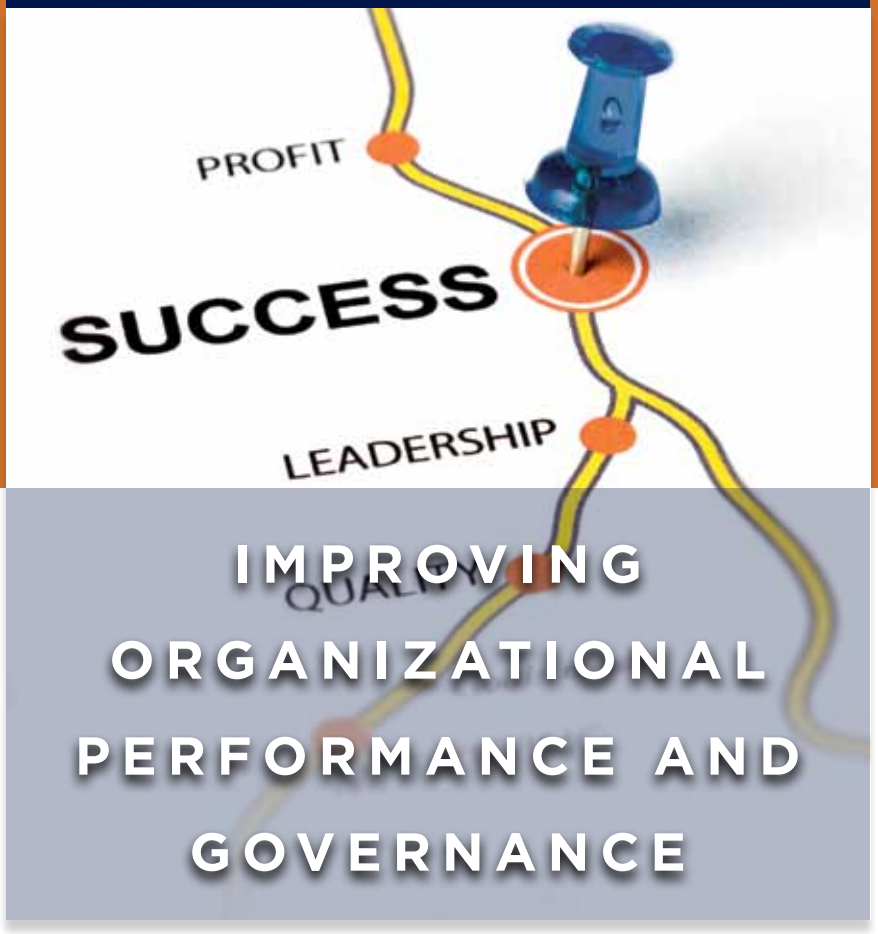
COSO

Committee of Sponsoring Organizations of the Treadway Commission

Governance and Operational Performance



IMPROVING ORGANIZATIONAL PERFORMANCE AND GOVERNANCE

How the COSO Frameworks Can Help

By

protiviti®

James DeLoach

ima® The Association of Accountants and Financial Professionals in Business

Jeff Thomson CMA, CAE

Authors

Protiviti

James DeLoach
Managing Director

IMA (Institute of Management Accountants)

Jeff Thomson, CMA, CAE
President and CEO

Acknowledgements

The authors wish to thank David Landsittel, Larry Rittenberg, James Pajakowski and Jay Thompson for their valued input and ideas in framing this paper and Michael McGarry and Darci Lowe for their assistance with the necessary research. In addition, they wish to thank the COSO Board for its support of this project.

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)

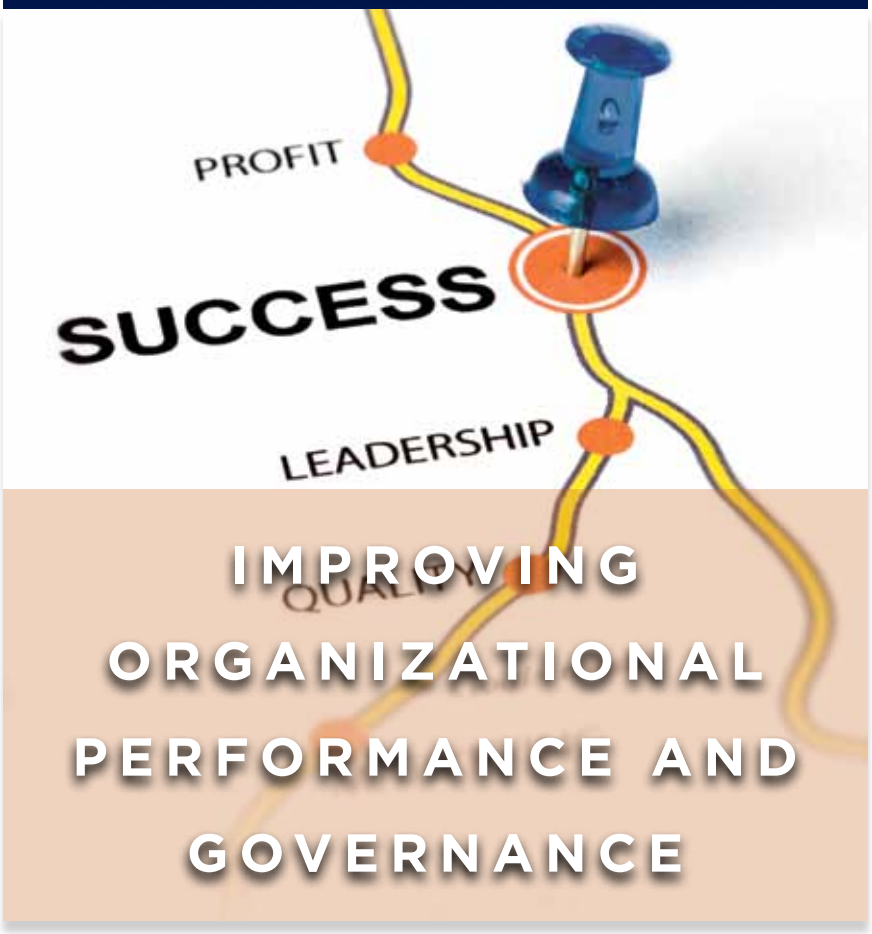
The Institute of Management Accountants (IMA)

The Institute of Internal Auditors (IIA)

COSO
Committee of Sponsoring Organizations of the Treadway Commission

www.coso.org

Governance and Operational Performance



IMPROVING ORGANIZATIONAL PERFORMANCE AND GOVERNANCE

How the COSO Frameworks Can Help

Research Commissioned by

COSO

Committee of Sponsoring Organizations of the Treadway Commission

February 2014

1234567890 PIP 198765432

Contents

Introduction

The mission of the Committee of Sponsoring Organizations (COSO) reads, in part, "to improve organizational performance and governance." Since their inception, COSO's Enterprise Risk Management — Integrated Framework[1] and Internal Control — Integrated Framework[2] (collectively referred to as "the COSO frameworks") were both intended to provide guidance for management on how to implement and evaluate effective enterprise risk management (ERM) and internal control processes, leading to the improvement of management and governance processes. When applied effectively, the frameworks' concepts contribute to the end result of improving organizational performance and governance in significant ways.

Our purpose in writing this paper is to relate the COSO frameworks to an overall business model and describe how the key elements of each framework contribute to an organization's long-term success. COSO's fundamental premise is that good risk management and internal control are necessary for long term success of all organizations and we seek to support that premise by articulating how the frameworks contribute to improving organizational performance and governance. We do not seek to compare the two frameworks directly, as each framework includes a comparative analysis in an appendix.[3] As we proceed, we intend to draw from the COSO frameworks, as appropriate, with a presumption that the reader has an understanding of the frameworks. In addition, this paper applies to any organization choosing to use either or both of the COSO frameworks.

[1] *Enterprise Risk Management – Integrated Framework*, Committee of Sponsoring Organizations, September 2004. Available at www.coso.org.

[2] *Internal Control – Integrated Framework*, Committee of Sponsoring Organizations, May 2013. Available at www.coso.org.

[3] See Appendix C of *Enterprise Risk Management – Integrated Framework and* Appendix G of *Internal Control – Integrated Framework*.

Executive Summary

This paper describes the COSO frameworks in the context of a fairly standard leadership umbrella for governing and managing a successful organization. The frameworks are intended to be integrated within the governance and management processes to establish accountability for ERM and internal control. Either framework can be applied with positive results, i.e., companies can implement the internal control framework without implementing the ERM framework. The governance concepts included in both frameworks,[4] are vital to their effective application by organizations.

Within the context of its mission, an organization is designed to accomplish objectives. It is presumed that the organization's leaders can articulate its objectives, develop strategies to achieve those objectives, identify the risks to achieving those objectives and then mitigate those risks in delivering the strategy. The ERM framework is based on objective setting and the identification and mitigation or acceptance of risks to the achievement of objectives. The internal control framework is designed to control risks to the achievement of objectives by reducing them to acceptable levels. Thus, each of the frameworks is inextricably tied into the operation of a business through the achievement of objectives. ERM is applied in the strategy-setting process while internal control is applied to address many of the risks identified in strategy setting.

The ERM framework asserts that well-designed and effectively operating enterprise risk management can provide reasonable assurance to management and the board of directors regarding achievement of an entity's objectives. Likewise, the internal control framework asserts that internal control provides reasonable assurance to entities that they can achieve important objectives and sustain and improve performance. The "reasonable assurance" concept embodied in both frameworks reflects two notions. First, uncertainty and risk relate to the future, which cannot be precisely predicted. Second, risks to the achievement of objectives have been reduced to an acceptable level.

In general, ERM involves those elements of the governance and management process that enable management to make informed risk-based decisions. Informed risk responses, including the internal controls that accompany them, are designed to reduce the risk associated with achieving organizational objectives to be within the organization's risk appetite.[5] Therefore, ERM/internal control and the objective of achieving the organization's strategic goals are mutually dependent.

[4] Specifically, governance concepts are included in the internal environment component in *Enterprise Risk Management – Integrated Framework* and control environment component in *Internal Control – Integrated Framework.*

[5] For more information on the development of risk appetite, see the COSO thought paper *Enterprise Risk Management – Understanding and Communicating Risk Appetite*, Dr. Larry Rittenberg and Frank Martens, January 2012. Available at www.coso.org.

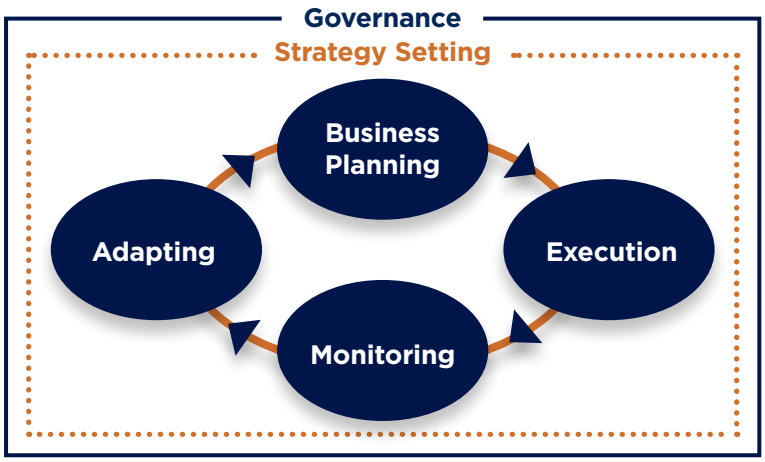
A Contextual Business Model

We have chosen a simple but holistic view of governance and management processes (see **Figure 1**) to illustrate the integration of the COSO frameworks into the core activities of a business. This general business model encompasses most management processes.

The model begins with **governance**, which starts with the organization's vision and mission and consists of oversight from the board of directors of the enterprise's planning and operations. Also included are the activities of executive management in ensuring the effectiveness of strategy setting and the organization's other management processes.

Next is **strategy setting**, which is the process by which executive management (and, depending on the size of the enterprise, the board of directors) articulates a high-level plan for achieving one or more goals consistent with the organization's mission. Together, the two elements of governance and strategy setting provide direction to the enterprise and clearly have a place in ensuring the organization's success in meeting the demands and expectations of stakeholders.

Figure 1: Contextual Business Model



Inside the business model are four elements based on the time-honored concept of the "Plan, Do, Check, Act Cycle."[6] We have described these elements as **business planning**, **execution**, **monitoring** and **adapting**. These elements are essentially what operating management does in managing the execution of the strategy approved by executive management and the board.

The six attributes of the contextual business model introduced above are further described below:

- **Governance** is the act or process of providing oversight or authoritative direction or control. One author defines it as the allocation of power among the board, management and shareholders.[7] It is often applied to describing what the board of directors and executive management does in providing direction and oversight to the organization's affairs. Corporate governance is typically the domain of the board of directors and refers to the framework of rules and practices by which a board oversees strategy setting and the management of the organization. Effective governance ensures accountability, fairness and transparency in the organization's relationships with its various stakeholders, e.g., shareholders, lenders, customers, suppliers, employees, governments, regulators and the communities in which it operates.
- **Strategy setting** sets the context for business planning by providing management's high level plan for what the organization seeks to achieve over its selected strategic planning horizon, including its overall direction, environmental scan, differentiating capabilities and the infrastructure needed to make the differentiating capabilities a reality in the marketplace. Strategy is often presented in the form of overall goals, initiatives and tactics. This is but one point of view regarding strategy setting and there are others.

[6] An iterative four-step management method used in business for the control and continuous improvement of processes and products, the "Plan-Do-Check-Act cycle" was made popular by Dr. W. Edwards Deming, a pioneer in modern quality control.

[7] Richard M. Steinberg, *Governance, Risk Management and Compliance* (New York: John Wiley & Sons, Inc., 2011, 2.

The management cycle for delivering the strategy is a continuing, ongoing process. To illustrate the elements of this dynamic process:

- **Business planning** formally articulates specific goals or roadmaps on how operating management will contribute to achieving the overall strategic objectives, explains why those objectives are achievable and provides an enabling process for deploying and executing the corporate strategy across the organization within the specified planning horizon. Business planning:
  - Links the traditional processes of strategic planning, risk mitigation, budgeting, forecasting, and resource allocation;
  - Breaks down the corporate strategy into achievable plans, with financial and operational targets, including key performance indicators (KPIs) and key risk indicators (KRIs), to establish management accountability for results;[8] and
  - Aligns business objectives, key metrics, plans and budgets across the organization down to the level of greatest achievability and accountability, and engages the appropriate managers with the resources needed to implement strategic objectives (typically resulting in an operational plan).
- **Execution** consists of the organization's core operations in place to design, build and operate the processes that make the business plan work and deliver expected performance in accordance with the values and strategy of the organization.
- **Monitoring** consists of the activities established by management to review and oversee execution of the organization's operations against the overall strategic plan, including the level of acceptable risk. Monitoring activities consider both (a) performance metrics that demonstrate progress towards achievement of business objectives and long-term strategic goals and (b) risk metrics to ensure risk remains at acceptable levels. They are focused both externally and internally to scan for economic, competitor, regulatory and other developments and trends.
- **Adapting** describes the organizational processes by which issues identified through monitoring activities as requiring management follow-up and corrective action are translated into implementable changes to the corporate strategy, business plan and/or execution tactics (including risk responses and /or internal controls). Adapting is important when considering the organization's resiliency and agility that is so vital to success in a rapidly changing business environment. It includes improvements in processes to close performance gaps related to stakeholder expectations and competitors as well as "mid-course corrections" in response to changes in the external and internal environment that alter assumptions underlying the strategy and/or business plan.

The above six elements provide an illustrative structure for demonstrating how the COSO frameworks contribute value to the overall governance and management processes of an organization.

To that end, the ERM framework defines enterprise risk management as:

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

The internal control framework also defines internal control as "a process, effected by an entity's board of directors, management, and other personnel," but more specifically states that it is:

> Designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.

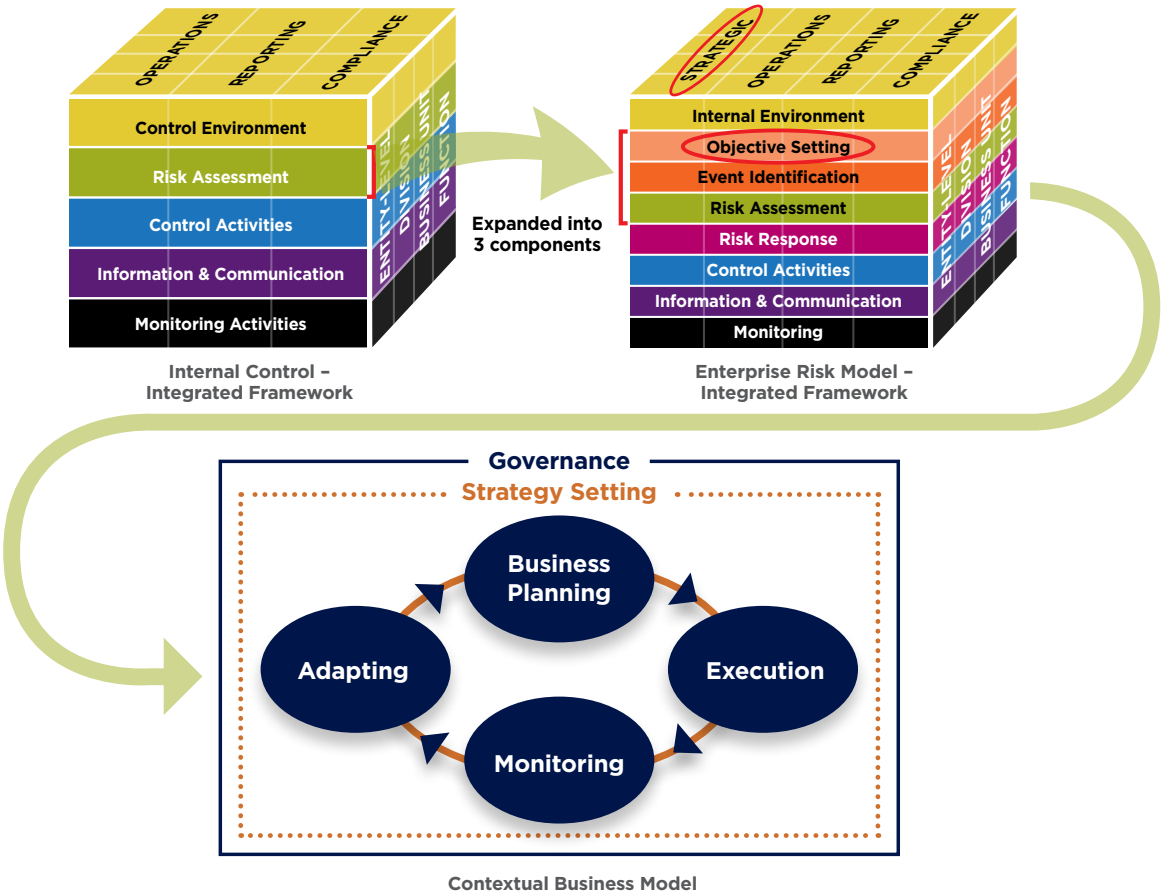
[8] For more information on the development of key risk indicators (KRIs), see the COSO thought paper *Developing Key Risk Indicators to Strengthen Enterprise Risk Management: How Key Risk Indicators Can Sharpen Focus on Emerging Risk*, by Mark S. Beasley, Bruce C. Branson and Bonnie V. Hancock, December 2010. Available at www.coso.org.

[9] *Enterprise Risk Management – Integrated Framework,* 4.

[10] *Internal Control – Integrated Framework, 33* (Digital Edition).

Figure 2 illustrates how internal control is an integral part of ERM, while ERM is an integral part of the business model. As a subset of the contextual business model and broader than internal control, ERM elaborates on internal control and focuses more directly on risk. ERM focuses on strategic objectives and internal control does not, because achievement of strategic objectives is subject to external events not always within the organization's control. ERM encompasses objective setting, whereas internal control is applied to established objectives to provide reasonable assurance they are achieved. The ERM framework is broader than, and encompasses, internal control because it deals with alternative risk responses (risk avoidance, acceptance, sharing and reduction), while the internal control framework deals primarily with risk reduction.

Figure 2: Relationship of ERM and Internal Control to Contextual Business Model



In viewing the interrelationships in **Figure 2**, ERM and internal control contribute value to, and are inextricably integrated as part of, the overall governance and management process. To illustrate using the components of the ERM framework:

- The internal environment and objectives setting components permeate governance, strategy setting and business planning.
- The event identification, risk assessment and risk response components are applied in strategy setting and business planning, the control activities component in execution and the monitoring component in monitoring.
- The event identification, risk assessment and monitoring components are also applied in adapting.
- The information and communication component is pervasive throughout, affecting all six elements of the business model.

As a subset of ERM, internal control also contributes value to the organization. The sections that follow will discuss more specifically how the frameworks contribute value to each of the six elements of our contextual business model. In addition, the appendix to this paper provides excerpts of commentary from both frameworks regarding their value contributed.

Why the Frameworks Are Important to Governance

Robust enough to be applied independently on their own, the two COSO frameworks have a common purpose — to help the enterprise achieve its objectives and to optimize the inevitable tension between the enterprise's value creation and value protection activities. Therefore, both facilitate and support the governance process when implemented effectively.

The board of directors has a separate and distinct role from executive management in governing the organization. The board approves strategic decisions, establishes appropriate boundaries, oversees execution and ensures accountability, fairness and transparency. Executive management aligns strategy, processes, people, reporting and technology to accomplish the organization's mission in accordance with its established values. An important aspect of the delineation of responsibilities between the board and management is the setting of boundaries, which provide a broad context for balancing the organization's objectives and performance goals for creating enterprise value with the policies, processes and control systems deemed appropriate to preserve enterprise value.

Why Boundaries Are Important

A board's communications to a chief executive set performance expectations to define success from a stakeholder perspective. When a board sets strategic boundaries around the decisions a chief executive may make, that direction implies that anything the board does not expressly prohibit or does not define as being outside its limits of acceptability is permissible so long as it is a reasonable interpretation of the board's intentions. Rather than tell the chief executive what to do or how to run the business, the board provides direction as to what not to do through what one author referred to as "a constructive ring fence around behavior."[11]

Clearly defined boundaries provide a framework for managing the inevitable tension between the enterprise's value creation and value protection activities. They frame the "strategic sandbox" within which management may play in executing the business model, providing a means by which:

- The board and the chief executive can agree on what the organization should not do, providing a context for what it can do, and
- The chief executive can provide leadership to focus the organization from a strategic, operational and financial standpoint.

Boundaries have strategic importance as they reduce the risk of strategic drift leading to a lack of focus in managing the organization's risk profile. They also allow for faster decision-making and help to avoid wasted effort on initiatives that are not likely to achieve approval because they are off-strategy.

The dynamic of boundaries is evident in a recent report on the priorities of directors in providing oversight for their companies. Asked to indicate the top three challenges facing their boards, the participating directors noted growth strategy, economic climate and risk strategy as their top three concerns. More importantly, a general theme that emerged in the study as a key challenge for boards was "balancing growth strategies and risk." This theme is likely a priority because of directors' concern over uncertainty in the external environment. Indeed, an unbridled focus on growth may not be such a good idea in uncertain times, and that is one reason why a robust ERM process is important.[12]

[11] David R. Koenig, *Governance Reimagined: Organizational Design, Risk and Value Creation* (New York: John Wiley & Sons, Inc., 2012, 184.

[12] *The Eversheds Board Report: The Effective Board,* Eversheds LLP, 2013. Available at www.eversheds.com/global/en/what/publications/board-report2/index.page.

The internal environment of the ERM framework, the control environment of the internal control framework and the information and communications component of both frameworks provide positive contributions to the governance process, as described in our illustrative contextual business model. ERM instills within the organization a discipline around managing risk in the context of managing the business such that discussions of opportunities and risks and how they are managed are virtually inseparable from each other. Three ways ERM makes this contribution are discussed below:

Risk Management Philosophy

One of the elements of the ERM internal environment is the risk management philosophy, which is the set of shared beliefs and attitudes characterizing how the entity considers risk in everything it does, from strategy development and implementation to its day-to-day activities. It is a communication from executive management to the board of directors and to the organization at large regarding the importance of understanding and managing risk in the context of the organization's strategy and business plan. For example, it:

- Reiterates the organization's purpose, mission and strategic priorities to provide a context for identifying and managing risk.
- Reaffirms executive management's commitment to ethical and responsible business behavior, an open and transparent environment and a strong focus on risk management in the context of executing the organization's strategy and business plan.
- Defines what ERM is, its related objectives, why it is important and what it means to the organization's personnel.
- Reiterates key assertions in the organization's risk appetite statement around acceptable and unacceptable risks and the parameters within which the organization's business model will be conducted.
- Delineates the roles and responsibilities of management and the board and describes the process for articulating the organization's risk appetite in the context of its strategy and sustaining a risk appetite dialogue with the board.

Every organization has a risk management philosophy; it's just a question of (1) how well developed it is, (2) whether it is explicit or implicit and (3) how its personnel understand and embrace it as part of the organization's culture. Conversations and open communications about risks, their interrelationships and their impacts on business objectives are a sign of a positive, proactive risk management culture.

Risk Appetite

Another element of the ERM internal environment, risk appetite reflects the enterprise's risk management philosophy, and in turn influences the entity's culture and operating style. It is considered in strategy setting, consistent with the view that a disciplined approach around protecting enterprise value should be integrated with the aspirational objectives established through the strategy-setting process. The risk appetite statement frames the risks the organization should accept, the risks it should avoid and the strategic, financial and operating parameters within which the organization should operate.

Because risk appetite sets boundaries around executing the business model, it is fundamental to any governance process that seeks to appropriately balance the organization's activities around value creation and value protection. These boundaries are not intended to be excessively rigid. They must be flexible enough to respond to changes and opportunities in the business environment while at the same time being viewed as an authoritative benchmark that has been vetted and approved by the board. If risk appetite is constantly altered to accommodate every emerging opportunity or meet quarterly forecasts at all costs, it loses its value as a disciplinary rudder for navigating through unpredictable and rough waters.

Control Environment

The ERM framework articulates other elements of the internal environment that are important to the organization's governance process. These additional elements are similar in substance to the five principles comprising the control environment, as described by the internal control framework:

1) The organization demonstrates a commitment to integrity and ethical values.

2) The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control

3) Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

4) The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

5) The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

The above principles strengthen the governance process by laying a vital foundation for effective risk management and internal control. The core of any business is its people — their individual attributes, including integrity, ethical values and competence — and the environment in which they operate. The above principles strengthen that core.

In summary, applying either or both COSO frameworks will strengthen the impact of the governance process on the organization's risk culture and, ultimately, the achievement of its business objectives as agreed upon by executive management and the board.

Why the Frameworks Are Important to Strategy Setting and Business Planning

The ERM framework is applied in strategy setting and addresses strategic objectives. Internal control is more tactical, directed to execution of the business and to reducing risk to the achievement of objectives. Therefore, ERM has more of an impact on strategy setting and business planning. That said, the COSO internal control framework makes it clear that business objectives, including risk tolerances, are a precondition for designing and evaluating the system of internal control.

Elements from the objective setting, event identification, risk assessment and risk response components of the ERM framework have a direct impact on strategy setting and business planning. The positive contributions of these COSO ERM components are further discussed below:

Objective-setting Component

In objective setting, strategic and related objectives are established and risk appetite and risk tolerances are considered. For example, risk is inherent in any decision to expand into new markets, introduce new products, acquire a different line of business, build a new plant and invest in uncharted research and development activities. Every evaluation of risk ultimately leads to a decision to accept or reject the risk based on an assessment of whether it is desirable or undesirable.

A major factor in this discussion is the organization's risk appetite, as discussed previously. In determining risk appetite, management should undertake three steps: (1) develop it, (2) communicate it and (3) monitor and update it. These three steps should be undertaken with the board's review and concurrence. Considerations influencing risk appetite are illustrated in **Figure 3**.[13]

Figure 3: Overview of Considerations Affecting Risk Appetite

[13] *Enterprise Risk Management: Understanding and Communicating Risk Appetite*, Dr. Larry Rittenberg and Frank Martens, 1, 4. Available at www.coso.org.

Risks an organization determines it is willing to accept tend to be foundational in nature, meaning they are inherent in the current business model and related strategy for creating enterprise value. These risks are likely the ones that "pay off" through effective execution of the strategy, rewarding the company with satisfactory returns that compensate for the downside exposures it has accepted. To illustrate, global organizations accepting the myriad challenges of operating in diverse countries, with distinctively different cultures, in pursuit of new markets are an example of acceptable risk. Organizations choosing to accept these risks typically do so based upon a satisfactory risk/reward balance and a determination by management that the organization can execute the strategy effectively while managing the related risks. A choice to make significant investments to expand into or acquire a new line of business outside the company's current core business is yet another example, as long as execution risk is reduced to an acceptable level.

The risk appetite statement contributes discipline in undertaking new risks as it drives the appropriate dialogue between executive management and the board, serving as a guidepost when considering emerging opportunities and risks. Our experience is that only a minority of directors are satisfied with their board's discussions with management regarding acceptable levels of risk.

A well-articulated risk appetite statement that is communicated effectively to operating units can provide clarity and focus to the business planning process and surface the need for dialogue as market conditions change significantly. A result of objective setting, risk tolerances can be an effective tool in this regard if they are sufficiently granular and expressed in such a way that they can be: (a) mapped into the same metrics the organization uses to measure success in achieving an objective, (b) applied to all categories of objectives (strategic, operations, reporting and compliance) and (c) implemented by operating personnel throughout the organization. Because risk tolerances are defined within the context of objectives, risk appetite and performance metrics, they set the boundaries of acceptable performance variability.[14]

Event Identification Component

The strategy setting process sets forth strategic aspirations and objectives, differentiating capabilities and the infrastructure needed to deliver those capabilities to the marketplace. When formulating strategy and developing business plans, management is confronted with uncertainty. Whether or when an event will occur or the extent of its impact on the organization should it occur creates uncertainty over the planning horizon. This is where the event identification component of the ERM framework becomes highly relevant.

Management initially considers a range of potential events as part of the organization's environment scanning and intelligence gathering processes. These events may stem from both internal and external sources — without necessarily focusing on whether their impact is positive or negative. In this way, both risks and opportunities arise for consideration during the planning process. Event identification supports strategy setting and business planning in many ways by considering key influencing factors, deploying appropriate event identification techniques, analyzing event interdependencies and identifying signs of relevant change.

Risk Assessment Component

An organization's strategic direction and its ability to execute on that direction are both fundamental to the risks it undertakes. Risks are implicit in any organization's strategy. Accordingly, risk assessment should be an integral part of the strategy-setting process. Strategic and other risks should be supported or rationalized by management's determination that the upside potential from assuming those risks is sufficient and/or the organization can manage the risks effectively.

[14] Ibid.11.

Another reason why the risk assessment component is applicable to strategy setting and business planning is because strategic objectives are included within the scope of the ERM framework. The risk assessment process considers inherent and residual risk and applies such factors as likelihood of occurrence, severity of impact, velocity of impact, persistence of impact and response readiness to analyze and prioritize risks. Risk assessment techniques include contrarian analysis, value chain analysis, scenario analysis, at-risk frameworks (e.g., value, earnings, cash flow or capital) and other quantitative and qualitative approaches to evaluating risk. Furthermore, risk assessment considers relationships between seemingly unrelated events to develop thematic insights on potential long-term trends, strategic possibilities and operational exposures.

Risk Response Component

The risk response component is the capstone of applying the ERM framework to strategy setting and business planning processes. For many risks, appropriate response options are obvious and well accepted, e.g., financial and compliance risks. For other risks, available options might not be readily apparent and/or are subject to management discretion, e.g., strategic and operational risks. Risk response entails an evaluation and selection of possible alternatives for reducing risk to an acceptable level. A portfolio view of risk may be gained by focusing on major risks or event categories across business units, or on risk for the company as a whole, using such metrics as risk-adjusted capital or capital at risk. The ERM framework states that such composite measures are particularly useful when measuring risk against objectives stated in terms of earnings, growth, and other performance measures, sometimes in relation to allocated or available capital.

While the ERM framework deals with alternative risk responses (risk avoidance, acceptance, sharing and reduction), the internal control framework deals primarily with risk reduction. Given that management cannot control external events, ERM focuses on strategic objectives while internal control provides an important risk response option in executing the strategy and business plan. The concepts of focusing on a portfolio view of risk and aggregating the effect of risk responses across the organization are not contemplated in the internal control framework.

Why the Frameworks Are Important to Execution

The control activities and information and communication components in either COSO framework support the execution of the strategy and business plan insofar as the achievement of objectives is concerned. The respective contribution of each of these two components in both the ERM and internal control frameworks is discussed below:

Control Activities Component

These activities consist of actions of people to implement established policies, directly or through application of technology, to help ensure that management's risk responses are carried out. Control activities can be categorized based on the nature of the organization's objectives to which they relate e.g., operations, reporting, and compliance. Once selected and developed, they support the implementation of risk responses and are deployed through policies and procedures.

Whether preventive or detective, automated or manual or applied at the entity or process level, control activities contribute significant value to the organization if designed and operating effectively. They are vital to successful execution of the business model because they are intended to mitigate the risks of relevant objectives not being achieved. In effect, they serve as mechanisms for managing the achievement of objectives.

Information and Communication Component

In either COSO framework, information is vital to all aspects of the organization and informs decisions made with respect to formulating strategy, developing business plans and executing those plans. Both financial and non-financial information is obtained from internal and external sources and is relevant to multiple business objectives.

For example, the internal control framework states that information systems provide information to appropriate personnel so that they can carry out their respective operating, reporting and compliance responsibilities. Specifically, Principle 13 states that "the organization obtains or generates and uses relevant, quality information to support the functioning of other components of internal control."

Inherent in information systems in either COSO framework, communication takes place in a broader sense, dealing with expectations, responsibilities of individuals and groups, and other important matters relevant to execution. Both information and communication are vital to execution at all levels of an organization to identify, assess and respond to risk on an ongoing basis and ensure the achievement of objectives.

Why the Frameworks Are Important to Monitoring

The monitoring component of both frameworks plays an important role in an organization because it provides the discipline to improve risk management capabilities and internal control continuously in a changing business environment. According to both COSO frameworks:

- Business conditions — both internal and external — change and as the business environment changes, new risks emerge and risk profiles change. The ability to identify changes in known risks or the emergence of new risks on a timely basis is vital to the success of an organization in these dynamic times. New product introductions, acquisition of a different line of business, personnel turnover, new or substantially modified processes or systems and changes in strategic assumptions or direction alter risk profiles.

- Due to emerging risks and changes to existing risks, organizational objectives may change, risk responses that were once effective may become irrelevant or obsolete and/or control activities may become less effective or may no longer be performed.

- As the environment and conditions change, management needs to determine whether the functioning of ERM or internal control continues to be effective.

Monitoring assesses progress towards attaining objectives and evaluates performance of processes, risk responses and internal control. It identifies new issues, risks and problems as well as deficiencies in ERM and/or internal control. According to both frameworks:

- Monitoring can be applied either through ongoing activities or separate evaluations, e.g., Principle 16 of the internal control framework.

- The greater the degree and effectiveness of ongoing monitoring, the less there is a need for separate evaluations.

- The frequency of separate evaluations necessary for management to obtain reasonable assurance about the effectiveness of ERM or internal control is a matter of judgment. In making that determination, management must give consideration to the extent, nature and speed of change occurring over time and the associated risks, the competence and experience of the personnel implementing risk responses and related controls, and the results and effectiveness of ongoing monitoring.

- Some combination of ongoing monitoring and separate evaluations are often applied to ensure that ERM and/or internal control maintain their effectiveness over time.

- The ERM framework emphasizes timely evaluation, communication and remediation of deficiencies in ERM while the internal control framework does the same for internal control, e.g., Principle 17 of the internal control framework states that "the organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate."

Why the Frameworks Are Important to Adapting

Former heavyweight boxing champion, Mike Tyson, once said that everyone has a plan until they get punched in the mouth. Adapting is a game every organization must play to be successful in a rapidly changing business environment. From the printing press to the steam engine driven industrial revolution to the Internet, disruptive change is inevitable. Over the last 15 years, we have seen such disruptive displacements as chemical photography being displaced by digital photography, light bulbs by light-emitting diodes, mechanical calculators by digital calculators, and VHS tapes by DVDs. To illustrate, as we look forward, consider the potential effects of:

- Disruptive technological developments, such as:
  - Technology innovation by consolidation to help users through friendlier, more intelligent devices
  - Increased mobile connectivity, bigger/thinner TVs, 3D displays and speech recognition on consumer behavior and the workplace
  - Hybrids on the profitability of the automotive industry
  - Bandwidth availability on markets for personal messaging, telemedicine, telecommuting, real hi-definition entertainment and distance learning
- Disruptive market forces, such as:
  - Significant demographic changes arising from aging populations and concentrations of people in resource-stressed regions and intensifying fiscal pressures on the viability of affected regions
  - Political and social instability in emerging economies or economies emerging from political instability (such as in the Middle East)
  - Highly volatile commodity markets on manufacturing and product pricing, e.g., sudden spikes in the cost of, or limits on the availability of, critical commodities
  - Introduction of new far-reaching legislation, such as the Dodd-Frank Act or Affordable Healthcare Act in the United States
- Emerging new and/or unexpected threats, such as:
  - Cyber-security issues on critical infrastructure, brand image and reputation
  - More catastrophic natural disasters like the Japanese tsunami or terrorist events like 9/11

The point is that organizations must "plan" for disruption and build and refine their radar systems to measure and be on the alert for changes in key risk indicators (leading indicators) versus rely solely on key performance indicators (which are often lagging and retrospective in nature). Looking forward will enable an organization's culture to support an experimental and adaptable mindset.

Adapting is all about positioning companies to quickly recognize a unique opportunity or risk and use that knowledge to evaluate their options and seize the initiative either before anyone else or along with other organizations that likewise recognize the significance of what's developing in the marketplace. Early movers have the advantage of time, with more decision-making options before market shifts invalidate critical assumptions underlying the strategy. Failing to adapt can be fatal in today's complex and dynamic business environment.

Organizational resiliency is the ability and discipline to act decisively on revisions to strategic and business plans in response to changing market realities. This capability begins to emerge as organizations integrate strategic plans, risk management and performance management and create improved transparency into the enterprise's operations to measure current performance and anticipate future trends. With the emphasis on identifying and reacting to change, the event identification, risk assessment, information and communication, and monitoring components of the ERM framework contribute insights that can support an entity's efforts to become adaptive. Likewise, the risk assessment, information and communication, and monitoring components of the internal control framework can support an entity's efforts to become adaptive in disruptive times. For example, Principle 9 supporting the risk assessment component states that "the organization identifies and assesses changes that could significantly impact the system of internal control."

Is Your Organization Resilient? – Some Questions to Consider

Boards and executive management of companies that aspire to be resilient in the face of change would do well to consider the following questions in light of their existing structure, operations and circumstances:

- Are executive management and the board knowledgeable of the critical assumptions underlying the corporate strategy? Does the organization proactively identify, source and mitigate the risks inherent in the strategy?
- Is there a process for identifying emerging risks? For example:
  - Are effective scenario analysis capabilities in place to evaluate situations arising from an event or combination of events that could invalidate one or more of the organization's critical strategic assumptions?
  - Is the company's competitive intelligence aligned with the external drivers that could invalidate the most important strategic assumptions? Does an organization only have in place a competitive analysis capability which looks backwards to assess the past, or one that looks forward with a market-sensing capability to anticipate emerging risks and opportunities?
  - Is information around strategic assumptions and insights gained from scenario analyses and intelligence gathering distilled on a timely basis and reported to decision makers and the board of directors to provide an effective early warning capability?
- Is the board satisfied that management pays attention to the warning signs and gives timely consideration to formulating and evaluating the organization's options?
- Is the company able to act timely on emerging opportunities and risks as well as changes in the business environment affecting the viability of its strategy and business model? If not, why not?

Key Takeaways and Observations

Figures 4 and **5** illustrate how the components of the COSO frameworks tie into the contextual business model:

Figure 4: Relationship of ERM Components to Contextual Business Model

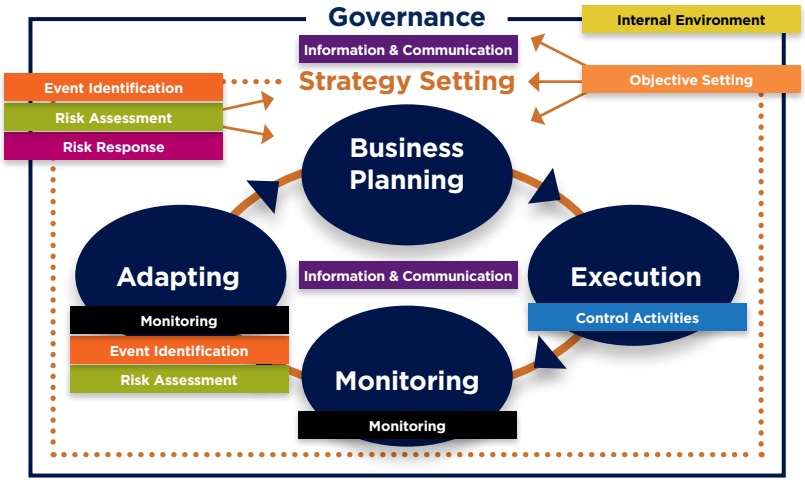
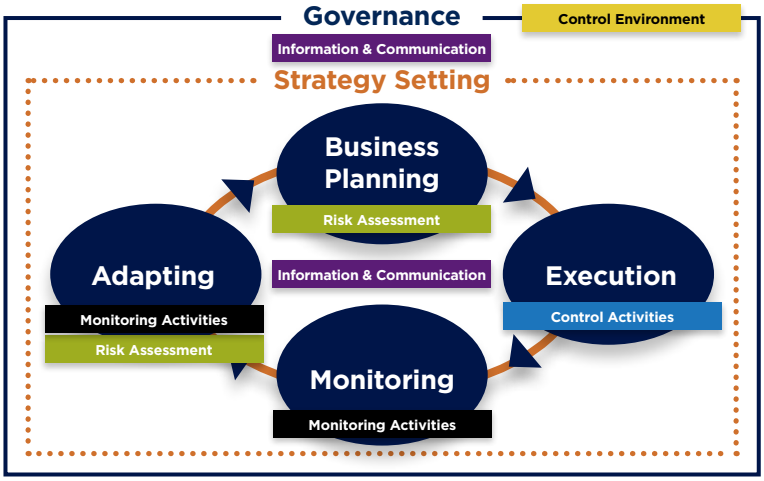


Figure 5: Relationship of Internal Control Components to Contextual Business Model



Using our contextual business model to illustrate the appropriate linkages, we have demonstrated how both COSO frameworks contribute value to helping organizations succeed. We see a number of major takeaways and observations around successful implementation of the frameworks, with emphasis on their positive impact in an organization striving to achieve its strategic goals and objectives within an effective governance structure and in a changing business environment:

- Regarding the implementation of the frameworks themselves:
  - The COSO frameworks are fundamental to the success of any organization in serving its mission and achieving its strategic goals within an effective governance context. The COSO frameworks affect how risks are managed, how the culture encourages appropriate behavior, the quality of managerial decisions, and the resiliency of the enterprise to identify and react to change — all for the purpose of ensuring objectives are achieved.
  - While the COSO frameworks are intended to be flexible in application, both must involve the board, both are focused on the standard of "providing reasonable assurance that objectives are met" and both seek to reduce risk to an acceptable level. The ERM framework includes strategic objectives within its scope; it is applied in strategy setting and deploys risk appetite as a tool for managing the level of enterprise risk.

  - Objective setting is a component of ERM, whereas objectives are a precondition for designing and evaluating the system of internal control.

  - Both frameworks have their purpose. From an application standpoint, the ERM framework is more strategic while the internal control framework is more tactical. While the best overall organizational results are achieved when both frameworks are implemented together, each framework is robust and can be implemented without the other.

  - As we've demonstrated, there is some significant overlay between ERM and internal control. After all, internal control is a subset of ERM. That said, both frameworks address separable purposes and objectives. Full implementation of internal control does not eliminate the benefits of implementing ERM.

  - The process of identifying, prioritizing and responding to risks on an enterprise-wide basis is a significant source of insight, even if objectives are implicit. However, when objectives are explicitly articulated or more objectives are considered in the scope of implementing either COSO framework, the quality of the insight increases.

- Organizations should look for ways to apply either framework or both frameworks on a broader basis to improve governance, risk management and internal control. For example, although the original COSO internal control framework supported objectives in the areas of operations, compliance and financial reporting, the passage in the United States of the Sarbanes-Oxley legislation led to an almost exclusive focus on the framework's application to internal control over external financial reporting. Thus, there are opportunities to broaden the focus of the framework to consider operations, compliance and other reporting objectives.

- Managing the tension between creating enterprise value and protecting enterprise value is the most difficult task of risk management and internal control. For that task to function effectively when a crucial decision-making moment arises, directors and executive management must be committed to making it work. Alignment of the governance, risk management and internal control processes toward striking the appropriate balance is crucial in this regard. The objective is to balance the entrepreneurial activities and the control activities of the organization so that neither one is too disproportionately strong relative to the other. Both frameworks contribute to optimizing the natural tension between value creation and value protection within the contextual business model we have described.

- Some tips on using the frameworks: Following are some specific suggestions for using the frameworks to better enable an organization to achieve its strategic goals and objectives in the context of an effective governance structure:

  - In applying ERM, ensure it is integrated with such core management processes as strategy setting and business planning. Recognize that ERM cannot stand alone and will only operate effectively if integrated with the ongoing management processes across the enterprise.

  - Work on improving the risk appetite dialogue between executive management and the board of directors and on cascading risk tolerances downward into the organization in appropriate areas to supplement the performance management process.

  - Strengthen the organization's risk culture by focusing on improving either the internal environment component of the ERM framework or the control environment component of the internal control framework (or both). Consider the use of surveys, focus groups and other assessment techniques to evaluate the current state of the organization's risk culture to identify opportunities for improvement and take appropriate steps to act on those opportunities.

  - Improve the process of identifying, prioritizing and responding to risks by (1) structuring the risk assessment approach according to the characteristics of the risks being assessed (e.g., applying appropriate analytical frameworks germane to strategic, operational, financial and compliance risks and considering factors other than likelihood and impact) and (2) assigning ownership of the risk assessment process to the managers who are best positioned to act on the assessment results (usually, these managers are the unit leaders and process owners whose activities create the risk). These two concepts facilitate the integration of risk management with core management processes.

  - Take a fresh look at internal control to identify ways to strengthen the internal control structure, specifically using the 17 principles of the updated internal control framework (May, 2013).

  - Use this paper's contextual business model, or a variation thereof, for integrating the use of both frameworks in the organization efficiently and effectively.

Closing Remarks

Whether applied individually or together, ERM and internal control in the context of enhancing the broader leadership umbrella for governing and managing an organization are critical for optimal achievement of mission and execution of strategy. The major takeaways and observations around successful implementation of the frameworks summarized above provide insights as to how the COSO frameworks support the achievement of strategic goals and objectives in the context of an effective governance structure, as well as suggestions for enhancing the effectiveness of their implementation. This paper has demonstrated that the COSO ERM and internal control frameworks contribute value to the six attributes of the illustrative contextual business model it introduces — the governance, strategy setting, business planning, execution, monitoring and adapting processes of an organization.

Every organization exists to be successful in achieving its vision, mission, values and strategy. The COSO frameworks, whether applied singularly or together, enable directors, executive management and internal and external stakeholders to communicate more effectively through a common language. This enhanced risk-focused communication facilitates discussion about issues germane to improving governance, assessing risk, designing risk responses and control activities, facilitating relevant information and communication flows, and monitoring ERM and internal control performance. There is significant value to this enhanced dialogue and sharper focus on managing risk in disruptive and challenging times, and it can lead to strengthening organizations in significant ways as they serve their mission, stakeholders and society.

Appendix — What the Frameworks Say

The COSO Frameworks provide perspectives on how ERM and internal control contribute to an organization's management and governance processes. To that end, this Appendix includes specific commentary sourced from each of the COSO frameworks. The commentary included herein is intended to be illustrative and does not purport to provide a comprehensive summary of all relevant commentary included in the frameworks.

Enterprise Risk Management — Integrated Framework

The ERM framework discusses its components in the context of what management does in running a business. The framework asserts that management judgments, with appropriate board oversight, guide the implementation of strategy, risk management and control. The following examples illustrate:[15]

- Ensuring there is an appropriate process for objective setting is a critical component of ERM. The particular objectives selected by management are a management decision that influences the implementation of ERM. Different managers may set different objectives in similar circumstances.

- Responding to risks, based on an appropriate risk assessment, is an integral part of ERM. The specific risk responses selected by management and the associated allocation of entity resources in effecting those risk responses influences the implementation of ERM significantly. Although there are potentially several ways to respond to risk, there is a presumption under the framework that the selection of specific risk responses should be sufficient to enable the organization to accomplish its objectives within its risk appetite or risk tolerances.

- Establishing and executing control activities to help ensure the risk responses management selects to reduce risk are effectively carried out is an important part of ERM. The particular control activities chosen by management influences the implementation of ERM. Although there are potentially several ways to design control activities to reduce risk, there is a presumption that the selection of specific control activities should be sufficient to enable the organization to accomplish its objectives within established risk tolerances.

The COSO framework emphasizes that ERM involves those elements of the management process that enable management to make informed risk-based decisions. Strategy, risk management and control are all affected by management decisions and board decisions. Therefore, one organization's risk appetite may differ from that of another organization. Strategy and risk management are related as every organization undertakes risks in pursuing its objectives (including the risk of not doing anything). Therefore, it is imperative that management decisions be formulated to select the appropriate risk responses and internal controls that will achieve the organization's objectives within the parameters of its risk appetite set in its strategy-setting process.[16]

Given the above, an entity's "internal environment" must be aligned with management's strategic process and the board's oversight. According to the ERM framework, the internal environment component encompasses the tone of an organization, and establishes the context for how risk is viewed and addressed by an entity's personnel, including the risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate. The operating environment is framed by the board's oversight and the organization's commitment to competence, organizational structure, assignment of authority and accountability, and human resource standards. These elements of the internal environment provide the foundation for the remaining components of ERM and have a significant effect on management decision-making.[17]

[15] *Enterprise Risk Management – Integrated Framework*, page 14.

[16] Ibid.

[17] Ibid., page 22.

According to the ERM framework, ERM encompasses the following:[18]

- **Aligning risk appetite and strategy –** Management considers the entity's risk appetite in evaluating strategic alternatives, setting related objectives and developing mechanisms to manage related risks.
- **Enhancing risk response decisions –** ERM provides a framework of alternative risk responses — risk avoidance, reduction, sharing, and acceptance — to address identified risks. The richness of the alternative responses enables management to make decisions in selecting the appropriate response to address a given risk or group of related risks. The actual decision-making process in selecting the appropriate risk response is a management and governance function.
- **Reducing operational surprises and losses –** By enhancing capability to identify potential events and establish responses, the organization reduces the risk of unwanted surprises and their associated costs or losses.
- **Identifying and managing multiple and cross-enterprise risks –** Every enterprise faces myriad risks affecting different parts of the organization. ERM facilitates understanding the interrelated impacts and formulating an effective response, including integrated responses to multiple risks (for example, related risks identified at point of sale and in the back office).
- **Seizing opportunities –** By considering a full range of potential events, management is positioned to identify and proactively pursue opportunities that are consistent with the strategy. Risk management becomes more than a means to limit costs or losses; it also helps give visibility to unforeseen opportunities to sustain profitable growth.
- **Improving deployment of capital –** Obtaining robust risk information allows management to effectively assess overall capital needs and enhance capital allocation.

The above capabilities inherent in ERM help management achieve the entity's performance and profitability targets and prevent loss of resources.

The framework makes it clear that risk appetite is a vital aspect of ERM. It is the amount of risk — on a broad level — an entity is willing to accept in pursuit of value. It reflects the entity's risk management philosophy, as formulated by management and approved by the board, and in turn influences the entity's culture and operating style. For example, a company with a higher risk appetite may be willing to allocate a large portion of its capital to such high-risk areas as newly emerging markets. In contrast, a company with a low risk appetite might limit its short-term risk of large losses of capital by investing only in mature, stable markets. Directly related to an entity's strategy, risk appetite is considered in strategy setting, as different strategies expose an entity to different risks. When considering resource allocation decisions, management considers risk appetite when aligning the organization, its people, and its processes, and designing infrastructure necessary to effectively respond to and monitor its risks.[19]

The framework further notes that risk tolerances relate to the entity's objectives. A risk tolerance is the acceptable level of variation relative to achievement of a specific objective, and is best measured in the same units as those used to measure the related objective. For example, from an operational perspective, an objective may be to improve service quality by improving both reliability of service delivery and responsiveness to the customer. Given that customer satisfaction is the metric used, the risk tolerance might be expressed as "the percentage of customers who are dissatisfied with our services must not exceed three percent."

[18] Ibid., pages 2-3.

[19] For more information on risk appetite, see *Enterprise Risk Management – Understanding and Communicating Risk Appetite,* by Rittenberg and Martens. Available at www.coso.org.

In setting risk tolerance, management considers the relative importance of the related objective and aligns risk tolerances with risk appetite. Operating within risk tolerances helps ensure that the entity remains within its risk appetite and, in turn, that the entity will achieve its objectives.[20]

The ERM framework states that human judgment is vital to making decisions on the appropriate way to respond to risk and establish controls, considering the relative costs and benefits. The framework provides structure to facilitate the exercise of judgment, which results in better decisions.

The potential for breakdowns due to human failures, circumvention of controls through collusion, and/or management override of established risk responses presents opportunities to design risk responses, control activities and monitoring processes that would minimize the possibility of losses due to problems these limitations could present.[21]

Internal Control — Integrated Framework

A system of internal control allows management to stay focused on the organization's pursuit of its operations and financial performance goals, while operating within the confines of relevant laws and minimizing surprises along the way. Internal control enables an organization to deal more effectively with changing economic and competitive environments, leadership, priorities, and evolving business models.[22]

Internal control is an integral part of ERM, as the components of the ERM framework encompass the components of the internal control framework. While the ERM framework encompasses internal control, thereby forming a more robust conceptualization and tool for management, COSO designed the internal control framework so that it could be implemented without the organization having a formal ERM process in place throughout the organization. Given the relatively low level of ERM adoption around the world, a robust internal control framework with risk management as a foundational component is a reasonable alternative, although COSO recommends adoption of an ERM process for optimal business outcomes. Much like everything else, a systematic and disciplined approach makes the process much more robust, and thereby much more likely to succeed, which increases the likelihood of achieving strategic success.[23]

An effective internal control system provides reasonable assurance that objectives can be achieved. It reduces the risk of not achieving an entity objective to an acceptable level. To that end, internal control plays a vital role in ensuring an organization's success. Following are illustrative examples for each component of internal control:

Control Environment:[24]

- An organization that establishes and maintains a strong control environment positions itself to be more resilient in the face of internal and external pressures. It does this by demonstrating behaviors consistent with the organization's commitment to integrity and ethical values; adequate oversight processes and structures; organizational design that enables the achievement of the entity's objectives with appropriate assignment of authority and responsibility; a high degree of competence; and a strong sense of accountability for the achievement of objectives.

Risk Assessment:[25]

- As part of the process of identifying and assessing risks, an organization may also identify opportunities, which are the possibility that an event will occur and positively affect the achievement of objectives. These opportunities are important to capture and to communicate to the objective-setting processes.

[20] *Enterprise Risk Management – Integrated Framework*, page 8. See also *Enterprise Risk Management – Understanding and Communicating Risk Appetite*, pages 11-14, for a practical discussion of risk tolerances.

[21] Ibid., page 84.

[22] Ibid., page 1.

[23] Ibid., page 13.

[24] Ibid., page 64 (Digital Edition).

[25] Ibid., page 94 (Digital Edition).

- Risk affects an entity's ability to succeed, compete within its industry, maintain its financial strength and positive reputation, and maintain the overall quality of its products, services, and people. There is no practical way to reduce risk to zero. Indeed, the decision to be in business incurs risk. Management must determine how much risk is to be prudently accepted, strive to maintain risk within these levels, and understand how much tolerance it has for exceeding its target risk levels.

Control Activities:[26]

- Control activities serve as mechanisms for managing the achievement of an entity's objectives and are very much a part of the processes by which an entity strives to achieve those objectives. They do not exist simply for their own sake or because having them is the right or proper thing to do.

- Control activities are those actions that help ensure that responses to assessed risks, as well as other management directives, such as establishing standards of conduct in the control environment, are carried out properly and in a timely manner.

Information and Communication:[27]

- Information is necessary for the entity to carry out internal control responsibilities to support the achievement of its objectives. Management obtains or generates and uses relevant and quality information from both internal and external sources to support the functioning of internal control.

- Internal communication is the means by which information is disseminated throughout the organization, flowing up, down, and across the entity. External communication enables inbound communication of relevant external information and provides information to external parties in response to requirements and expectations.

- The information and communication component supports the functioning of all components of internal control. In combination with the other components, information and communication supports the achievement of the entity's objectives, including objectives relevant to internal and external reporting. Controls within Information and Communication support the organization's ability to use the right information within the system of internal control and to carry out internal control responsibilities.

Monitoring:[28]

- An entity's system of internal control will often change. The entity's objectives and the components of internal control may also change over time. Also, procedures may become less effective or obsolete, may no longer be deployed in the manner in which they were selected or developed, or may be deemed insufficient to support the achievement of the new or updated objectives. Monitoring activities are selected, developed, and performed to ascertain whether each component continues to be present and functioning or if change is needed. Monitoring activities provide valuable input for management to use when determining whether the system of internal control continues to be relevant and is able to address new risks.

- Management considers the rate at which an entity or the entity's industry is anticipated to change. An entity in an industry that is quickly changing may need to have more frequent separate evaluations and may reconsider the mix of ongoing and separate evaluations during the period of change. Usually, some combination of ongoing and separate evaluations will validate whether or not the components of internal control remain present and functioning.

[26] Ibid., pages 126,127 (Digital Edition).

[27] Ibid., pages 146, 147 (Digital Edition).

[28] Ibid., pages 166 and 169 (Digital Edition).

The COSO framework points out that there are aspects of the management process that are not part of internal control but can affect the organization's performance in achieving its objectives. For example, an entity's weak governance processes for selecting, developing, and evaluating board members may limit its ability to provide appropriate oversight of internal control. Similarly, an entity with ineffective strategy-setting and objective-setting processes may be challenged in its ability to achieve poorly specified, unrealistic, or unsuitable objectives.[29]

The COSO framework points out that internal control can only be as effective as the people responsible for its functioning. This assertion points to the importance of the governance process in implementing an effective internal control system. The internal control framework states:[30]

> A system of internal control can be circumvented if people collude. Further, if management is able to override controls, the entire system may fail. Even though an entity's system of internal control should be designed to prevent and detect collusion, human error, and management override, an effective system of internal control can experience a failure.

The opportunity is to design internal controls to mitigate these risks.

[29] Ibid., page 180 (Digital Edition).

[30] Ibid., page 37 (Digital Edition).

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 Institute of Internal Auditors (IIA), the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), and the Institute of Management Accountants (IMA).

About the Authors

Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit. Through its network of more than 70 offices in over 20 countries, Protiviti has served more than 35 percent of FORTUNE 1000® and FORTUNE Global 500® companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies.

Jim DeLoach, a Managing Director with global consulting firm Protiviti, has 35 years of experience in governance, risk and compliance matters. He has advised hundreds of global companies about governance and risk management and served for eight years on the COSO Advisory Council. DeLoach has authored more than 250 thought leadership pieces on various aspects of governance and risk. In 2011, he was named to *Consulting* magazine's Top 25 Consultants list. In 2012 and 2013, he was named to the NACD Directorship 100 list.

IMA

IMA®, the association of accountants and financial professionals in business, is one of the largest and most respected associations focused exclusively on advancing the management accounting profession. Globally, IMA supports the profession through research, the CMA® (Certified Management Accountant) program, continuing education, networking, and advocacy of the highest ethical business practices. IMA has a global network of more than 65,000 members in 120 countries and 300 professional and student chapter communities. IMA provides localized services through its offices in Montvale, N.J., USA; Zurich, Switzerland; Dubai, UAE; and Beijing, China. For more information about IMA, please visit www.imanet.org.

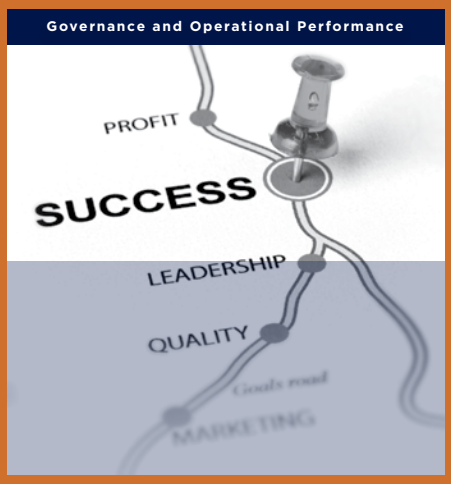
Jeff Thomson, CMA, CAE is president and CEO of the Institute of Management Accountants. Jeff served on the COSO Board for over five years, is a recognized thought leader in performance management, and, formerly was the CFO of a multi-billion dollar multi-national telecommunications organization.

Governance and Operational Performance

COSO

Committee of Sponsoring Organizations
of the Treadway Commission

www.coso.org



IMPROVING ORGANIZATIONAL PERFORMANCE AND GOVERNANCE

COSO

Committee of Sponsoring Organizations of the Treadway Commission

www.coso.org