Effective risk management and internal control (RM/IC) is an important driver of business performance and one of the best defenses against business failure. Highly successful organizations know how to take advantage of opportunities and counter threats, thereby continually improving their overall performance. Others could leverage RM/IC more effectively than they do today.

Until recently, many organizations were overly focused on a financial reporting controls-based monitoring framework. But the global financial crisis highlighted that many of the most impactful risks stem from external circumstances. Moving forward, risk management and control systems should take a wider perspective since organizations exist as part of an open system of dynamic variables.

As a management accountant, most likely you’re in a position of cross-functional leadership to plan, implement, execute, evaluate, and improve RM/IC for your organization. Therefore, you should be aware of related developments and emerging trends as well as recently developed or revised frameworks and guidance that might help you.
In this article we highlight several of the common pitfalls to effective RM/IC that many organizations experience and define and discuss current thinking on risk management and internal control. Then we identify the building blocks of effective RM/IC and offer a brief overview of some useful RM/IC frameworks and guidance by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), the International Organization for Standardization (ISO), and the International Federation of Accountants (IFAC). Finally, we challenge you with a “call to action” regarding the important role you can play in implementing good RM/IC.

The Pitfalls—Setting the Scene
Several factors caused the recent global financial crisis. Ethical flaws and regulatory overload, leading to legalistic compliance, played a role. So did ineffective governance, risk management, and internal control. For some organizations, governance, risk management, and internal control existed in name only, not in spirit or in practice. For others, risk and control systems were focused too narrowly on financial reporting controls only. Indeed, there has been and continues to be an overwhelming load of bad RM/IC practices (see Table 1).

Some entities have mistakenly viewed risk management and internal control as objectives in their own right rather than as tools to be leveraged in setting and achieving overall strategies, goals, and objectives. Others have tried to “bolt on” stand-alone RM/IC systems or implement off-the-shelf risk management applications rather than integrate risk management into existing processes and customize controls to address their unique nature and risks. At some organizations, RM/IC processes remain static, becoming out-of-date as the entity continues to evolve. Management often views RM/IC activities as only adding cost instead of creating results and sustainable value. And many focus their RM/IC activities just on threats, but they should focus on opportunities as well.

This article is based on our presentation “Leveraging Effective Risk Management and Internal Control for Your Organization” at the 2013 IMA® Annual Conference & Exposition. It describes the main features of the most important risk management and internal control guidelines, identifies the main pitfalls to risk management and internal control, and provides strategies regarding how to avoid or overcome these pitfalls and otherwise gain insight into improving risk management and internal control in your organization.

A follow-up presentation titled “Upgrading Risk Management and Internal Control in Your Organization” is scheduled for this year’s Annual Conference & Exposition in Minneapolis, Minn. This hands-on session will provide a case study and practical examples on how you can upgrade your organization’s risk management and internal control, leveraging the implementation guidance of the popular ISO 31000 Risk Management standard and the recently revised COSO Internal Control—Integrated Framework.

The safest place for a ship is in its harbor, but that isn’t what ships are made for. They are made to transport people and goods to other locations, and that involves risk. The same concept holds for organizations.

Setting and Achieving Objectives
Before discussing risk management and internal control, we must address setting and achieving objectives—the ultimate goal of organizations. Risk management and internal control contribute to achieving those objectives. Every organization should have a defined mission and/or vision, whether altruistic (e.g., to eradicate world hunger and/or disease) or pragmatic (e.g., to become the number one supplier of a given product globally). Through its strategic planning process and with board oversight, management must determine how to achieve its vision. Specifically, management must make choices regarding how the organization will seek to create, preserve, and realize value for its stakeholders. The objectives and their subsequent execution, whether at the entity level or deeper within the organization, are a reflection of these choices.

These objectives can be strategic in nature or can fall into several other categories, including operational,
reporting, and/or compliance, and they should be linked at different levels of the organization. An entity-level objective, for example, could be to develop a presence in high-growth markets such as Brazil, China, or India. The organization’s Latin America division could then include objectives (and subobjectives as needed) such as conducting market research regarding Brazilian consumer needs, initiating export sales to a Brazilian test market, and identifying potential Brazilian business partners in its plan. Finally, the market research manager for the division could have personal objectives to conduct specific Brazilian consumer research during the upcoming year. It’s in setting and achieving your organization’s objectives that risk comes about.

What Is Risk?
When working toward its objectives, every organization faces a wide range of uncertain internal and external factors. The effect of this uncertainty on the organization’s objectives is called risk, which can be either positive, representing opportunity, or negative, representing a threat. For example, the safest place for a ship is in its harbor, but that isn’t what ships are made for. They are made to transport people and goods to other locations, and that involves risk. The same concept holds for organizations. Risk should always be assessed in light of setting and achieving your organization’s objectives. If there are no objectives, there is no risk.

And Risk Management?
While establishing its objectives, an organization should consider the wide range of uncertain internal and external factors—the risks—that may affect the achievement of these objectives. Then, having identified and assessed the relevant risks, and depending on the organization’s risk appetite or limits for taking risks, management (you and your colleagues) can determine how best to manage these risks. In some cases, the risk response may be acceptance—that is, taking no action apart from monitoring the changes in risk. In other cases, you may opt for (1) avoidance—not participating in or exiting the activities giving rise to a given risk; (2) reduction—removing the source, changing the likelihood, or changing the nature, magnitude, or duration of the consequences of a given risk; or (3) sharing—transferring a portion of the risk via insurance, hedging, a joint venture, or other technique. Your final risk response could be exploitation or even taking on more risk, treating the risk as an opportunity.

Financial leveraging of a company, attracting more debt and thus increasing the debt/equity ratio (gearing level), is a good example of taking on more risk in the pursuit of better (financial) performance. Effective risk management can support determination of the optimum gearing level, taking into account the company’s particular objectives, its limits for risk taking, and the ever-changing circumstances.

This risk assessment process is both dynamic and iterative. Once you and your colleagues have identified and assessed risk in pursuit of your organization’s objectives, proper risk management helps you make informed decisions about the level of risk you want to retain and implementation of the necessary controls. Then, as objectives and circumstances change internally and externally, your organization’s risk management response may also need to be revised.

What Is Internal Control?
Internal control, as defined by COSO in its Internal Control—Integrated Framework (2013), is “a process, effected by an entity’s board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.” Effective internal control is an integral part of an organization’s governance system and ability to manage risk.
the governing body, management, and other personnel in your organization should understand, affect, and actively monitor internal control to take advantage of the opportunities and to counter the threats to achieving your organization’s objectives.

Risk management and internal control can be viewed as two sides of the same coin in that risk management focuses on the identification of threats and opportunities, and controls are designed to effectively counter threats and take advantage of opportunities. Before designing, implementing, applying, or assessing a control, your organization should consider the risk or combination of risks at which the control is aimed. It should also consider the need to remain agile, avoid overcontrol, and not become overly bureaucratic. Risk management and internal control should enable, not hinder, the achievement of organizational objectives.

Since risk can never be fully managed, you must build resilience into all actions your organization takes so it can respond adequately to significant changes in circumstances or deal with the effects of unforeseen consequences. After all, it isn’t the strongest or even the most intelligent of a species that survives but rather the one most adaptable to change.

Effective RM/IC Building Blocks
Risk management and internal control can be effective only when those involved clearly understand how they relate to their roles in setting and achieving their organization’s objectives. Therefore, RM/IC should be integrated through formal and informal channels into the elements of the organization’s system of management in which they are intended to operate, including the related objectives, activities, processes, systems, risks, and responsibilities.

Establishment of effective RM/IC should include:

◆ Implementing a RM/IC framework and processes in accordance with the standard(s) and/or guidance leveraged by the organization;
◆ Defining the entity’s risk management strategy, approving the limits for risk taking where feasible, and determining the criteria for internal control;
◆ Ensuring that RM/IC is part of all decision making and subsequent planning and execution;
◆ Monitoring changes in the internal and external environment, determining their effect on the organization’s objectives, and revising responses consistent with the organization’s policies for the management of risk;
◆ Reviewing the effectiveness of the risk management framework and processes on a regular basis; and

◆ Reporting on the organization’s performance, including the effectiveness of its RM/IC arrangements and, where necessary, plans to address significant issues.

One of the most critical aspects of an effective implementation is to remember that risk management and internal control aren’t objectives in their own right. Rather, they help your organization set and achieve its strategic, operational, reporting, compliance, and other objectives. RM/IC shouldn’t be implemented in isolation but should be built into your organization’s overall system of management, including its policies; its planning, execution, and reporting processes; its values; and its culture.

Leveraging Available Standards, Guidelines, and Resources
If you want to establish more effective RM/IC in your organization, you can leverage several new or newly revised standards, guidelines, and resources. Let’s take a look at some of them.

COSO Internal Control—Integrated Framework (2013)
In May 2013, COSO issued a revised version of its Internal Control—Integrated Framework (ICIF). The updated Framework consists of three volumes and a companion document.

◆ Internal Control—Integrated Framework Executive Summary represents a high-level overview of the 2013 Framework and is intended for the CEO and other senior management, boards of directors, and regulators.
◆ Internal Control—Integrated Framework and Appendices sets out the Framework in detail, defining internal control, describing the components of internal control and their underlying principles, and providing direction for all levels of management in designing and implementing internal control and assessing its effectiveness. The appendices to this volume, including a glossary, specific considerations for smaller entities, and a summary of changes compared to the 1992 version, provide additional reference but aren’t considered part of the Framework.
◆ Internal Control—Integrated Framework Illustrative Tools for Assessing Effectiveness of a System of Internal Control provides templates and scenarios to support management in applying the Framework, specifically in terms of assessing effectiveness.
◆ Internal Control over External Financial Reporting: A Compendium of Approaches and Examples provides
practical approaches and examples illustrating how the components and principles in the Framework can be applied in preparing external financial statements. It is intended to be used as a resource for questions and research on specific principles and components rather than being read from cover to cover.

As shown in Figure 1, the guidance builds on five components of internal control: control environment, risk assessment, control activities, information and communication, and monitoring activities. The fundamental concepts underlying the five components are conveyed in the form of 17 guiding principles and more detailed points of focus. (Also see Revised COSO Framework: Improved but Further Adjustments Warranted, IFAC, July 2013, and The 2013 COSO Framework & SOX Compliance: One Approach to an Effective Transition, COSO, June 2013.) Although all components are necessary for effective internal control, the Framework doesn’t prescribe specific controls. Instead, the selection of controls to effect the relevant principles and associated components is a function of management judgment based on factors unique to the organization.

The revised Framework will supersede the original Framework at the end of 2014, giving your organization, when applicable, time to transition. COSO anticipates a relatively easy transition process for those organizations that have applied the original 1992 Framework properly. In fact, the new principles and points of focus should make it easier for organizations to see what is covered and where gaps may exist.


COSO’s Enterprise Risk Management (ERM) Framework was published in 2004 and provides guidance to help businesses and other entities develop and apply their ERM activities. The Framework expands on internal control and provides key principles and concepts on the
broader subject of enterprise risk management. Specifically, the COSO ERM Framework identifies and describes eight interrelated components that are necessary for effective ERM, including internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, and monitoring.

Internal control is an integral part of ERM, which is part of an organization’s overall governance arrangements. Thus COSO’s ERM Framework complements COSO’s newly released ICIF. ERM is applied in setting strategies as well as in achieving operational, reporting, and compliance objectives. COSO’s ERM Framework also expands the ICIF risk assessment component into event identification, risk assessment, and risk response, and it introduces the concepts of risk appetite and risk tolerance (see Figure 2 for a comparison of the two frameworks). A summary of both COSO frameworks and other materials are available for free, and the frameworks are available for sale, at www.coso.org.

The ISO’s Standard 31000:2009—Risk Management, published in 2009, sets out principles, a framework, and a process for managing risk that are applicable to any type of organization in the public or private sector. The rationale behind this standard is that all of an organization’s activities involve risk and that organizations need to manage this risk effectively. ISO 31000 describes how to do this in a systematic and logical way.

As shown in Figure 3, ISO 31000 specifies 11 principles for managing risk, which include the idea that risk management creates value, represents an integral part of organizational processes, and is part of decision making. In addition, risk management is systematic, structured, and timely; explicitly addresses uncertainty; and is based on the “best available information.” Risk management also should be tailored to the specific circumstances of the organization, consider human and cultural factors, and be transparent and inclusive. Finally, it is dynamic, iterative, and responsive to change, and it facilitates continuous improvement.

The ISO 31000 risk management framework (see Figure 3) provides the foundations and organizational arrangements for designing, implementing, monitoring, reviewing, and continually improving risk management throughout the organization. These arrangements need to be in place to enable good risk management.

The ISO risk management process (see Figure 3) is composed of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring, and reviewing risk. These are the iterative steps that need to be considered as an integrated part of
management and execution in every decision or action. One note: The principles, framework, and process in the ISO 31000 standard are interrelated, and all need to be implemented and applied in order for risk management to be effective in your organization.

Implementing ISO 31000 enables your organization to:
- Be aware of the need to identify and treat risk throughout the entity;
- Improve the identification of opportunities and threats;
- Establish a reliable basis for decision making and planning;
- Increase the likelihood of achieving its objectives;
- Improve operational effectiveness and efficiency;
- Enhance health and safety performance as well as environmental protection;
- Comply with relevant legal and regulatory requirements;
- Improve mandatory and voluntary reporting; and
- Improve stakeholder confidence and trust.

The standard doesn’t mandate a one-size-fits-all approach. Instead, it emphasizes the fact that the management of risk must be tailored to the specific needs and structure of your organization.

The ISO Standard 31000 is available for sale at [http://webstore.ansi.org](http://webstore.ansi.org). Many organizations use both the COSO ERM and the ISO 31000 frameworks. The biggest challenge, however, is that the terms and concepts underlying both standards aren’t aligned (see Table 2).

### IFAC’s Evaluating and Improving Internal Control in Organizations

Despite the existence of sound internal control guidelines, the application of such guidelines often fails or could be further improved in many organizations. Evaluating and Improving Internal Control in Organizations, part of IFAC’s International Good Practice Guidance series, is a practical guide focused on how you can support your organization in evaluating and improving internal control as an integral part of its governance system and risk management (see Figure 4). The guidance is complementary to existing internal control guidelines because it highlights a number of areas where the practical application of such guidelines often fails in many organizations.

Specifically, IFAC’s guidance helps you and your organization answer many key questions, including:
- What should be the scope of our internal control?
- Who should be responsible for internal control?
- How should controls be selected, implemented, and applied?
- How can internal control be better integrated into the DNA of our organization?
- How should our organization report on internal control performance?

Both the full guidance as well as an executive summary are available at [www.ifac.org](http://www.ifac.org).

### The Role of Management Accountants

In many organizations, management accountants are in a position of cross-functional leadership, which means they can play a key role in planning, implementing, executing, evaluating, and improving risk management and internal control.

First, they can champion the importance of good risk management, including internal control. Because of their attitude and behavior, they can set the tone for good
RM/IC throughout the organization as well as drive the integration of RM/IC into line management. They also enable appropriate application of RM/IC principles by organizing training sessions in understandable language. Most important, however, they can ensure RM/IC is part of every decision-making process and subsequent planning and execution.

Second, management accountants can support line management by providing high-quality information. Decisions should be made only with explicit understanding of related risks and the potential consequences for achieving an organization’s objectives. Thus decision makers require relevant and reliable information for decision making and control processes. Management accountants are responsible for providing objective, accurate, and timely information and analyses, which often are produced through the finance and control systems, thereby ensuring decision makers have the high-quality information they need.

Third, management accountants should establish RM/IC for the finance function. Since they usually are responsible specifically for finance and control, they should make RM/IC part of every decision and subsequent steps related to achieving the organization’s finance function objectives.

Fourth, management accountants can evaluate and improve the effectiveness of their organization’s risk management and internal control framework and processes. They also can play a leading role in ensuring that RM/IC continues to be an integral part of their organization’s system of management.

Finally, management accountants can also take the lead in analyzing and reporting on the organization’s performance, including the effectiveness of its RM/IC arrangements.

**Call to Action**

Now you know that having effective RM/IC is both an important driver of business performance and one of the best defenses against business failure. And you realize that highly successful organizations know how to take advantage of opportunities and counter threats, thereby continually improving their overall performance. You have gained insight into good vs. bad RM/IC practices and have been introduced to several of the most respected RM/IC frameworks and guidance available.

Armed with this knowledge, you and your colleagues can play an important role in evaluating and further improving RM/IC in your organization. Specifically, we challenge you to:

- Continue to build subject matter expertise regarding the key frameworks, guidelines, and regulations impacting governance, risk management, and internal control;
- Educate your organization’s governing body, audit committee, C-suite, operating unit, and/or functional management, as well as other staff, on the pitfalls to effective RM/IC, and provide insight into strategies on how to avoid or overcome these pitfalls;
- Champion the importance of leveraging good RM/IC practices;
- Enable effective decision making by providing line management with high-quality information, including explicit understanding of related risks and their potential consequences;
- Establish effective RM/IC specifically for the finance function; and
- Audit or review your organization’s RM/IC arrangements and report on their effectiveness.

By doing all this, you can truly support your organization in leveraging effective risk management and internal control, thereby enabling sustainable success. **SF**

J. Stephen McNally, CPA, is finance director and controller for Campbell Soup Company’s Napoleon & Flavor Operations. He represented IMA on COSO’s Internal Control—Integrated Framework Refresh Project Advisory Council and chaired IMA’s related COSO Advisory Panel. Steve also served on IMA’s Global Board of Directors and is a member of IMA’s Toledo Chapter. You can reach Steve at j_stephen_mcnally@att.net.

Vincent H. Tophoff, RA, is senior technical manager at the International Federation of Accountants, working directly with the Professional Accountants in Business Committee. Previously he was partner at INTE-Q Integration Management, a management-accountancy-related consulting firm in Utrecht, Netherlands. He is a member of Nederlandse Beroepsorganisatie van Accountants, the Dutch institute of registered accountants. On behalf of IFAC, Vincent participated on the COSO Advisory Council for the revision of the Internal Control—Integrated Framework and is part of the ISO Project Committee developing implementation guidance for the ISO 31000 Risk Management Standard. You can reach Vincent at VincentTophoff@ifac.org.

Copyright © 2014 by International Federation of Accountants (IFAC). Used with permission. All rights reserved. Written permission from IFAC is required for use of this text, including permission to translate. Contact permissions@ifac.org.