Enterprise Risk Management: Practical Implementation Advice

The concept underlying enterprise risk management (ERM), namely a portfolio view of risk, has been around a long time. The application of this concept emerged in financial institutions and world-class corporate treasuries as they applied at-risk frameworks, capital attribution techniques and other measurement methodologies to the management of market and credit risk. Market developments over recent years have made it clear that volatility isn’t just a currency, interest rate or equity security risk anymore. Customer preferences, competitor product offerings, labor markets and technology are all changing with increasing frequency, with their behavior resembling that of financial markets. Change is no longer linear, but exponential, as the life cycles of organizational business models compress. The bottom line: No business model on the planet is impregnable. Successful companies must innovate and create new sources of value for their customers and markets over time or they will lose ground to nimbler, more creative rivals. Strategy-setting is a fluid, dynamic process. Risk management, which augments that process, is equally fluid and dynamic.

Many executives have no idea what the value proposition of ERM is. Some executives and directors may even consider ERM a fad or “flavor of the month,” and are just humming the dialogue, wishing it would go away. What leaves many cold on the subject of ERM is the inability to quickly grasp what it is. This issue of The Bulletin addresses these and other relevant questions.

What is ERM?

ERM aligns strategy, people, processes, technology and knowledge with the objective of continuously improving the organization’s risk management capabilities over time. The COSO Enterprise Risk Management – Integrated Framework, issued in September 2004, defines ERM as follows:

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.

Note the context of the above definition is strategy-setting. The application is enterprisewide. The standard is the enterprise’s risk appetite.

ERM advances the enterprise’s capabilities around managing its priority risks. When an ERM approach is effectively integrated with strategy-setting, management’s attention is directed to the uncertainties affecting the enterprise’s entire asset portfolio, including its customer assets, its employee/supplier assets and such organizational assets as its differentiating strategies, distinctive products and brands and innovative processes and systems. This expanded focus is important in this era of market capitalizations significantly exceeding balance sheet values and the desire of many companies to reduce the risk of reputation loss to an acceptable level.

Why implement ERM?

Traditional risk management approaches tend to be fragmented, compartmentalizing risks into silos. These approaches often limit the focus to managing uncertainties around physical and financial assets. Because they focus largely on loss prevention, rather than enhancing enterprise value, traditional approaches do not provide the framework most organizations need to redefine the risk management value proposition in a rapidly changing world.

ERM, on the other hand, provides an organization with the process it needs to become more anticipatory and effective at evaluating and managing the uncertainties it faces as it creates sustainable value for stakeholders. ERM helps an organization manage its risks to protect and enhance enterprise value in three ways:

• First, it focuses on establishing sustainable competitive advantage. ERM helps management overcome silo behavior by aligning and integrating varying views of risk and enabling the enterprise to successfully respond to a changing environment. ERM elevates
risk management to a strategic level by broadening the application and focus of the risk management process to all sources of enterprise value, not just physical and financial ones.

• Second, it optimizes the cost of managing risk. Through ERM, management aggregates risk acceptance and transfer decisions, eliminates redundant activities and determines the level of risk the organization is prepared to accept as it executes its business model.

• Third, it helps management improve business performance. ERM assists management with reducing unacceptable performance variability and loss exposure by (a) anticipating the impact of major events and (b) developing responses to prevent those events from occurring and manage their impact on the organization if they do occur. ERM transitions risk management from “avoiding and hedging bets” to a differentiating skill for protecting and enhancing enterprise value as management seeks to make the best bets in the pursuit of new opportunities for growth and return.

ERM invigorates opportunity-seeking behavior by helping managers develop the confidence that they truly understand the risks they are taking on and have the capabilities at hand within the organization to manage those risks. Our research over the years, including our recently issued Protiviti U.S. Risk Barometer (available at www.protiviti.com), consistently indicates that six of ten senior executives “lack high confidence” that their company’s risk management practices identify and manage all potentially significant business risks. The focus of ERM is on integrating risk management with strategy-setting. The emphasis is on identifying future potential events that can have both positive and negative effects and evaluating effective strategies for managing the organization’s exposure to those future events. ERM transforms risk management to a proactive, continuous, value-based, broadly focused and process-driven activity. These contributions redefine the value proposition of risk management to a business.

**Five steps to implementing ERM**

For organizations choosing to implement ERM, we recommend five practical steps. While the following steps provide a simplified view of the task of implementing ERM, the implementation process does not occur overnight. ERM is a journey and these steps provide a practical starting point.

**STEP 1: Conduct an enterprise risk assessment (ERA)**

Using the business strategy as a context, an ERA identifies and prioritizes the organization’s risks and provides quality inputs for purposes of formulating effective risk responses, including information about the current state of capabilities around managing the priority risks. If an organization has not prioritized its risks, ERM becomes a tough sell because the value proposition can only be generic. Identifying gaps relating to the entity’s priority risks provides the basis for improving the specificity of the ERM value proposition. So avoid endless dialogues about ERM: Get started by conducting an ERA to understand the risks inherent in your business model.

**STEP 2: Articulate the ERM vision and value proposition using gaps around the priority risks**

This step provides the economic justification for going forward. The ERM vision is a shared view of the role of risk management in the organization and the capabilities needed to manage its key risks. A working group of senior executives should be empowered to (a) articulate the role of risk management in the organization and (b) define relevant goals and objectives for the enterprise as a whole and its business units.

To accomplish this task, management needs a reliable fact base grounded in specific capabilities that must be developed to improve risk management performance. This is where a gap analysis becomes handy. To illustrate:

(A) Begin with prioritizing the critical risks and determine the current state of capabilities around managing those risks. This is an ERA, as discussed in Step 1. Once the current state of capabilities is determined for each of the key risks, the desired state is assessed with the objective of identifying gaps and advancing the maturity of risk management capabilities to close those gaps. “Risk management capabilities” include the policies, processes, competencies, reports, methodologies and technology required to execute the organization’s risk response.

(B) ERM infrastructure consists of the policies, processes, organizational structure and reporting in place to instill the appropriate oversight, control and discipline around continuously improving risk management capabilities. Examples of elements of ERM infrastructure include, among other things, an overall risk management policy, an enterprisewide risk assessment process, presence of risk management on the Board and CEO agenda, a chartered risk committee, clarity of risk management roles and responsibilities, dashboard and other risk reporting, and proprietary tools that portray a portfolio view of risk.

Here is the message: The greater the gap between the current state and the desired state of the organization’s risk management capabilities (Point (A) above), the greater the need for ERM infrastructure (Point (B) above) to facilitate the advancement of those risk management capabilities over time.
**STEP 3: Advance the risk management capabilities of the organization for one or two priority risks**

This step focuses the organization on improving its risk management capabilities in an area where management knows improvements are needed. Like any other initiative, ERM must begin somewhere. There are many possible starting points. Examples include:

- Compliance with Sections 404 and 302 of the Sarbanes-Oxley Act
- One or two priority financial or operational risks based on the enterprisewide risk assessment results (see Step 1), e.g., operational risk in a financial institution
- Regulatory compliance risks and/or governance reform issues
- Integration of ERM with the management processes that matter, e.g., strategic management, annual business planning, new product launch or channel expansion, quality initiatives, capital expenditure planning and performance measurement and assessment

Regardless of where an organization begins its journey, the focus of ERM is the same – to advance the maturity of risk management capabilities for the priority business risks.

**STEP 4: Evaluate the existing ERM infrastructure capability and develop a strategy to advance it**

It takes oversight, control and discipline to advance the capabilities around managing the critical risks. The policies, processes, organization and reporting that instill that oversight, control and discipline is called “ERM infrastructure.”

The purpose of ERM infrastructure is to eliminate significant gaps between the current state and the desired state of the organization’s capabilities around managing its key risks. We provided some examples of ERM infrastructure above when discussing Step 2. Other examples include a common risk language, knowledge sharing of best practices, common training, a chief risk officer (or equivalent executive), definition of risk appetite and risk tolerances, integration of risk responses with business plans, and supporting technology.

ERM infrastructure facilitates three very important things with respect to ERM implementation. First, it establishes fact-based understanding about the enterprise’s risks and risk management capabilities. Second, it ensures there is ownership over the critical risks. Finally, it drives closure of unacceptable gaps.

ERM infrastructure is not a one-size-fits-all. What works for one organization might not work for another. The elements of ERM infrastructure vary according to the techniques and tools deployed to implement ERM, the breadth of the objectives addressed, the organization’s culture and the extent of coverage desired across the organization’s operating units. Management should decide the elements of ERM infrastructure needed according to these and other relevant factors.

**STEP 5: Advance the risk management capabilities for other key risks**

After the first four steps are completed, it will often be necessary to update the ERA for change. Once there is a refined definition of the priority risks, based on the updated ERA, management must determine the current state of the capabilities for managing each risk and then assess the desired state. The objective is the same as with the one or two priority risks addressed in Step 3, i.e., to advance the maturity of the enterprise’s capabilities around managing its key risks. In taking this step, management broadens the enterprise’s focus to other priority risks.

**Improving risk management capabilities is the objective**

For each priority risk, management evaluates the relative maturity of the enterprise’s capabilities. From there, management needs to make a conscious decision: How much added capability do we need to continually achieve our performance goals and objectives? Improvements in risk management capabilities must be designed and advanced, consistent with the organization’s finite resources and management’s assessment of the expected costs and benefits. The goal is to identify the organization’s most pressing strategic exposures and uncertainties and to focus the improvement of capabilities for managing them. The ERM infrastructure management has chosen to put in place drives progress toward this goal.

Companies in the early stages of developing their ERM infrastructure often set the foundation with a common language, a risk management oversight structure and an enterprisewide risk assessment process. Some companies have applied ERM within specific business units. And a few companies have evolved toward more advanced stages, such as the management of market and credit risks in financial institutions and the management of compliance risks in regulated industries. Wherever a company stands with respect to developing its risk management, directors and management would benefit from a dialogue around how capable the entity’s risk management needs to be with respect to each of its priority risks using the business strategy as a context.

The capability maturity model, introduced in Issue 3 of Volume 2 of The Bulletin (available at www.protiviti.com), provides a scale for evaluating the maturity of an organization’s risk management capabilities. The model provides five states for rating the process capability, ranging from “initial” to “optimizing.” It is a powerful tool for rating the enterprise’s capabilities in strategically vital risk areas, identifying gaps based on the
level of capability desired in specific areas, and shifting the
dialogue on operating metrics to incorporate appropriate
emphasis on process maturity. The ERM infrastructure
ensures that the rating process is fact-based and conducted
with integrity by the participating risk owners.

ERM key success factors
Companies evolving toward ERM should keep in mind that it is
a journey, not a destination. ERM can potentially represent a
sea change in organizational behavior, requiring a process of
building awareness, developing buy-in and ultimately driving
the acceptance of ownership throughout the entity. Change
enabler is, therefore, a significant aspect of an ERM initia-
tive because everyone’s perspective about risk varies.

To help ensure success, keep in mind the following “first prin-
ciples” when implementing ERM:

• Develop a compelling business case linking the ERM agen-
da to real priority business needs; garner support from the
top and manage progress against milestones over time.
• Obtain agreement on risk management objectives and the
appropriate ERM infrastructure; consider relevant cultural
issues and focus on enterprisewide application.

• Integrate risk management with the strategy-setting and
business planning process and implement early an effec-
tive enterprisewide risk assessment process.
• Clarify process ownership issues around who (a) makes
decisions with respect to the desired risk management
capabilities, (b) is responsible for designing the improved
capabilities to close significant gaps, and (c) monitors
progress and performance.
• Remember the purpose of ERM infrastructure is to provide
the appropriate oversight, control and discipline around
continuously improving risk management capabilities.
• The COSO ERM framework provides criteria against which
to benchmark the organization’s ERM capabilities.

Summary
Properly implemented, ERM can help organizations pursue
strategic growth opportunities with greater speed, skill and
confidence by aligning the organization’s risk taking with its
core competencies and risk appetite. Markets notice strategi-
cally focused organizations and will differentiate these organi-
zations by the quality and extent – real or perceived – of their
risk management capabilities.

Want to know more about enterprise risk management? Protiviti has just published a comprehensive resource guide titled Guide
to Enterprise Risk Management: Frequently Asked Questions, which is available for download at www.protiviti.com. This new
publication includes more than 160 questions and answers relating to ERM fundamentals, the COSO framework, roles and respon-
sibilities, the risk management oversight structure, getting started, building and enhancing risk management capabilities,
defining a compelling business case and many other topics. For a printed version of the book and discussion of opportunities
relating to implementing ERM, contact your nearest Protiviti office or call 888.556.7420.