
Building Enterprise Risk Management on the Foundation Laid by Sarbanes-Oxley



By James W. DeLoach, Managing Director, Protiviti

Businesses have always faced a variety of risks, but these days the pace of change and the resulting risks seem to be even greater than ever. Some examples:

- Globalization has increased exposure to international events.
- The need for increased efficiency, innovation and differentiation, while always important, has escalated in importance as companies seek new ways to differentiate themselves.
- Competitor risk continues to be a priority, but the cost of strategic error is rising in the global marketplace. Financial markets are more volatile than ever. Obsolete business models create a losing hand in the game. And, even if the business model is the right one to establish sustainable advantage, it is a winner only if the organization is able to execute it effectively.
- Unfortunately, we now know the unthinkable can happen. The events of September 11, 2001 have changed how we think about business interruption risk.
- Due to the highly publicized public reporting fiascos, financial reporting is now a risk area as companies shore up their disclosure and internal controls.

Today these and other risks are among a continually changing profile of risks that have not only financial implications but strategic and operational impacts as well. The increasing complexity of business means that for many organizations, traditional risk management does not do enough to preserve shareholder value. Research we have done several times over the years indicates that many senior executives lack confidence that they are managing all of their potentially significant business risks. They can gain confidence from an effective process that engages everyone in the organization to manage risk.

Laying the Foundation

The Sarbanes-Oxley Act has been commanding headlines since President Bush signed it into law last year. Because of Sarbanes-Oxley, many public companies have taken a closer look at their governance processes, disclosure practices and internal controls. Even some privates and not-for-profits have joined the scramble to demonstrate to their stakeholders a commitment to improved governance. The push towards greater disclosure has grown to where many constituencies – investors, policy-makers, standard setters, regulators, exchanges, rating agencies – want more information relating to governance, risks and internal control.

Even with improved disclosure controls and procedures, business organizations will continue to succeed and fail as markets, customers, economies and risk profiles change. At Protiviti, we believe that an

effectively implemented enterprise-wide approach to assessing and managing risk will speed risk identification, giving decision makers more time to consider alternative actions and required disclosures. As investor and regulator “need to know” heightens, as the volume of calls for transparency in public reporting increases and as competitors develop and communicate increasingly value-added business models, boards and management must demonstrate greater competence in anticipating and managing business opportunities in the face of an uncertain future.

The good news is that compliance with Sarbanes-Oxley lays a foundation for implementing Enterprise Risk Management (ERM) capabilities that did not previously exist for many companies. While ERM can enhance the quality of internal and external reporting, integrity in reporting is a prerequisite, not a result, of ERM. A full and honest commitment to truthful reporting provides the vital signs of change to which business strategies and processes must respond. An organization cannot manage its risk when it suppresses information about business realities.

Companies that have implemented improved disclosure processes and internal control over financial reporting should take a closer look at how they can expand these capabilities to encompass *all* business activities. Doing so gives executives and directors alike greater confidence that their organizations are identifying and managing *all* potentially significant business opportunities and risks.

Compliance Isn't Enough

Management needs to reach beyond mere compliance with the provisions of the Sarbanes-Oxley Act. Companies need to keep their disclosure process fresh through a process-based chain of accountability that involves unit managers and process owners. More importantly, management needs to leverage the process to address other risks beyond financial reporting.

Most companies are demonstrating compliance with Sections 302 (which requires executive representations by certifying officers) and 404 (which requires an annual assessment of the effectiveness of internal control over financial reporting) of the Sarbanes-Oxley Act. They are documenting financial reporting policies and procedures and the relevant controls. They are also evaluating the controls design and controls operating effectiveness.

While these efforts are necessary and worthwhile, they are not enough. Many companies would benefit from benchmarking their processes against the best-performing companies. Others need to redesign their processes to reduce costs and improve controls. What is really needed, however, is for companies to implement improvements in their risk management processes, internal controls and performance metrics. This is where the real impact occurs in terms of managing risk.

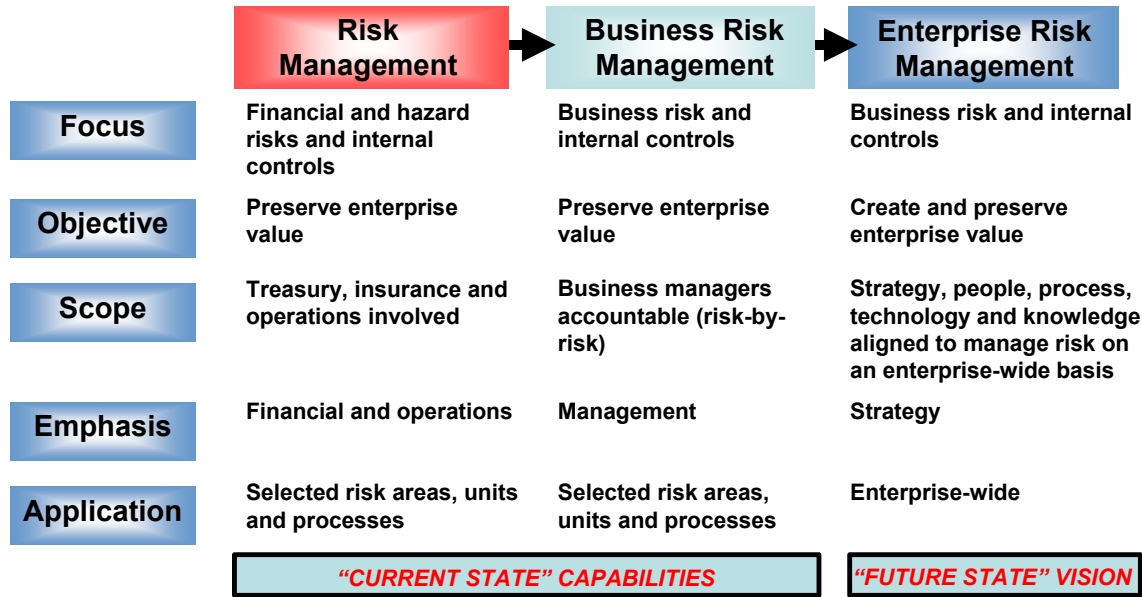
Our premise is this: An enterprise-wide process to do business risk management will help C-Level executives identify new and emerging risks for timely action, disclosure and response. The COSO Enterprise Risk Management Framework released for comment in July illustrates what needs to be done.

A Transition in Risk Management

As the rules of value creation and preservation evolve, traditional risk management approaches will not get the job done unless they are robust enough—even holistic enough—to assure success. In fact, they may even encourage risk adverse behavior that can contribute to failure.

Current risk management approaches are fragmented, treating risks as disparate and easily compartmentalized. Their tight focus on loss prevention is not necessarily a bad thing, but it also is not

such a good thing, because it does not adequately integrate with the identification, evaluation and optimization of growth and capital.



The current state of business risk management must evolve – dramatically. A new strategic business process is needed, one that identifies and addresses the full range of risks and opportunities. That new process is Enterprise Risk Management. As the diagram above indicates, ERM differs from current risk management approaches in terms of focus, objective, scope, emphasis and application.

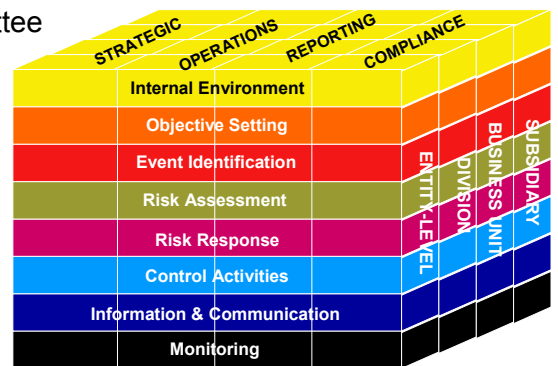
While ERM focuses on business risk and internal controls with an objective to preserve as well as create enterprise value, it aligns strategy, people, processes, technology and knowledge. The emphasis is on strategy. And the application is enterprise-wide.

By managing risks strategically across the enterprise, an organization not only supports Sarbanes-Oxley compliance but also brings to light new risks as they emerge. Transparency is the name of the game. Yes, the disclosure process is vital. But so is the process of managing other risks. ERM instills the discipline needed to continuously improve risk management capabilities.

The COSO ERM Framework

To help us accomplish all this, we now have the COSO (Committee of Sponsoring Organizations) ERM Framework, which provides a benchmark for companies to use to measure the chosen ERM solution. Space does not permit us to explain the framework, which is illustrated at right, in detail. See also <http://www.coso.org>.

The COSO Framework shows that ERM is a process put into effect by people in a strategy setting that is applied across the enterprise so that potential events are identified for risk management purposes. ERM is intended to provide reasonable assurance in supporting the achievement of the organization’s objectives.



The framework is a much needed, long awaited standard that will assist everyone in articulating the components of an ERM solution.

There are several messages we can draw from the COSO framework:

- Many possible elements make up an ERM solution. The COSO framework lists many of these elements.
- Companies have different objectives, strategies, structure, culture, risk appetite and financial wherewithal -- no two ERM solutions are alike.
- The specific policies, processes, skill sets, reports, methodologies and systems that make up the solution for one company may differ from another company.
- Companies looking for off-the-shelf ERM solutions are setting themselves up for disappointment in terms of what they find as well as in the results they get.

Implementing ERM

An ERM solution consists of the eight components of COSO, as noted in the ERM cube above. The design and implementation of an ERM solution entails several key attributes:

- A shared vision of overall goals and objectives.
- A definition of the outcomes that management wants.
- A description of the elements that must be in place to make those outcomes happen.
- A compelling business case and economic justification.
- A journey management plan.
- Effective program management.

The question companies face is where to begin and what to build?

We recommend eight categories of ERM journey elements organized into three groups – foundation elements, process elements and enhancement elements. A “journey element” consists of the processes, people, reports, methodologies, technology, or a combination thereof, integrated within the ERM solution to achieve the expected outcomes specified in the business case. There are many possible elements within each category.

Categories of ERM Journey Elements

FOUNDATION		PROCESS			ENHANCEMENT		
<i>Adopt common language</i>	<i>Establish oversight and governance</i>	<i>Assess risk and develop strategies</i>	<i>Design/ implement capabilities</i>	<i>Continuously improve</i>	<i>Quantify multiple risks Enterprise wide</i>	<i>Improve enterprise performance</i>	<i>Establish sustainable competitive advantage</i>

For example, the first category of elements is “adopt common language”. That category includes such elements as a risk model, risk management glossary, process classification scheme, other relevant frameworks, improved dialogue about risk and its sources, drivers or root causes, and more organized processes for sharing of information. Management selects from these (and other) elements the ones that are needed to realize the organization’s chosen vision, goals and objectives. These elements produce the expected outcomes of increasing the chances of identifying all key risks and enabling people from multiple disciplines to focus on issues faster.

Take the second category of elements, “establish oversight and governance”. Possible journey elements include: an overall risk management policy; top-down communications of risk management direction;

organizational oversight structure, with board oversight; risk management oversight committee and management accountability; a designated senior executive responsible for risk management; integrated risk management and governance processes; and a business risk management staff function. The result should be clarity of risk management role, purpose and accountabilities and faster action by executives with the power to act.

There are many indicators of the need for ERM. They include:

- Management wants more confidence that all potentially significant risks are identified and managed.
- Key decisions are being made without systematic evaluation of risk/reward trade-offs.
- There are no enterprise-wide strategies for taking and bearing risk.
- Risk management is not integrated with strategies and business planning.
- Risks are not identified, sourced, measured or managed on an aggregate basis.
- Units are managing similar risks differently.
- There is a need for improvement in the capital investment process.
- There are more demands for information relating to risks and internal controls from the board and investors.

All told, the company’s selected “journey elements” build the ERM components introduced by COSO in its new framework:

Categories of ERM Journey Elements

	FOUNDATION		PROCESS			ENHANCEMENT		
	Adopt common language	Establish oversight and governance	Assess risk and develop strategies	Design/ implement capabilities	Continuously improve	Quantify multiple risks Enterprise wide	Improve enterprise performance	Establish sustainable competitive advantage
Internal Environment	X	X	X	X	X	X	X	X
Objective Setting		X	X		X	X	X	X
Event Identification	X	X	X		X	X	X	X
Risk Assessment	X	X	X		X	X		
Risk Response		X	X	X	X	X	X	X
Control Activities		X		X	X	X	X	X
Information & Communication	X	X	X	X	X	X	X	X
Monitoring		X		X	X	X	X	X

The business case justifies the investment in an ERM solution. Once the business case is approved, the design and implementation of capabilities that deliver the solution are boiled down to a project plan that will make the solution happen.

ERM can potentially represent a sea change in organizational attitude and behavior. As with any significant change, the adoption of ERM is fundamentally a process of building awareness, developing buy-in and ultimately driving the acceptance of ownership throughout the organization. Change enablement is, therefore, a significant aspect of an ERM initiative because everyone’s perspective about risk varies. Thus the ERM journey is a growth process, which leads the firm to improving its risk management capabilities. As it navigates its journey, the organization becomes more sensitive to changes in the environment and within its business processes.

When implementing ERM, keep in mind the following keys:

- Obtain agreement on risk management objectives and oversight structure.
- Implement an effective enterprise-wide risk assessment process early.
- Clarify the process ownership issues – who decides, who designs, who builds and who monitors?
- Integrate risk management with business planning process.
- Consider relevant cultural issues.
- Focus on enterprise-wide application.

Properly carried out, organizations that engage in ERM can expect greater speed, skill and confidence in pursuit of strategic growth opportunities, more of a value-based approach to risk and a process that supports and builds on the Sarbanes-Oxley compliance efforts.

This is a summary of a presentation by James W. DeLoach, Managing Director – Business Risk Services for Protiviti, at the Enterprise Risk and Control Self Assessment Conference sponsored by The Institute of Internal Auditors in Orlando, Fla., on August 28, 2003.

Protiviti is the leading provider of truly independent internal audit and business and technology risk consulting services. We help clients identify, measure and manage operational and technology-related risks they face within their industries and throughout their systems and processes. And we offer a full spectrum of internal audit services, technologies and skills for business risk management and the continual transformation of internal audit function.

1.888.556.7420

www.protiviti.com