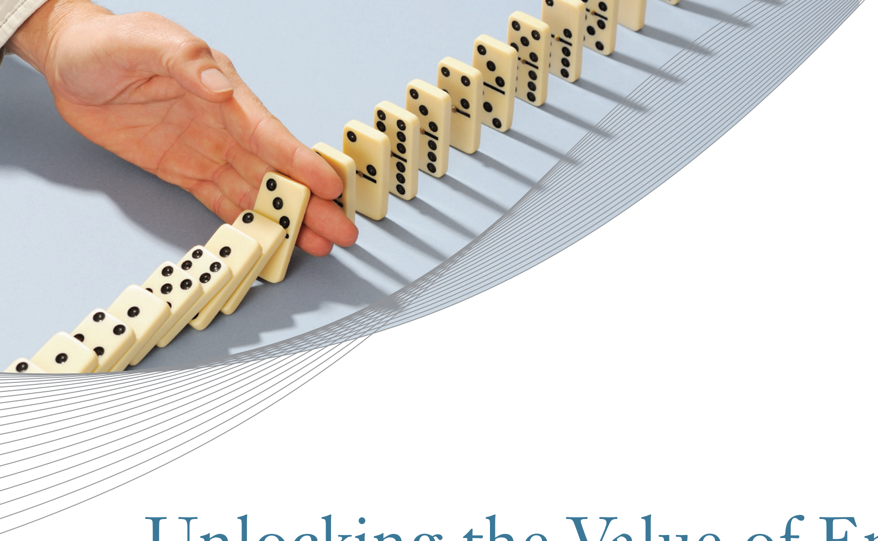

protiviti®
Risk & Business Consulting.
Internal Audit.

Unlocking the Value of Enterprise Risk Management in the Public Sector

POWERFUL INSIGHTS

Issue

Enterprise risk management (ERM) has demonstrated its value in the private sector, producing successful organizations that follow an effective process to minimize risks and achieve desired outcomes.

It should come as no surprise, then, that the federal government has taken a heightened interest in this proven practice, adapting it to public agencies in an effort to better manage risks that tend to hide in complex bureaucracies with limited interdepartmental communication.

In 2014, the Office of Management and Budget (OMB) issued a revised Circular No. A-11, which, for the first time, formally introduced ERM to federal government agencies. Government officials have been hesitant to embrace it, however, because of uncertainty about ERM's value and efficacy in the public sector, as well as concerns about implementation. Below, we address some of the most common concerns and offer information to overcome such hurdles, clearly defining ERM's benefits along with the proper steps for integrating it into an organization's culture and operations.

What Is ERM?

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) defines ERM 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."

Put simply, ERM is a strategic process sponsored at the highest level of an organization to protect it against being blindsided by unforeseen risks and to ensure that all risks are managed within a specific risk tolerance.

For a public sector agency, ERM can:

- Reduce unacceptable performance variability
- Align and integrate varying views of risk management
- Enhance governance
- Improve responses to a changing business environment
- Align strategy and organizational culture

Most importantly, ERM's scope is far broader and more strategic than conventional risk management approaches. Whereas traditional methods focus exclusively on protecting tangible assets and related contractual rights and obligations, ERM operates across the enterprise, and its application is targeted to the achievement of the agency's mission, goals and objectives, as well as to the protection and enhancement of the unique combination of tangible and intangible assets.

ERM elevates risk management to a strategic level by broadening its application to all sources of value – including brands, innovative processes, knowledge and reputation – and not just physical and financial ones.

Seeking Continuous Improvement

It is important to remember that COSO describes ERM as a means to an end, not an end in itself. The process of implementing ERM is fundamentally a process of education: building awareness, developing buy-in and, ultimately, assigning accountability and accepting ownership. ERM should be viewed as a commitment to continuous improvement, constantly anticipating and adapting to the changes of an evolving global environment.

Before embarking on an ERM initiative, it is critical for the public agency to have the necessary leadership to steer it. Because it is so important to the success of the organization, risk management deserves its own champion at the highest level of management. The responsibilities for executing ERM should not be folded, for example, under the duties of the chief financial officer (CFO) or its public sector equivalent. Rather, they should be assigned to a chief risk officer (CRO), who should be insulated from and independent of agency or departmental operations.

Such objectivity is essential to provide an agency's senior leadership with unbiased assessments of risks associated with transactions and deals – broken down into their fundamental components and evaluated with a balanced view so they can be measured and managed systematically.

As the chief advocate for ERM, the CRO works in a consultative and collaborative role with management to define the role of risk management in the organization – and, just as important, communicates that role to everyone within the organization. It is the CRO's responsibility to work with appropriate officials to monitor risk across the enterprise, oversee and enforce risk management policies, and instill discipline to close gaps in capabilities.

The CRO also develops measurement methodologies and monitoring methods, including dashboards and key risk indicators (KRIs), to aggregate risk exposures and risk management performance. These tools not only help improve the organization's performance, but also permit the CRO to provide quantifiable feedback and assessments to senior leadership. Ultimately, with the aid of such information, the CRO can help top officials make better decisions about capital and resource allocation.

Developing a Shared Vision

Before implementing ERM, leadership needs to develop a shared vision of the role of risk management in the agency. A working group of senior officials should be empowered to articulate this role and define relevant goals and objectives for the public entity and each of its business units.

A shared vision is a call for action to drive the organization to identify, design and build the risk capabilities needed to close significant gaps and make selected risk responses happen. To set objectives, leaders must define those goals within the context of the organization's business strategy. Such an exercise requires asking critical questions, including:

- What is it we are trying to accomplish as an agency – what is our mission?
- Which specific future events could interfere with our ability to achieve these objectives?
- What are our expected outcomes?
- If we accept risks or exposures as inherent to our business model, do we have sufficient resources to achieve our objectives, despite any anticipated setbacks?

Honest answers to these questions provide a powerful context for an organization to define its next steps, as well as its risk appetite. As defined by COSO, risk appetite is the amount of risk an entity is willing to accept in pursuit of value – or in the case of a public agency, mission. It articulates the risk a public agency chooses to accept and the risks it chooses to mitigate, transfer or avoid. Most importantly, it can set boundaries around opportunity-seeking behavior, providing individual units within an organization with a guidepost for aligned strategy.

Steps of Implementation

Again, it is important to remember that ERM is a journey, and that success will not be achieved overnight. The following are practical implementation steps to begin that journey:

- **Conduct an enterprise risk assessment (ERA) to assess and prioritize critical risks.** This step allows the agency to gather information and input from all stakeholders and evaluate accurately the current state of capabilities. If the agency has not identified and prioritized its risks, it is virtually impossible to gain buy-in from senior management and staff because the value proposition would be generic.
- **Articulate the risk management vision and support it with a compelling value proposition.** This action provides the economic justification for going forward. Once current management capabilities are determined for each priority risk, the organization must determine the desired state it wants to achieve. Ultimately, the goal is to identify gaps between current and desired states and advance strategies to close them. The wider the gap, the greater the need for ERM infrastructure – which includes policies, processes, oversight and reporting – to instill the necessary focus, discipline and control that allows for continuous improvement.
- **Evaluate the existing ERM infrastructure capability and develop a strategy for advancing it.** It takes discipline to advance an organization's capabilities. To manage systemic risk properly, public agencies need appropriate ERM infrastructure, which also can include the following: a common risk language and other frameworks; knowledge-sharing to identify best practices; common training; and integration of risk

responses with business plans. ERM infrastructure establishes fact-based understanding about risks and capabilities and designates ownership and accountability for risk management.

- **Update the ERM plan for change and broaden the focus to other priority risks.** Risk management capabilities must be advanced continually in the context of an agency's finite resources. This process requires leadership to make key decisions based on questions such as "What additional capabilities do we need to provide reasonable assurance we will achieve our mission?" and "What are the expected costs and benefits of increasing capabilities?" These questions help the organization identify its most pressing exposures and uncertainties and drives progress toward addressing them.

Avoiding Pitfalls

To implement the above steps successfully, senior management needs to be aware of – and avoid – some common pitfalls. For example, it is essential to obtain buy-in from across the organization. Skepticism can be countered best by demonstrating fact-based, measurable value that can be achieved through ERM.

Leadership also needs to understand the perspective and concerns of each organizational unit to avoid cultural resistance to an enterprisewide approach. Finally, ERM return on investment (ROI) must be properly defined. For a public agency, ROI doesn't necessarily mean cost savings. ERM outcomes can be measured by successful mission accomplishments – for example, generating research outcomes or earning educational accolades.

Once ERM takes root in an organization, its numerous benefits become apparent. They include:

- Instilling confidence in a systematic risk evaluation process
- Configuring risk-taking with mission and strategic goals
- Optimizing risk management through an agency-wide adherence to a methodology
- Eliminating redundant and unnecessary activities
- Reducing operational losses and surprises
- Improving capital deployment and resource allocation
- Improving compliance, reporting and risk responses

The last point is particularly compelling for public agencies. ERM reporting enables more measurable and consistent disclosure, contributing to an organization that operates with greater transparency.

Conclusion

Leaders of public sector organizations face serious challenges: They must continuously direct scarce resources to sustain vital government activities and services; they must manage their operations in the face of constantly changing circumstances; and they must provide assurance to various stakeholders that they can protect and enhance their organizations. ERM redefines the value proposition for public agencies by providing the processes and tools they need to become more anticipatory and effective in managing uncertainties. By better managing risk at an "enterprise" level, government can run more efficiently, resulting in more missions accomplished, fewer surprises and greater public trust.

PROVEN DELIVERY

How We Help Companies Succeed

Many government agencies and public companies are increasingly paying attention to government operations' risks, especially in the areas prone to fraud, waste, abuse and mismanagement, or focusing on operations in need of transformation to better address economy, efficiency or effectiveness challenges. These agencies recognize that solutions to risk problems offer the potential to save billions of dollars, improve service to the public and strengthen performance and accountability.

Protiviti helps public sector companies mitigate high-risk issues, translating risk into billions of dollars saved and further improving the performance of federal programs and operations. Our risk management professionals leverage best-in-class frameworks and practices from the private industry that are also applicable to and have been used with great success in government settings. Our experts work with all levels of state and federal government to enable a more transparent and risk-aware culture inside agencies, by helping to develop a formal risk strategy through the modification of processes and establishment of a risk management organization and structure.

Contacts

John DiDuro
+1.703.299.4718
john.diduro@protiviti.com

Gene Weber
+1.571.382.7814
gene.weber@protiviti.com

About Protiviti

Protiviti (**www.protiviti.com**) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit, and has served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. Protiviti and our independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Named one of the 2015 *Fortune* 100 Best Companies to Work For®, Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.

protiviti®
Risk & Business Consulting.
Internal Audit.