# RISK MANAGEMENT FRAMEWORKS:

# Adapt, Don't Adopt

## Here's a primer on how to use two well-known approaches.

**By Mark L. Frigo, CMA, CPA, and Richard J. Anderson, CPA**

As enterprise risk management (ERM) continues to evolve, a body of knowledge about that process is being developed. It includes terminology, accepted key components, leading practices, and overall conceptual frameworks. While ERM should be viewed as a still developing process, the conceptual frameworks can be useful tools for developing, implementing, or enhancing an organization's ERM initiative. Here we'll provide a background, overview, and some suggestions for how you can use ERM frameworks. We also will discuss the two most widely recognized risk management frameworks in use today: the *COSO Enterprise Risk Management—Integrated Framework* (2004) and *ISO 31000 - Risk management—Principles and guidelines* (2009).

In what ways can an ERM framework be a useful tool for management and risk professionals who want to build or enhance their processes and capabilities? It provides a structure, an inventory of practices, and a conceptual picture of what enterprise risk management can encompass. For organizations initiating ERM, a framework can provide a useful roadmap to help guide them in developing their plans and related processes. For those seeking to enhance their current ERM processes, a framework gives them a way to assess the development, maturity, and completeness of their existing practices to identify gaps or areas they need to strengthen. It also helps them identify and focus on the development of key processes, such as a common risk language and definitions that span the entire organization and facilitate a common view of risk and risk management. Finally, because of how they were developed and the organizations involved in developing them, the two frameworks we discuss here give a basic level of credibility to the risk management actions and plans being undertaken that are based on them. For example, a large public company that was urged by its board of directors to develop more formal risk management processes used the ISO 31000 framework as the basis for plans to implement a formal ERM initiative. Its risk management working group communicated to the directors that the actions the group was taking were consistent with that framework, which gave the directors additional confidence in the plans being developed.

## Adapt, Don't Adopt

Yet you shouldn't view the risk management frameworks as simply "plug and play" tools. Any business process ultimately must be gauged against the challenge of whether it helps the organization achieve its objectives or not. Both ERM frameworks discussed here are grounded in that aim, helping organizations achieve their business objectives. But that aim isn't achieved through simply implementing one of the frameworks. An ERM initiative that's intended to achieve that aim must be tailored to reflect the culture, processes, management style, and types of risks specific to that organization. As Anette Mikes, assistant professor of business administration at Harvard Business School, noted in "The Struggle to Codify Risk Management," *Risk & Regulation*, Winter 2012, "Cultural theorists have shown us that risk means different things in different organizations, while experience tells us that a given risk model will work in some contexts and not in others." The two frameworks acknowledge this important fact and communicate to potential users the need for tailoring their specific risk management processes in the actual application. Therefore, organizations should view the frameworks as important working tools and apply them according to the philosophy of W. Edwards Deming, a founding father of Total Quality Management (TQM), in his book *Out of the Crisis*: "Adapt, don't adopt!"

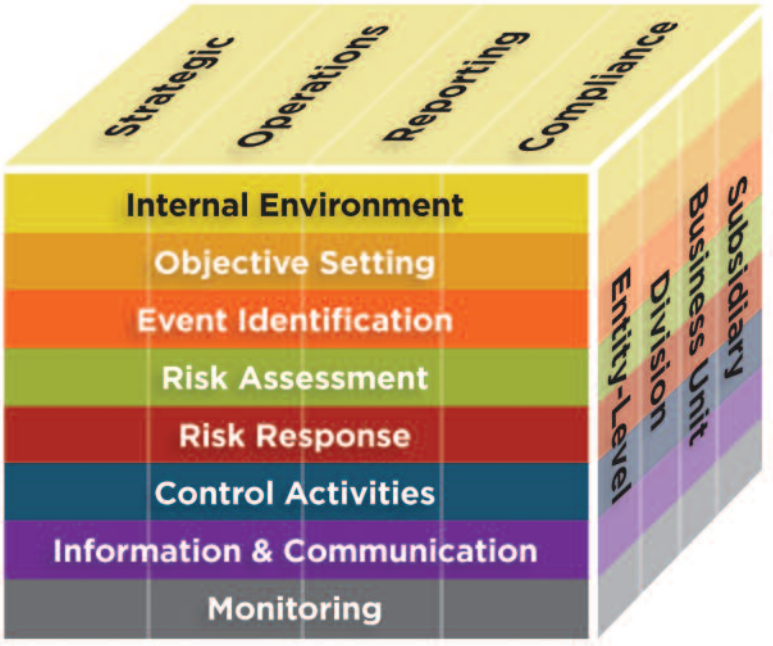
The analogy of risk management and TQM provides valuable insight. Experience from TQM tells us that standardization at the early stage of development of business practices such as ERM can impede innovation. This advice isn't applicable only to how organizations can use risk management frameworks but also to how they should view risk practices other organizations use. In other words, they should resist the temptation to simply duplicate or blindly adopt a risk framework or risk management practices from other companies since the risk practices that work at one company may not fit the needs or expectations of another company. Accordingly, there's value in using ERM frameworks, but that value isn't in rigidly attempting to implement a complete framework. It's in their use as tools and guides for these processes.

As a management accounting or financial professional, you also need to think strategically about how risk management can create as well as protect value in your organization. While risk is usually viewed in terms of its negative impacts, it also has a positive side. It can point to opportunities for organizations to take on more risk if that additional risk fits within their risk appetite and strategy. A recent article in *Strategic Finance* ("Strategic Risk Management at the LEGO Group" by Mark L. Frigo and Hans Læssøe, February 2012) makes this point very well: "Risk management is not about risk aversion. If, or rather when, you want/need to take bigger chances than your competitors—and get away with it (succeed)—you need to be better prepared. The fastest race cars in the

world have the best brakes and the best steering to enable them to be driven faster, not slower. Risk management should enable organizations to take the risks necessary to grow and create value." Accordingly, as organizations develop their risk management processes, they can use those processes to consider the opportunity side of risk and use those processes to both protect and create value.

In the end, you need a clear strategy for risk management in your specific organization that's based on sound risk management concepts and practices but is also tailored to fit your organization. For example, the quantitative risk models and practices that may be necessary and appropriate for an organization with more mature risk processes and significant financial risk exposures are probably not the place to start when implementing an initial ERM initiative in another organization.

**Figure 1: COSO ERM "Cube" Model**






## Two ERM Frameworks

As we mentioned, the two most widely recognized ERM frameworks are:

- *Enterprise Risk Management—Integrated Framework*, issued in September 2004 by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), and
- *ISO 31000 - Risk management—Principles and guidelines*, issued in 2009 by the International Organization for Standardization (ISO).

Both frameworks were developed by internationally recognized thought leadership (COSO) and standards-setting (ISO) bodies, and, during development, each received significant input and vetting from a wide range of risk management experts and professionals. As such, both frameworks have received much recognition and are used in practice.

### The COSO ERM Framework

*Enterprise Risk Management—Integrated Framework* incorporates COSO's previously issued *Internal Control—Integrated Framework* and, according to COSO, "expands on internal control, providing a more robust and extensive focus on the broader subject of enterprise risk management."

The framework defines enterprise risk management as follows:

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

Several key concepts are contained in that definition:

- ERM is a process, not just an event;
- It is directly related to setting strategy;
- It applies across the entire entity; and
- It is geared toward achieving the entity's objectives.

The actual ERM framework identifies and defines eight interrelated components of enterprise risk management:

1. Internal Environment,
2. Objective Setting,
3. Event Identification,
4. Risk Assessment,
5. Risk Response,
6. Control Activities,
7. Information and Communication, and
8. Monitoring.

COSO also says that "almost any component can and does influence another."

The COSO ERM "cube" model (Figure 1) is intended to display the relationship between the components, the

organization's objectives, and the organization's structure. As such, it's a robust model, especially in portraying a complete "end point" picture of ERM. The three dimensions of the cube reflect and relate the components of risk management, the organization's business objectives, and its organizational structure: the "complete picture." The three-dimensional structure of the COSO cube also facilitates addressing parts of the framework during implementation. For example, by taking one slice through the cube, you could construct a plan focused on risk processes related to just one of the strategic objectives or take a different slice and construct a plan to develop risk processes for one business unit.

### ISO 31000

Regarding *ISO 31000 - Risk management—Principles and guidelines*, ISO notes that "the adoption of consistent processes within a comprehensive framework can help to ensure that risk is managed effectively, efficiently and coherently across an organization." Like the COSO framework, ISO 31000 was developed with extensive input and vetting by a working group and was approved by the ISO member bodies.

ISO 31000 includes a number of key concepts:

- It can be used by all organizations.
- It can be applied throughout the life of an organization and to a wide range of activities.
- It can be applied to any type of risk.
- It recognizes the need to take into account the varying needs of a specific organization.

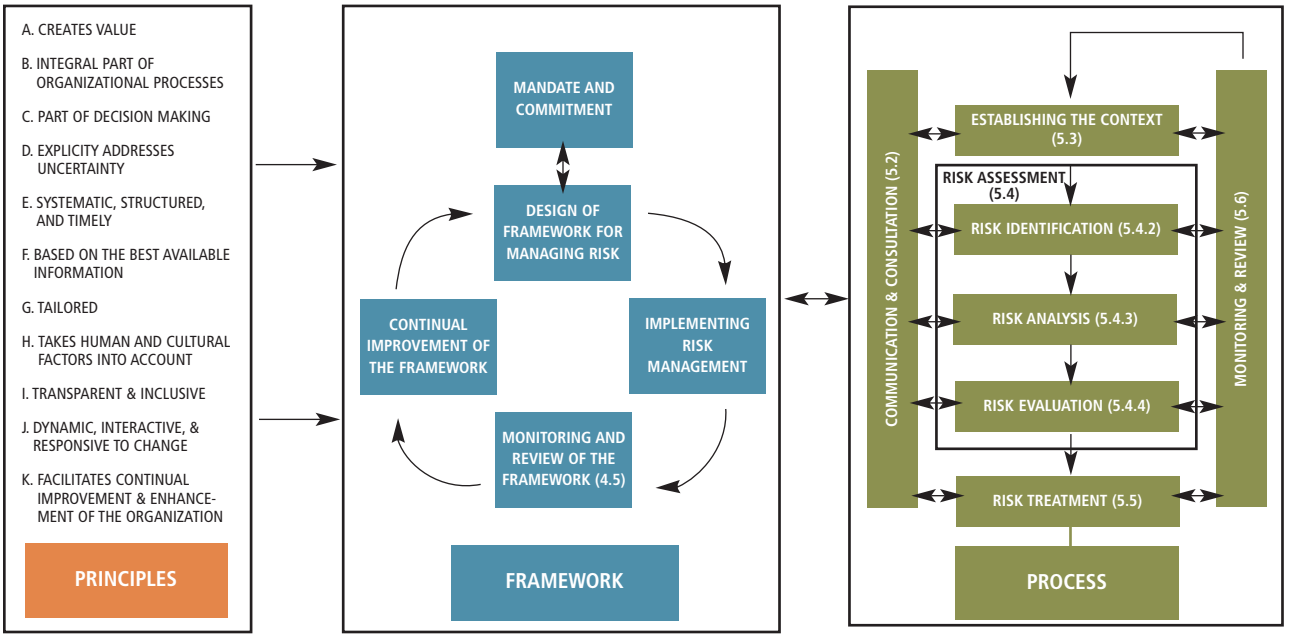
Figure 2 demonstrates the relationships between principles, a framework, and the supporting risk processes. In particular, it begins by listing 11 principles that are the foundations of risk management:

1. Creates and protects value;
2. Integral part of all organizational processes;
3. Part of decision making;
4. Explicitly addresses uncertainty;
5. Systematic, structured, and timely;
6. Based on the best available information;
7. Tailored;
8. Takes human and cultural factors into account;
9. Transparent and inclusive;
10. Dynamic, iterative, and responsive; and
11. Facilitates continual improvement of the organization.

Some managers see the ISO 31000 risk management model as intuitive because it moves from principles to framework to processes. ISO also strongly emphasizes the need to tailor the risk processes to individual organizations.

Each risk management framework has its strengths and advantages, and both are well grounded in their development and use. Accordingly, their usefulness isn't based on determining whether one is viewed as superior to the

**Figure 2: ISO 31000 – Risk Management**



other. Rather it is in having these two frameworks available to give organizations and risk personnel a more robust knowledge base to utilize as they evolve their own risk processes.

## Fitting the Needs of Your Organization

As we mentioned, both ERM frameworks note the significant benefits of using a framework, and both note the need to tailor risk processes to an organization. Thus the proper way to use a framework isn't as a checklist or concrete model but as a tool to identify risk approaches and processes that would work best in a specific organization.

When undertaking a risk management initiative, you can review each framework, consider how it would be applicable to your organization and how it would be applied, and determine if your organization would be more comfortable using one or the other for guidance in achieving its specific needs. For example, organizations that are using the *COSO Internal Control—Integrated Framework* may find it easier and more familiar to use the COSO ERM Framework, which incorporates the COSO Internal Control Framework. Other organizations may want to start by articulating or redefining their risk principles, in which case ISO 31000 may be a better fit because risk principles are more prominent in that framework. In either case, an organization should carefully review the detail of the framework it selects to determine where tailoring needs to be done.

A next step would be to consider where in the selected framework to start the ERM initiative. As we've observed, ERM initiatives tend to be most successful when taken in iterative steps. Therefore, reviewing the selected framework is a good place to determine where the initial or next step should be taken (see Mark L. Frigo and Richard J. Anderson, *Embracing Enterprise Risk Management: Practical Approaches for Getting Started*, COSO, 2011). For example, if you are using the COSO framework, you may find that you can start by taking one of the business objectives and developing the risk management components related to that objective. Another possible approach is to take one major business unit and develop the risk processes across that unit. If you are using ISO 31000, developing your organization's statement or policy of its risk principles may be a starting point.

## Develop Your Own Plan

While ERM processes are continuing to evolve and mature, many organizations are taking steps to implement more formal and structured risk management processes. A recognized and accepted risk management framework can be a useful and helpful tool for these organizations as they develop or significantly enhance their risk management practices. By using and tailoring one of the two risk management frameworks we've discussed, your organization's management and directors can benefit from giving their risk management initiatives a strong conceptual grounding and a supporting body of knowledge that will help them test the completeness and direction of their ERM initiative. Again, enterprise risk management processes, capabilities, and frameworks continue to develop, but they are currently at a stage where standardized implementation can impede innovation and the development of tailored risk management practices. Management and boards need to adapt rather than rigidly adopt a specific framework and develop a clear strategy for risk management that fits the needs of the organization. **SF**

*Mark L. Frigo, CMA, CPA, Ph.D., is director of the Center for Strategy, Execution and Valuation and the Strategic Risk Management Lab in the Kellstadt Graduate School of Business and Ledger & Quill Alumni Foundation Distinguished Professor in the Driehaus College of Business at DePaul University in Chicago, Ill. He is an advisor to executive teams and boards in the area of strategic risk management and strategy development and execution. You can reach Mark at mfrigo@depaul.edu.*

*Richard J. (Dick) Anderson, CPA, is a clinical professor in the Center for Strategy, Execution and Valuation and the Strategic Risk Management Lab at DePaul University and a retired partner of PricewaterhouseCoopers LLP. At PwC, he was a regional leader in the Financial Services Advisory practice, consulting with major financial services organizations on internal auditing practices, risk management, and audit committee activities. You can reach Dick at rander37@depaul.edu.*