

## Is Enterprise Risk Management an Imperative for the Financial Services Industry?

Enterprise Risk Management (ERM) – the holistic process of planning, organizing, leading and controlling the activities of an organization in order to minimize the effects of risk on its capital and earnings process<sup>1</sup> – is not a new concept. In fact, financial services companies have been among the leaders in developing and implementing ERM frameworks. In the 1980s, for example, many of the money center financial institutions made significant progress in migrating beyond their traditional silo approaches to risk management (where each major category of risk was separately managed) toward a portfolio view of risk. Their transitions, however, were not easy nor quickly effected, and other financial institutions tended to shy away from embarking on the ERM journey. Financial services companies continued to talk about ERM – intuitively, it seemed like the right approach – but eventually the buzz died down. Most financial services companies simply were unable to convince themselves of the value proposition of ERM. But, the buzz is back, and this time the outcome may be different.

In the two decades since the money center banks started focusing on ERM, the financial services industry has been subject to pervasive change – the kind that affects all sizes and types of financial services companies. For larger financial institutions, this change may have included developing new and sometimes complex product offerings, as well as expansion into new businesses and new geographies. For financial institutions

of every size, the effects of technology and regulation on how business is conducted are undeniable.

It's true that change is not limited to the financial services industry. In a survey of 76 senior executives of Fortune 1000 companies that was commissioned by Protiviti in September 2005, nearly five in 10 senior executives indicated that changes in their businesses in just the last two years have resulted in their organization's risk profile becoming more risky.<sup>2</sup> It's also true that companies of all types in the United States and other jurisdictions that have enacted corporate governance regulations continue to feel the pressure to avoid the mistakes of some of their competitors, and may be increasingly turning to ERM as a hallmark of a sound corporate governance program. Findings of another recent survey of board members of Fortune 100 companies<sup>3</sup> indicate a growing recognition by board members that historically they have tended to tackle risk issues on a case-by-case basis, and not on a systemic, holistic basis. While noting that the risk management practices of financial services companies are generally more robust than those in other industries, the survey's findings nonetheless disclose the following:

- Only 77.4 percent of directors say they fully understand the risk/return tradeoffs underlying the current strategy.
- Only 73.4 percent of directors say their companies fully manage risk.



### In This Issue:

Is Enterprise Risk Management an Imperative for the Financial Services Industry?

Scope of Routine Broker-Dealer Examinations is Broadening

Want to know more about Enterprise Risk Management?

<sup>1</sup> As defined at [www.whatis.com](http://www.whatis.com).

<sup>2</sup> *U.S. Risk Barometer: Survey of C-Level Executives with the Nation's Largest Companies*, available at [www.protiviti.com](http://www.protiviti.com).

<sup>3</sup> *The Role of U.S. Corporate Boards in Enterprise Risk Management*, a study by The Conference Board in conjunction with McKinsey & Company and KPMG's Audit Committee Institute, June 2006, available at [www.conference-board.org](http://www.conference-board.org).

- Only 59.3 percent of directors fully understand how business segments interact in the company's overall risk portfolio.
- Only 54 percent report their companies clearly have defined risk tolerance levels.
- Only 47.6 percent of boards rank key risks.
- Only 42 percent have formal practices and policies in place to address reputational risk.<sup>4</sup>

Beyond a director's concern with meeting his or her fiduciary responsibility – indeed, not a trivial consideration in this post-Sarbanes-Oxley Act environment – why else would a company decide to implement and maintain an ERM framework? ERM improves the capabilities of a company to anticipate and manage change. It provides the tools to protect and enhance enterprise value in three ways:<sup>5</sup>

- **It focuses the company on establishing sustainable competitive advantage.** ERM helps companies overcome silo behavior by aligning and integrating varying views of risk and enabling the enterprise to respond effectively 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 financial considerations.
- **It optimizes the cost of managing risk.** Through ERM, a company aggregates risk acceptance and transfer decisions, eliminates redundant activities, and determines the level of risk it is prepared to accept as it executes its business model.
- **It helps management improve business performance.** ERM assists management with reducing unacceptable performance variability and loss exposure by anticipating the impact of major events and developing responses to prevent those occurrences and/or manage their impact if they do occur.

If financial services companies still are not convinced of the benefits, there now may be another reason for them to consider developing and implementing an ERM framework: ERM increasingly is becoming a favorite topic of financial services regulators, led by the Federal Reserve Board. In recent speeches, former Governor Olson and Governor Bies highlighted the importance of financial institutions having “the tools and risk management processes that allow them to cope with inevitable changes”<sup>6</sup> and also noted that some financial institutions “may not be paying close enough attention to aggregation of exposures across the entire organization.”<sup>7</sup> Moreover, we are beginning to see specific ERM requirements being incorporated into regulatory

enforcement actions. We are quick to caution, however, that financial services companies that implement ERM only to satisfy their regulators may run the risk of missing the real benefits of ERM.

Financial services companies that decide to implement ERM would be well served to execute the following practical steps:<sup>8</sup>

1. **Conduct an Enterprise Risk Assessment (ERA).** ERM is a journey and a company needs to understand where that journey starts. An ERA identifies and prioritizes a company's risks, provides information about the current state of capabilities and aids in formulating effective risk responses.
2. **Articulate the ERM vision and value proposition using gaps around the priority risks.** Articulating the vision and value proposition provides the economic justification for embarking on the ERM journey. An ERM vision should be a shared view of the role of risk management in the organization and the capabilities needed to manage key risks. The greater the gap between the current state and the desired state of a company's risk management capabilities, the greater the ERM value proposition.
3. **Advance the risk management capabilities of the company for one or two of the primary risks.** Did the ERA suggest that the company had the most to gain in improving its management of operational risk and compliance risk? If so, then begin by improving risk management capabilities in those areas.
4. **Evaluate the existing ERM infrastructure capability and develop a strategy to advance it.** Determine what enhancements need to be made to the ERM infrastructure – the policies, processes, organization and reporting that support risk management capabilities – and develop a plan for implementing these enhancements. They may range from developing and implementing a common risk language to improving the company's quantification of risk through sophisticated modeling.
5. **Refine the ERA based on the preceding steps and continue to advance the risk management capabilities for other key risks.** The goal is to continue to improve risk management capabilities until all of the company's key risks have been addressed. But, even then, the journey will not be over, because changes in the company's business, in the marketplace, in regulation, in technology and elsewhere, will need to be considered continuously. However, the difference will be that now an ERM framework will be in place to allow these changes to be factored into the company's risk profile more easily and effectively.

<sup>4</sup> Idem.

<sup>5</sup> *The Bulletin*, Volume 2, Issue 6, “Enterprise Risk Management: Practical Implementation Advice,” available at [www.protiviti.com](http://www.protiviti.com).

<sup>6</sup> Remarks by former Governor Mark W. Olson at The Fiduciary and Investment Risk Management Association's Twentieth Anniversary Training Conference, Washington, D.C., April 10, 2006, available at [www.federalreserve.gov](http://www.federalreserve.gov).

<sup>7</sup> Remarks by Governor Susan Bies at the Financial Women's Association Washington Briefing, Washington, D.C., June 12, 2006, available at [www.federalreserve.gov](http://www.federalreserve.gov).

<sup>8</sup> *The Bulletin*, Volume 2, Issue 6, “Enterprise Risk Management: Practical Implementation Advice,” available at [www.protiviti.com](http://www.protiviti.com).

For financial services companies still on the fence, the views of some early adopters may be insightful. These views<sup>9</sup> support the proposition that ERM makes good business sense. It provides a “unifying framework” for managing risk as well as a competitive advantage. Also, it helps companies face

competitive pressures and solve major business issues. It even can help them with revenue growth. ERM well may be the imperative financial services companies need to remain competitive.

## ■ Scope of Routine Broker-Dealer Examinations is Broadening

For financial services companies, one of the main drivers of change is the regulatory environment. While regulatory changes are widespread across the entire financial services industry, securities firms, in particular, currently are dealing with a number of regulatory challenges.

Each broker-dealer firm is impacted differently by the requirements and expectations of the various securities regulators and other interested parties – the National Association of Securities Dealers (NASD), the Securities and Exchange Commission (SEC), the Exchanges and State Attorneys General. One of the main challenges a firm faces is maintaining a compliance program that is in-line with the myriad rules and regulations that apply. Changing rules and regulations impact nearly every facet of a firm’s operations. In a letter dated May 17, 2006, Robert Errico, executive vice president of member regulation for the NASD, outlined to member firms some of the issues they can expect to deal with in their upcoming examinations.

*In order to ensure that the firm’s supervisory system is designed reasonably to achieve compliance with applicable laws and regulations, the new rules require that a firm annually test its supervisory procedures.*

At the top of Mr. Errico’s list is supervision. For the first time, many broker-dealers will be examined for compliance with the new supervisory rules, NASD 3012 and 3013, which became effective last year. In order to ensure that the firm’s supervisory system is designed reasonably to achieve compliance with applicable laws and regulations, the new rules require that a firm annually test its supervisory procedures. Additionally, there is a new requirement that the CEO certify annually that these procedures are in place. The approach that firms have taken to comply with these new requirements varies significantly, from essentially maintaining the *status quo* to developing and implementing documentation similar to that used to support Sarbanes-Oxley Section 404 compliance (to evidence the compliance effort). The first round of compliance examinations for these requirements will occur in the summer of 2006; these examinations will provide the industry with definitive guidance as to what regulators believe constitutes adequate compliance.

The requirement that all firms develop and implement a written anti-money laundering (AML) program is another area that has continued to be a hot topic in the industry, and is receiving heightened attention now that the NASD and SEC have issued enforcement actions for noncompliance with AML program requirements. In May 2006, the NASD published its annual “Improving Examination Results,” which outlined the importance of an effective, written Customer Identification Program (CIP) that is tailored to the firm’s size and type of business. Also, effective as of March 6, 2006 is interpretive memo 3011, which was adopted to clarify the independent test requirements of the AML compliance program.

E-mail monitoring and retention also continue to be a focus for regulators and many compliance departments. Mr. Errico’s letter reiterates the requirement that all electronic correspondence, irrespective of where the message originated, must be captured and is subject to the supervision requirements. The NASD also has stated that its examining staff will be focusing on whether or not firms have complied with the requirement to file notification regarding their use of electronic storage media.

In addition to the previously outlined items, which apply to virtually every broker-dealer, there are several key areas that relate directly to sales practices and products offered by various firms. These items do not apply as broadly because they are dependant on the types of products and services that a firm offers. Some of the key areas receiving regulatory attention include: new product offerings, mutual fund sales practices and real estate investment trusts.

When the decision is made to offer a new product or service, a firm’s regulators tend to pay particular attention to the new activity. New products and services not only result in new regulatory requirements, but also often affect other operational areas such as accounting and finance. New policies and procedures must be put into place to ensure firmwide compliance with respect to the new product or service. Further, many new products are becoming more complex and often raise suitability questions; therefore, firms should expect examiners to review due diligence and customer-specific suitability reviews.

Breakpoints and share classes are two of the top challenges involved in mutual fund supervision. One of the areas that the NASD has noted as being of high importance

<sup>9</sup> “ERM Lessons Across Industries,” Tillinghast-Towers Perrin, March 2003, available at [www.irmi.com](http://www.irmi.com).

in mutual fund supervision is appropriate share classes and ensuring that customers are charged the correct sales fees. Firms are expected to analyze the effects of various fee structures on investor returns and then recommend the most appropriate share class for the customer. The examination staff intends to review mutual fund activity to ensure that reasonable fees are charged and appropriate recommendations are made.

Recently, Real Estate Investment Trusts (REITs) have been given a good deal of attention by the general investing public, partly because of the strong housing market. As with any hot investment, suitability questions arise and so the NASD has declared that REIT activities will be an area of

focus for this year. The regulators are planning to pay close attention to sales and compensation practices surrounding these investments.

These are only a sampling of some of the regulatory issues facing firms in the securities industry today. In order to mitigate compliance and reputation risk, it is paramount that broker-dealer firms ensure they are taking a firmwide risk-based approach to regulatory compliance. By maintaining a comprehensive compliance program that is tailored to a firm's unique set of products and activities, the compliance challenge can be managed much more successfully in today's constantly evolving regulatory environment.

## *Want to know more about Enterprise Risk Management?*

Read Protiviti's *Guide to Enterprise Risk Management: Frequently Asked Questions*, which is available in PDF format at [www.protiviti.com](http://www.protiviti.com). This publication includes more than 160 questions relating to ERM fundamentals, the COSO framework, roles and responsibilities, 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.



## For More Information ...

Protiviti is a leading provider of independent internal audit and business and technology risk consulting services. We help companies identify, measure and manage operational, technology-related, compliance and credit risks they face within their industry and throughout their systems and processes.

Protiviti's dedicated Financial Services Practice includes professionals with deep industry experience in banking, insurance, brokerage and investment companies. These financial services professionals can work with you to find approaches to help you improve and establish strategies for your business as changes in the industry and regulatory environment impact your organization.

For additional information about the issues reviewed in *FS Insights* or Protiviti's services, please contact:

Carol M. Beaumier  
Managing Director  
Office: 212.603.8337  
[carol.beaumier@protiviti.com](mailto:carol.beaumier@protiviti.com)

Scott Jones  
Managing Director  
Office: 213.327.1442  
[scott.jones@protiviti.com](mailto:scott.jones@protiviti.com)

Daniel O'Keefe  
Managing Director  
Office: 312.476.6388  
[daniel.okeefe@protiviti.com](mailto:daniel.okeefe@protiviti.com)

Carmen Rossiter  
Managing Director  
Office: 647.288.4917  
[carmen.rossiter@protiviti.com](mailto:carmen.rossiter@protiviti.com)