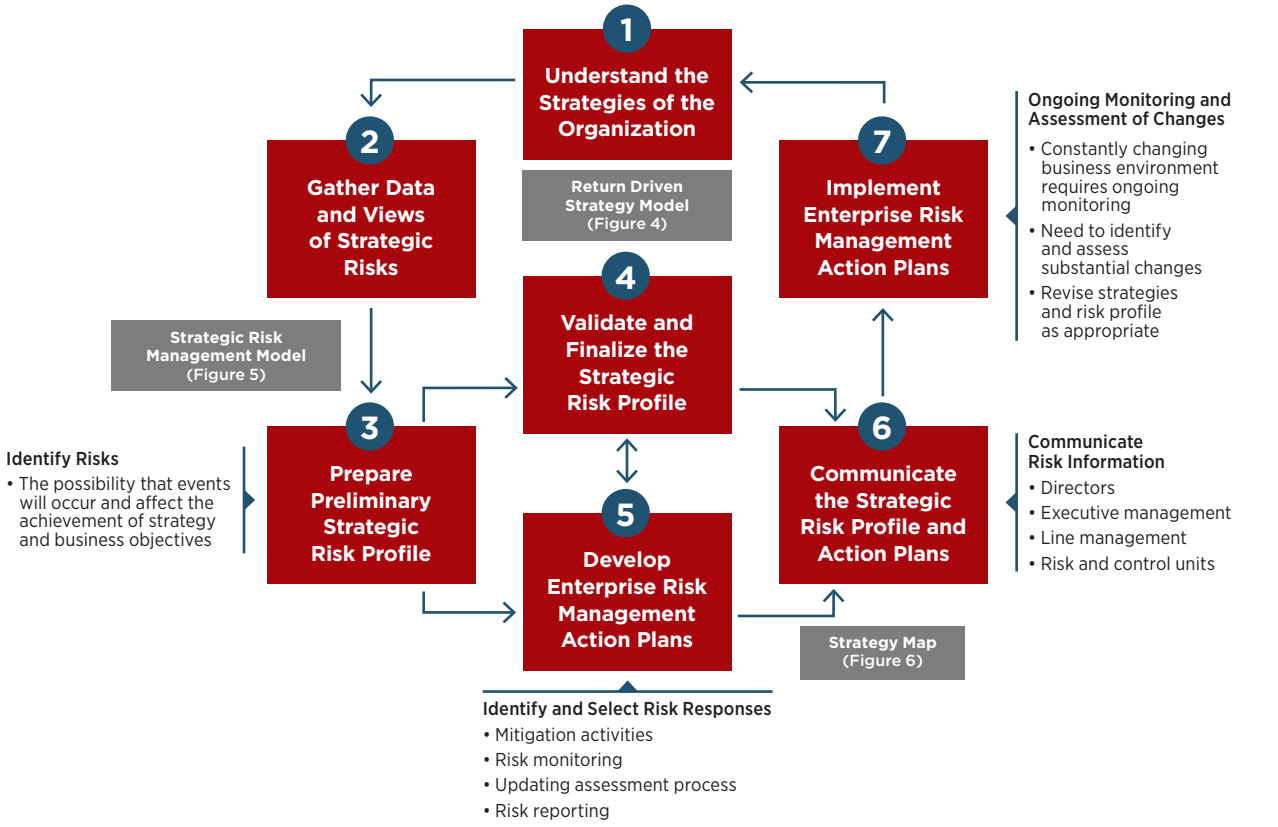
EXAMPLE 10

The Strategic Planning Group as Owner of "Black Swan" Risks

"Black Swans" or "Unthinkable Risks" are low-frequency/high impact events, which can have severe negative impacts on organizations. A major manufacturer of transportation products has tasked their strategic planning group with the responsibility for their "Black Swan" risk process. The planning group identifies and assesses "improbable" risk events. The risks identified are then communicated and discussed with their internal risk committee. The strategic planning group also considers the possible impact of these risk events on the organization's long-term strategic plans. Finally, the risks, possible impacts on the organization's strategies and business activities, and the related risk management actions are then reported to and discussed with the Board.

Organizations can benefit from using a Strategic Risk Assessment Process. The seven-step process shown in Figure 3 has been used in the Strategic Risk Management Lab at DePaul University in its graduate seminar courses and workshops and applied at organizations in risk assessment and other ERM initiatives.

Figure 3. Strategic Risk Assessment Process



Source: Adapted from Frigo, Mark L., and Richard J. Anderson. "Strategic Risk Assessment: A First Step for Risk Management and Governance." Strategic Finance (December 2009) and Frigo, Mark L. and Richard J. Anderson, *Strategic Risk Management for Directors and Management Teams* (2011). Used with permission.

The Strategic Risk Assessment Process includes seven steps, representing a continuous process for organizations to assess and manage risks. While depicted differently in Figure 3, these seven steps align with the components in COSO's 2017 Framework.

1. Understand the strategies of the organization
2. Gather data and views on strategic risks
3. Prepare a preliminary strategic risk profile
4. Validate and finalize the strategic risk profile
5. Develop enterprise risk management action plans
6. Communicate the strategic risk profile and action plans
7. Implement the enterprise risk management action plans

The Strategic Risk Assessment Process, along with its supporting models have been used in the Strategic Risk Management Lab at DePaul and has been successfully applied and vetted at many organizations. This risk assessment approach can be useful in both identifying the key strategies of the organization and the related critical risks. These supporting models are to be used sequentially. First, the Return Driven Strategy Model is used to identify the major strategic initiatives of the organization. While the organization may have many initiatives underway, the model is used to identify those strategies that are most critical to the achievement of the organization's overall business objectives. Second, once those key strategies are identified, the Strategic Risk Management Model is used to identify corresponding risks related to those key strategies. See Appendix D- *Examples of the Relationship between Strategies and Risks* for examples of the thought process for the assessment of risks related to strategies.

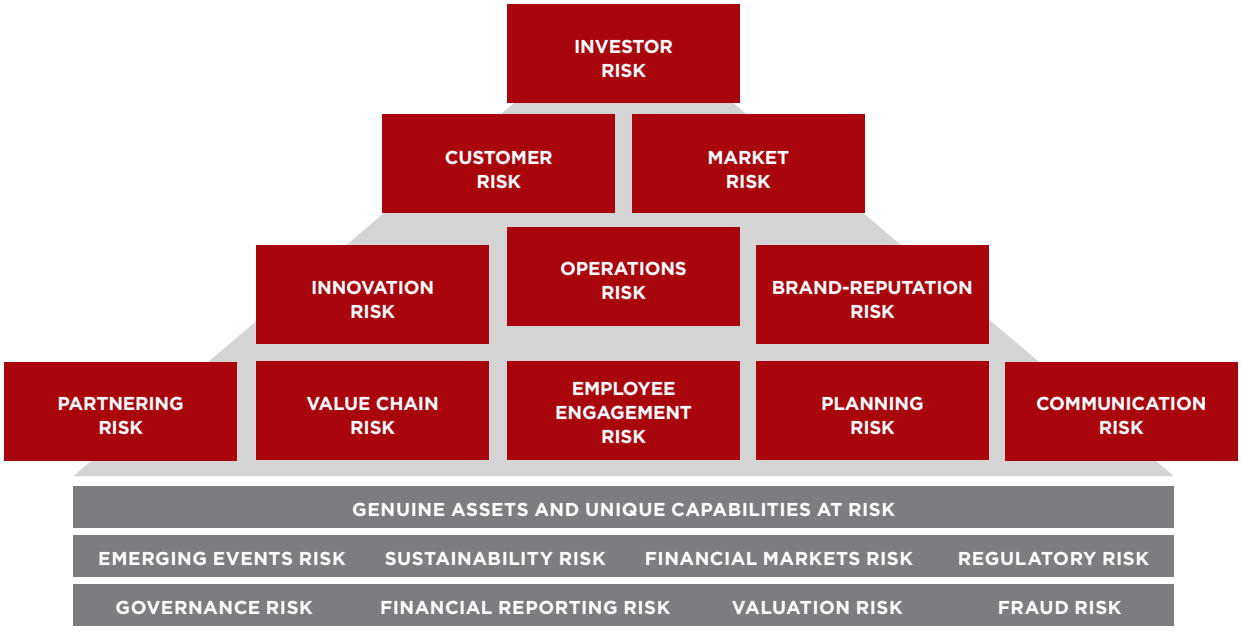
The Return Driven Strategy Model (see Figure 4) provides a way to understand the strategy of the organization as a first step in the Strategic Risk Assessment Process. It provides a structure that is useful to break down the strategies of the organization into separate, discrete components. This can be especially helpful to identify and categorize individual strategies so that the related risks can then be considered.

In this part of the analysis, input from business line leaders is imperative to ensure that the analysis includes all critical business strategies. This detailed analysis of the strategies then allows for a strategic risk assessment utilizing the related Strategic Risk Management Model (see Figure 5).

Figure 4. Return Driven Strategy Model

Source: Frigo, Mark L. and Joel Litman. *DRIVEN: Business Strategy, Human Actions and the Creation of Wealth*. Strategy & Execution (2007). Used with permission.

Figure 5. Strategic Risk Management Model



Source: Frigo, Mark L. and Richard J. Anderson, *Strategic Risk Management for Directors and Management Teams* (2011). Used with permission.

The Strategic Risk Management Model provides a way to identify the risks related to each of the strategies identified. It is used as an aid in the second step in the Strategic Risk Assessment Process.

Utilizing these two models in the sequence of first identifying the critical strategies and then the related key risks provides a methodology that is consistent with the COSO ERM principles, including starting the process by focusing on the strategies not the risks. The Strategic Risk Assessment Process and related models also provide an approach to identify and work with a manageable number of critical risks that are most significant in regard to the key strategies of the organization. This process also establishes a clear linkage between the strategies and the related risks and provides a way to prioritize those risks.

EXAMPLE 11

Thinking the "Unthinkable"

The audit committee chair of a public company believed that the audit committee did not have sufficient time in its regular agenda for detailed discussions on the topics of risk and ERM given their normal committee activities. In particular, the chair was concerned that among other risks, the audit committee needed to consider "unthinkable risks," which are low-frequency/high-severity risks that do not generally receive the same level of focus as high-probability/high impact risks. Accordingly, they added four meetings to the annual audit committee agenda that would be focused solely on risk and ERM. One meeting is focused solely on cybersecurity. Two other meetings are focused on selected risk topics as circumstances dictate. The fourth meeting is then devoted solely to a discussion of "unthinkable risks" and has proven to be very valuable in fostering robust discussion among the directors and identifying new areas of risk for consideration.

For additional information regarding identifying and assessing risks, review the Performance component of the COSO ERM framework and Principles 10 – 14 that are contained in that component.

Step 6.

Develop a Consolidated Action Plan and Communicate to Board and Management

Develop action plans and respond and manage the risks identified. Enterprise risk management is more than just identifying risks. The real value of ERM is developing action plans to respond and manage the risk identified. This is the key to helping the organization achieve its strategy and business objectives. An effective ERM process develops and implements risk responses to enhance its ability to be successful. This is consistent with Principle 13 of COSO ERM Framework which indicates that: "The organization identifies and selects risk responses."

Risk responses in an action plan may take many forms. The 2017 ERM Framework cites five types of risk responses; accept, avoid, pursue, reduce, and share. The risk response to each critical risk identified needs to be appropriate for that specific risk and the organization's risk appetite. The action plans should be developed and combined into a consolidated action plan addressing the organization's responses to the critical risk identified. The action plan should also prioritize actions and responses and allocate resources across those actions. In particular, the organization should assign specific responsibility and accountability for actions and monitoring.

The consolidated initial action plan should then be presented to and discussed with the board and management. Here, the organization's risk leader or management risk committee should be actively engaged. Consideration should also be given to developing a communications plan to communicate risk identified and responses across the organization

Step 7.

Develop and/or Enhance Risk Reporting

Consider risk reporting that will be part of the organization's ongoing ERM process. Given the dynamic nature of risk and ongoing changes to the organization's strategies, a robust risk reporting process is necessary. Initial risk reporting should be simple and clear. In particular, users of the risk reporting should receive information that is focused, understandable, and clearly communicates risk priorities and severity. As risk management processes mature, risk reporting can become more granular and detailed and possibly include some quantification. The organization should also consider how its risk reporting process fits and integrates into its existing performance measurement processes rather than developing a separate line of reporting. A starting point here is to review its existing

performance reporting processes and then integrating risk reporting into those existing processes. For example, many organizations use balanced scorecards as part of their performance reporting processes. Some of these organizations have expanded their balanced scorecards to include risk reporting and monitoring. Consideration should also be given to periodic reporting of emerging or systemic developing risks.

The use of colors, graphics, and other visuals have also proven helpful in bringing clarity to this reporting. For example, some organizations have used "risk dashboards" to facilitate this reporting. Another useful visual tool is a strategy map, which are visual tools linking the organization's objectives, strategies, risk, and risk management processes. An example of a strategy map is below in Figure 6.

Figure 6. Strategy Map Example

Create and Protect Shareholder and Stakeholder Value

Strategic Objectives	Improve Productivity	Profitable Growth from New Technologies and Services	Increase Value from Existing and New Customers	Organizational Efficiency and Leverage
Customer Strategic Objectives	Cost & Quality Leadership	Develop Technologies to Improve Cost and Performance	Deliver Highly Valued Solutions	Customer Focused
Strategic Themes	**Return Driven Strategy Tenets**			
Internal Process Strategic Objectives	Fulfill Otherwise Unmet Customer Needs	Ethically Maximize Wealth		Target Appropriate Customer Groups
	Innovative Offerings	Deliver Offerings	Brand Offerings	Partner Deliberately
	Map and Redesign Processes	Engage Employees and Others	Balance Focus and Options	Communicate Holistically
Strategic Risk	**Strategic Risk Management Framework Risks**			
	Genuine Assets and Unique Capabilities Risk			
	Emerging Events Risk	Sustainability Risk	Financial Markets Risk	Regulatory Risk
	Governance Risk	Financial Reporting Risk	Valuation Risk	Fraud Risk
ERM Components	Governance and Culture | Strategy and Objective-Setting | Performance			
	Review and Revision | Information, Communication, and Reporting			

Source: Adapted from Frigo, Mark L. and Richard J. Anderson, *Strategic Risk Management for Directors and Management Teams* (2011). Used with permission.

EXAMPLE 12

Integrating ERM Strategic Objectives in Strategy Maps

A global technology company used the Strategic Risk Assessment Process and related frameworks as the basis for starting their ERM initiative. The company had started an ERM initiative and realized the company needed to better describe its strategy before conducting a risk assessment and ERM. Strategy Maps like the one in Figure 6 were developed to help describe the strategy of the company as part of its Strategic Risk Assessment Process. The company also established an overall strategic objective in its Strategy Map which was highly aligned with risk management: Create and Protect Shareholder and Stakeholder Value. The management team then developed specific objectives relating to ERM in a Strategy Map, including developing strategic risk management skills and culture. They also created specific risk management objectives in each of its four internal process strategic themes: Conducting Strategic Risk Assessments; Protecting IP; Protecting Customer Information; and Minimizing Product Defect. These objectives help to integrate risk management with the strategy and performance of the company. The tactical action plan used by the company was to include specific risk management strategic objectives in the strategy of the company and to reflect those in the strategy map and also to develop performance measures and action plans related to those strategic objectives which further helped the company connect risk management with strategy and performance.

Step 8.

Develop the Next Phase of Action Plans and Ongoing Communications

Conduct a critical assessment of the accomplishments of the working group and develop the next steps in the evolution of their risk management processes. This assessment can include such activities as the identification of benefits achieved to date, assessing the level of integration with strategic planning and performance measurement processes and assessing the impact on the culture of the organization. In this step, the group should revisit the COSO ERM Framework as an aid to identify the next risk management processes for enhancement. Consideration can be given to actions such as;

- Establishing or articulating the risk appetite of the organization.
- Implementing a process to identify and react to organizational or strategic changes.
- Determining how the ERM process can be enhanced to identify opportunities not just threats.

The new action plan should also identify tangible steps including the specific benefits sought and target dates. The plan should be reviewed with executive management and the board, to assure that the new action plan receives appropriate resources and support. The risk leader should also consider scheduling additional ERM sessions with directors and executive management to further educate them and to update them on the progress and benefits of the ERM initiative. Finally, the risk leader should continue an organization-wide communication process to further build and reinforce the desired risk culture of the organization.

IV. CONTINUING ERM IMPLEMENTATION

The intent of this paper is to provide simple, straightforward, and practical ideas on a basic approach to implementing an ERM initiative, with the ultimate objective of creating and protecting value. As such, it is a beginning point not an end point. It also describes a continuous process to avoid treating ERM as an event. Given the dynamic nature of risk, rapid disruptive changes in the environment, and the evolving nature of ERM, organizations must continue to be vigilant to the forces of change and the need to periodically review and enhance their ERM processes.

COSO Principle 17: "*Pursues Improvement in Enterprise Risk Management*" in the updated Framework sets the tone for this continual improvement process. As noted in Principle 17: "Management pursues continual improvement throughout the entity (functions, operating units, divisions) to improve the efficiency and usefulness of enterprise risk management at all levels." One of the responsibilities of the risk management leader is to build this thinking into the risk culture of the organization and to ensure that it becomes one of the ongoing activities of any risk management effort.

This continual improvement process can occur in different forms. For some organizations, the improvement process will be accomplished by embedding continual evaluations in their ongoing ERM processes. For others, separate periodic evaluations will be performed.

Regardless of the approach used, organizations should strive to continually challenge themselves to enhance their ERM processes as they become more familiar with the process and see opportunities to enhance it in response to the dynamic nature of risk in today's business environment. As it seeks to enhance its process, the organization should continue to approach it through iterative steps rather than a large one-time quantum project.

Continual improvement efforts should also seek opportunities to further link and integrate the organization's ERM efforts with its strategy setting and performance of business processes. For example, organizations should take a hard look at their decision-making processes at both the management and board levels to identify ways in which better risk related data and information can contribute to enhancing the decision-making processes. The organization's performance measurement and reporting processes can be similarly reviewed to determine if they are appropriately measuring and monitoring risks, the risk culture, and the performance of the risk processes.

As an aid to their continual improvement efforts, management should review the updated ERM Framework and the principles reflected in it (see Appendix A – *COSO's Updated Enterprise Risk Management Framework*) to identify possible gaps in those principles that could be addressed to enhance its processes. Again, work based on iterative steps rather than one quantum leap and identify specific, tangible steps and their related benefits.

Outlined below is a beginning list of possible areas to consider for improvements following an initial ERM effort. These activities are presented under the five components of the ERM Framework and are not intended to be a final comprehensive list but a simple working list of activities to consider as a starting point for discussion and review as the organization seeks to strengthen its risk culture and enterprise risk management activities.

Governance and Culture

- Development of formal board and corporate policies and practices for ERM
- Analysis and consideration of human resources needs including skillsets and technical or quantitative capabilities
- A more formal process to reinforce the risk culture through ongoing communications and training

Strategy & Objective-Setting

- Further integration of ERM processes into the organization's annual planning and budgeting processes
- More formal integration into the strategy development process
- Further discussion and articulation of the organization's risk appetite

Performance

- Further expansion and enhancements to the risk assessment processes
- More formal process to prioritize and assess the severity of risks
- Updates to the risk response and action plans

Review & Revision

- Considerations of significant organizational changes
- Development of performance processes, such as a balanced scorecard and strategy maps, to assess performance and benefits of ERM processes
- Development of a more formal continuous improvement process

Information, Communication, & Reporting

- Consideration of the possible uses or application of new technologies
- Consideration or development of new data sources and analytics
- Development of a program of continuing education for directors and executives
- Development of an ongoing ERM education and training for line management
- Considerations of the use of technology and artificial intelligence for enhanced risk monitoring

The above listing is not all inclusive but may be helpful as an organization considers possible next steps in enhancing its ERM processes. The specific steps to be taken must be determined based on the initial steps taken and tailored to the state of maturity and ERM objectives of the specific organization. The critical point, however, is to keep the momentum moving and continuing to evolve, expand, and deepen the organization's ERM capabilities such that they are tangibly contributing to the organization's ability to achieve its strategy and business objectives.

SUMMARY

The business environment today is one in which boards of directors and senior management will continue to face rapid changes, complexities, and volatile risks. Such an environment, however, also presents them with significant new opportunities. Organizations can enhance their abilities to be successful in both addressing risks and taking advantage of opportunities by enhancing their enterprise risk management processes and integrating ERM fully into their strategy setting and performance processes. Enhancing their ERM processes starts with a clear understanding of the role of ERM in assisting the directors and management to make better decisions and achieve their strategy and business objectives. The updated COSO ERM Framework clarifies both the relationship between strategy and risk and that the objective of ERM is to assist the organization to achieve its strategy and business objectives. Understanding these two key points is not only critical for success but important in setting and communicating the risk culture of the organization.

The concepts, approach, and guidance outlined in this paper provides useful insights in how management and directors can take initial steps in implementing or enhancing their ERM processes in alignment with the new guidance. Together with COSO's *Enterprise Risk Management – Integrating with Strategy and Performance* and other COSO thought papers, this paper is a starting point and foundation for an effective ERM initiative. Any ERM initiative needs to be tailored carefully to the needs of a specific organization. The ideas and recommendations presented in this paper are neither intended to be, nor are they, the only way to implement an ERM initiative. The approach of this paper and the updated ERM Framework and related guidance provide the flexibility to tailor an ERM initiative and realize fully its benefits. Keep in mind the benefits of taking small, incremental steps and building a culture of continuous improvement.

Above all, keep the momentum going and help ensure that the organization will increase its chances of successfully achieving its strategy and business objectives though a robust management of the risks that could impair that achievement. The goal is to develop the momentum for ERM which will continue to expand and deepen the organization's strategy setting, performance, and risk management processes in its pursuit of creating and protecting value.

APPENDIX A. COSO's Updated Enterprise Risk Management Framework

The 2017 COSO ERM Framework consists of the five interrelated components of enterprise risk management. The five components are supported by 20 principles which identify fundamental concepts associated with each component and describe things that organizations would do under each component. This principles-based Framework provides guidance that allows organizations to develop and implement specific ERM action steps that best fit their organization's governance structure and culture consistent with the 20 principles. Organizations can also use the Framework to assess the adequacy and completeness of their enterprise risk management processes and that those processes are present and functioning in an integrated manner.

More detailed information on enterprise risk management, the COSO Enterprise Risk Management Framework and related practices and activities is available through the COSO website at COSO.org.

Figure7. The COSO Risk Management Components and Principles

Governance & Culture

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

Strategy & Objective-Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Performance

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

Review & Revision

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues improvement in Enterprise Risk Management

Information, Communication, & Reporting

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

Source: COSO ERM Framework, 2017

APPENDIX B. Where to Start: Draft Action Plan for an ERM Initiative

Outlined below is an initial, draft high-level action plan to implement the ERM approach described in this thought paper. The draft action plan highlights key events and actions that organizations should consider when starting an ERM effort. The draft is not intended to be used as a complete action plan but rather as a starting point that would be tailored and expanded prior to use. The draft action plan adds details to the action plan detailed in section II above. This draft action plan reflects useful information and is a practical basis for developing an organization-specific action plan.

1. Seek Board and Senior Management Involvement and Oversight

a. Set an agenda item for the board and senior management to discuss ERM
   i. Clarify and establish the overall objective of ERM to enhance the performance of the organization not just to identify risks
   ii. The relationship of ERM to achieving the organization's business objectives and strategies
   iii. The need to integrate ERM with the organization's strategy and performance processes
   iv. The expected benefits from an integrated ERM approach
   v. The expected change in the culture of the organization
b. Agree on high-level objectives and expectations regarding a risk management initiative
c. Understand the process to communicate and set the tone and expectations of ERM for the organization
   i. Setting and communicating the "tone at the top" is an essential element of establishing and achieving the desired change in the culture
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 leader of the risk management initiative
   i. In-depth knowledge of the organization's overall business objectives and strategies
   ii. Does not have to be a newly created CRO (Chief Risk Officer) position or full-time equivalent; it often is led by an existing member of management who takes on the role of ERM leader in additional to their current responsibilities
   iii. Use existing management resources

b. Set authority, objectives and expectations for the leader
c. Allocate appropriate resources to enable success
   i. Review Principle 5: Attracts, Develops, and Retains Capable Individuals, of the COSO ERM framework, for additional ideas and information regarding human capital

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 level and stature
   ii. "C-suite" representation
   iii. Business unit management
   iv. Strategic planning head
c. Agree on objectives for the working group
   i. Build ERM using incremental steps
   ii. Define some sought-after benefits to evaluate each step
   iii. Establish reporting process for management and the board

4. Inventory the Existing Risk Management Practices of the Organization

a. Identify and inventory existing risk practices, whether formal or informal
b. Consider how those practices fit or align with the organization's strategy setting and performance review process
c. Identify gaps and opportunities to further integrate the organization's strategy and risk processes
   i. Identify initial opportunities for further integration
d. Develop specific action steps to close gaps and implement opportunities

5. Conduct an Initial Assessment of Key Strategies and Related Strategic Risks.

a. Start by identifying the organization's key strategies and business objectives
b. Discuss and identify the events/risks that could impair the success of each core strategy
c. Consider risk factors beyond just probability and impact, for example, organizations have considered factors such as;
   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 management responses
   iii. Identify opportunities to enhance risk management responses
e. Develop action plans to enhance risk management practices related to the risks identified
   i. Identify actions to implement the opportunities identified above
   ii. Establish target dates and responsibilities
   iii. Develop process to monitor and track implementation

6. Develop Consolidated Action Plan and Communicate to Board and Management

a. Consolidate the action plans developed in the above steps
b. Prioritize actions and allocate resources across the actions
c. Assign responsibility for actions and monitoring
d. Present consolidated initial action plan to Board and management
e. Develop communications plan to communicate risk initiative and results across the organization

7. Develop/Enhance Risk Reporting

a. Assess adequacy and effectiveness of existing risk reporting
a. Consider integration of risk reporting with existing performance reporting
b. Develop new reporting formats
   i. Consider extensive use of graphics and colors to indicate risk trending and significance
   ii. Consider developing a risk "dashboard" for the board
   iii. Consider use of strategy maps or other visuals to link strategies to risks
c. Develop process for periodic reporting of emerging risks
d. Assess effectiveness of new reporting with stakeholders and revise as appropriate

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

a. Conduct a critical assessment of the accomplishments of the working group
   i. Identify benefits to date
   ii. Assess the level of integration with strategic planning and performance measurement processes
   iii. Assess impact on the culture of the organization
b. Revisit the COSO ERM Framework and identify next risk management processes for enhancement
   i. Consider actions related to establishing or articulating the risk appetite of the organization
   ii. Consider organizational or strategic changes in the organization

APPENDIX B. (cont.)

iii. Consider how the ERM process can be enhanced to identify opportunities not just threats
iv. Identify tangible steps for a new action plan including benefits sought and target dates
v. Review with executive management and the board

c. Implement with appropriate resources and support
d. Schedule sessions for updating or further educating directors and executive management
e. Assess progress and benefits of ERM initiative against objectives and communicate to target audiences
f. Continue organization-wide communication process to build risk culture

APPENDIX C. Frequently Asked ERM Questions

- **Is *Enterprise Risk Management – Integrating with Strategy and Performance* applicable only for large, public companies?**
  No, the principles contained in *Enterprise Risk Management – Integrating with Strategy and Performance* are applicable to all organizations, including not-for-profit and governmental organizations regardless of size. All entities face uncertainty in the pursuit of value or in the case of not-for-profits or governmental agencies the achievement of their missions. Risk then affects any organization's ability to achieve its strategies and business objectives. Accordingly, while some small and mid-size organizations may implement the principles of enterprise risk management differently than large organizations, the principles remain applicable to every entity because every entity faces risks.

- **What is the real benefit to our organization of an investment in ERM?**
  The real benefit of an investment in integrated ERM is that it helps organizations enhance their performance and increase the likelihood that they can be successful in achieving their strategies and business objectives. The benefit is much broader than simply identifying risks or providing a supporting staff activity. By integrating ERM into the organization's strategy setting and performance processes, boards and management can optimize outcomes and ultimately enhance value by better understanding and managing the risks that are present in any strategies. This enhanced process of ERM enables boards and management to make better informed decisions about both their strategies and potential risks to those strategies.

- **What is the role of ERM related to the strategies of the organization?**
  ERM does not create the strategies of the organization; however, when integrated with the strategy setting process it provides management and the board with risk information that should be considered as they evaluate alternative strategies and finally select its strategies. This risk information enhances the board's decision-making process. ERM then provides an ongoing process to assist management and the board with monitoring and managing those events that could impair the ability of the organization to be successful with its chosen strategies. The role of ERM therefore is integral to both the decision-making process for the selection of strategies and the ongoing monitoring of the strategies be implemented.

- **Does the organization need to make a significant investment to achieve any benefit from ERM?**
  No, many organizations have found that they can begin to realize benefits from ERM by implementing simple steps based on the ERM principles with their existing resources and risk management activities. For example, organizations already have processes in place for strategy setting and budgeting. By taking simple steps to integrate some basic risk management actions into those existing processes, organizations can begin to achieve benefits. As a principles-based framework, the COSO ERM framework provides a structure that organizations can use to develop and implement basic risk management practices appropriate for their organization.

- **Does an implementation need to form a separate, functional ERM unit?**
  No, ERM as defined by COSO is the "culture, capabilities, and practices, integrated with strategy-setting and its performance that organizations rely on to manage risk in creating, preserving, and realizing value." It is more of a process than a functional group. Many organizations have started ERM using management committees or working groups of their existing personnel. These groups can take the lead in developing the organization's initial approach to ERM. It is critical to the success of these groups or committees to have the right people on the committee, especially those who understand fully the key strategies of the organization and the related risks. This means that the groups must include key business unit leaders, not just staff personnel. Typically, these groups also must have a strong, credible leader, such as the head of strategic planning or chief financial officer, and support from top management.

APPENDIX C. (cont.)

- **If the organization already manages risks on a day-to-day basis, what's wrong with just continuing those informal risk management processes?**
  While most organizations currently have some informal risk management processes, those processes are often lacking transparency and frequently not aligned or integrated to the strategies and business objectives of the organization. As a result, the organization is not gaining the full benefits of an enterprise-wide risk management process. The lack of transparency is a major short-fall as increasingly, boards and other stakeholders, such as rating agencies, are looking for ERM processes that are transparent, repeatable and aligned with the overall business and strategies of the organization. Also, informal risk activities are most likely to be performed on an ad hoc basis and done separately and, therefore, lacking consistency and enterprise-wide communications and knowledge sharing. This can create "silos of knowledge" which can delay decision making and jeopardize the organization's ability to make timely decisions or react to urgent events.

- **Does an organization need to appoint a "Chief Risk Officer" or have dedicated ERM staffing?**
  No, many organizations have started ERM using existing staff and appointed one of their key, senior level personnel as the leader of their initiative. For example, given the linkage between strategies and risk, some organizations have used their Head of Strategic Planning to begin their ERM project. Organizations have also used their CFO, General Counsel, Chief Operating Office, or Chief Audit Executive in that role. Regardless of title, the person selected to lead the ERM initiative must have the stature, authority, business knowledge, and senior leadership skills to effectively serve as the catalyst for the ERM initiative. As their ERM processes mature, some organizations reach a point where they believe they need a dedicated Chief Risk Officer; however, organizations do not need to create a CRO position to get started nor does a more mature ERM process necessarily require a dedicated CRO.

- **Do I need to use technology or quantitative models or metrics to start ERM?**
  No, the use of technology or quantitative models and metrics may ultimately be useful in a more robust ERM environment, but they are not necessary to launch an ERM effort. Consistent with the ERM principles, many organizations have started with ERM process by undertaking an assessment of the top risks related to their organization's strategies and then reviewing how those risks are managed and monitored. Depending of 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 financial and market risks; however, the identification and quantification of all risks is not the goal. Management and the board need to develop a solid understanding of how an ERM effort can be integrated into their business processes to enhance the overall performance of the organization.

- **Must an organization implement the entire COSO ERM framework to achieve any benefit from ERM?**
  No, as noted in this thought paper, many organizations are taking a step-by-step approach to ERM to facilitate building their understanding and experience with the components and principles of ERM. This approach allows the board and management to come up a learning curve about ERM and to achieve specific benefits at each step of the process. Some organizations may use some form of maturity model under this approach. While this step-by-step approach to ERM has 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 realizing the full benefits that it could achieve from a fully integrated ERM process.

- **How to know if ERM is making a difference?**
  ERM is making a difference when management and the board feel that, as a result of their ERM activities, they are making better informed decisions that ultimately result in enhanced performance. Also, that the board and management believe they are more aware of the risks facing the organization because of transparency created by the ERM process. This difference is more than just the absence of a negative event, but it is a positive, cultural change in how the organization has integrated the consideration of risk into its planning and performance processes. Indications that are reflective of this culture change can be actions such as seeing a discussion of risk naturally flowing from any discussion of possible strategies or the identification of possible risk events that would not have occurred without the ERM processes being in place. Other indications are the presence of strategic planning staff on risk committees or even heading the risk committee and discussions of possible opportunities to enhance performance by taking additional levels of risk that are within the organization's risk appetite.

APPENDIX D. Examples of the Relationship between Strategies and Risks

In Step 4, of Section III, *Initial Action Steps and Objectives,* this paper discusses identifying the core strategies of the organization and then assessing the related strategic risks. In that section, two related models are presented to aid in these assessments: Figure 4, The Return Driven Strategy Model, displays a set of tenets and three foundational elements, while Figure 5, The Strategic Risk Management Model, displays various strategic risks related to each of the tenets and foundational elements. These frameworks are used in tandem first to identify core strategies and then to identify the risks corresponding to the specific tenets.

Displayed below are two examples of how these models can be used. In each example, core strategies are considered for the strategy tenet and then possible strategic risks corresponding to the strategies identified. Consistent with the updated COSO ERM Framework, the sequence is strategies first then the related risks. Such a sequence is important and ensures that organizations are not just trying to identify risks but are focused on those risks most critical to the success of their key business strategies.

It is also important to view these models as aids to foster discussion, not as simple templates to be used or filled out. The identification of strategy and related risks is a thought process and a mindset. The models should be used to prompt analyses and in-depth discussions on the strategies and their related risks.

Examples of the Linkage between Strategy Tenets and Strategic Risks	
Partner Deliberately	**Partnering Risk**
• Consider a wide range of potential partnerships and be creative in developing new types of relationships that can support the competencies of the firm • Deliberately choose partners based on an assessment of the Genuine Assets brought by each partner and how that can help the firm to build unique offerings as the competency tenets require • Create performance measures that bring incentives to the partner	• Significant failure in the supply chain by a strategic partner • Damage to reputation and value because of ethical, legal or regulatory matters of a strategic partner - Cyber-risk through a strategic partner a particular concern right now. • Losses due to fraud on the part of a strategic partner • Loss of intellectual property or proprietary processes

Source: Adapted from Frigo, Mark L. and Richard J. Anderson, *Strategic Risk Management for Directors and Management Teams* (2011). Used with permission.

Examples of the Linkage between Strategy Tenets and Strategic Risks	
Engage Employees and Others	**Employee Engagement Risk**
• Realize the existence of the complete end-to-end employee life cycle, including firm awareness and recruiting at one end and alumni or even customer status at the other end of the cycle • Create incentives, compensation plans, and other offerings throughout the entire employee life cycle that will create *employee engagement* toward the firm's goals • Create performance measures that are aligned with the achievement of the higher tenets	• Loss of investment and capital because of the lack of an adequate workforce to execute the strategy or staff growth plans. • Losses in revenue or opportunity losses because of; - Inability to attract and retain talent - Inability to attract a global workforce - Inability to provide the right incentive

Source: Adapted from Frigo, Mark L. and Richard J. Anderson, *Strategic Risk Management for Directors and Management Teams* (2011). Used with permission.

SELECTED REFERENCES

Anderson, Richard J., and Mark L. Frigo. "What Should Directors Ask about Risk Management?" Strategic Finance (April 2012).

Anderson, Richard J., and Mark L. Frigo. *Assessing and Managing Strategic Risks: What, Why, How for Internal Auditors*. Institute of Internal Auditors Foundation (2017).

Beasley, Mark S., and Mark L. Frigo. "Strategic Risk Management: Creating and Protecting Value." Strategic Finance (May 2007).

Beasley, Mark, et al. "Working Hand in Hand: Balanced Scorecards and Enterprise Risk Management." Strategic Finance (March 2006).

Frigo, Mark L. and Richard J. Anderson. "Strategic Risk Assessment: A First Step for Risk Management and Governance." Strategic Finance (December 2009).

Frigo, Mark L. and Richard J. Anderson. *Strategic Risk Management: A Primer for Directors and Management Teams.* (2011).

Frigo, Mark L. and Joel Litman. *DRIVEN: Business Strategy, Human Actions and the Creation of Wealth*. Strategy & Execution, 2007.

Frigo, Mark L. Driven Strategy: Creating Greater Long-Term Sustainable Value, Stanford University Press: Palo Alto, California (forthcoming).

Frigo, Mark L. and Mark Beasley. "ERM and Its Role in Strategic Planning and Strategy Execution." In *Enterprise Risk Management* Fraser and Simkins, Editors. John Wiley & Sons, 2009. Forward by Robert Kaplan, Harvard Business School.

Frigo, Mark L., Hans Læssøe, and Venkat Ramaswamy. "Strategic Risk Management in the Co-Creative Enterprise." Journal of Enterprise Risk Management (2015).

Sobel, Paul J. "*Who Owns Risk*". *The Global Internal Audit Common Body of Knowledge*. The Institute of Internal Auditors Research Foundation. 2015. p. 11.

ABOUT THE AUTHORS

Richard J. Anderson is a Clinical Professor of Risk Management at DePaul University and a retired Managing Partner of PricewaterhouseCoopers. With PwC he consulted with major financial institutions on internal audit, risk management, and audit committee activities. Prior to PwC, he served as head of internal audit and credit review for a global bank. A frequent speaker and author, with DePaul he is researching, writing and lecturing on strategic risk management and internal audit. He co-founded the Strategic Risk Management Lab at DePaul where he teaches graduate seminar courses on Strategic Risk Management. He is also active in the Institute of Internal Auditors where he has served on international committees and co-chaired the IIA's *CBOK Global Internal Audit Study*, the largest study ever conducted of the internal audit profession. He has received the IIA's highest award, the Bradford Cadmus Memorial Award, for his contributions to the global internal audit profession. A pioneer in the development of the new body of knowledge in Strategic Risk Management, his research and thought leadership on Strategic Risk Management have been published by COSO, IIA, IMA, The Conference Board and other leading organizations.

Dr. Mark L. Frigo is Distinguished Professor Emeritus and co-founder and Director Emeritus of the Center for Strategy, Execution and Valuation and the Strategic Risk Management Lab in the Kellstadt Graduate School of Business at DePaul University in Chicago where he directs ongoing research on strategy and strategic risk management at high performance companies. He served as the Ledger & Quill Distinguished Professor of Strategy & Leadership and Ezerski Endowed Chair of Strategy & Leadership in the School of Accountancy and MIS in the Driehaus College of Business at DePaul and he is the recipient of the *Via Sapientiae* Award, DePaul University's highest award for faculty. Author of seven books and over 125 articles, his work is published in leading business journals including *Harvard Business Review*. Dr. Frigo is a Certified Public Accountant (CPA), a Certified Management Accountant (CMA), a Chartered Global Management Accountant (CGMA) and holds a Ph.D. in Econometrics. A pioneer in the development of the new body of knowledge in Strategic Risk Management, his research and thought leadership on Strategic Risk Management have been published by Harvard Business Press, COSO, RIMS, AICPA, IIA, ICAEW, CIMA, IMA, The Conference Board and other leading organizations. He serves as an advisor to senior executive teams and boards of directors of Fortune 500 companies, and international organizations including United Nations agencies in Geneva, Switzerland and has presented keynotes and executive education programs throughout North America, Europe and Asia-Pacific.

ABOUT COSO

Originally formed in 1985, COSO is a joint initiative of five private sector organizations and is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management (ERM), internal control, and fraud deterrence. COSO's supporting organizations are the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), the Institute of Management Accountants (IMA), and The Institute of Internal Auditors (IIA).

ABOUT THE STRATEGIC RISK MANAGEMENT LAB

The Strategic Risk Management Lab 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.

The Strategic Risk Management Lab
Driehaus College of Business
Kellstadt Graduate School of Business
DePaul University

COSO

Committee of Sponsoring Organizations
of the Treadway Commission

coso.org

CREATING AND PROTECTING VALUE

UNDERSTANDING AND IMPLEMENTING ENTERPRISE RISK MANAGEMENT

COSO

Committee of Sponsoring Organizations of the Treadway Commission

coso.org