CNA

We can show you more.®

Enterprise Risk Management For Law Firms: A Discussion Paper

For a number of years, companies have been under pressure from regulators and shareholders to implement an integrated approach for assessing and measuring risks that may have a material impact on either the company's stock price or earnings. Many of these controls have been initiated to achieve compliance with regulations resulting from enactment of legislation such as the Sarbanes-Oxley Act of 2002 and the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010. However, audit committees and boards of directors are increasingly viewing Enterprise Risk Management (ERM) as a strategic function to provide tools for an organization's professional services, and business operations, as well as enhance shareholder value and earnings by identifying existing and emerging risks in order to implement systems and practices to manage them.

Enterprise risks in these areas continue to evolve and sometimes arise from unanticipated sources. These exposures can lead to devastating results, especially when handled ineffectively. Examples of such risks and events include:

- Demise of Arthur Andersen resulting from records management practices associated with Enron
- Phone hacking scandal at a News Corp. subsidiary
- Sexual abuse scandal at Penn State
- Gulf oil spill disaster
- Dissolution of large companies due to criminal fraud by management, including law firms, such as Dreier LLP

What is ERM and how does it differ from current risk management practices?

No specific definition of ERM applies to every enterprise. Rather, its purpose focuses upon identification and management of risks or events that could have a significant adverse impact on a firm. An effective ERM program has processes and controls in place to measure and systemically audit risks, while ensuring that business and professional vulnerabilities are anticipated and managed to permit the enterprise to fulfill its mission. A dynamic ERM program should clearly identify the individuals who have operational authority and responsibility for its implementation and results. Thus, every law firm should develop its own individual definition of ERM through an analysis of traditional and emerging risks to which it may be subject. Clearly, no two firms will have identical risk exposures.

Most law firms have defined rules of governance, as well as legal and regulatory risk management programs. However, they may not have developed an integrated approach to ERM. Many law firms look at insurable risks, which may include professional liability and property and casualty exposures. Law firms also tend to evaluate the available insurance products and determine whether such products provide value, based upon anticipated claims and the extent of coverage. For example, the implementation of loss prevention and disaster recovery procedures will enable the firm to expeditiously respond to both known and unanticipated events.

However, large companies and some professional service firms now evaluate all enterprise level risks -- whether or not insurable -- focusing upon foreseeable events that may significantly jeopardize the profitability or value of the enterprise. Some law firms whose existence is jeopardized due to claims arising out of financial mismanagement have reviewed and amended their procedures to protect the firm's assets, reputation and resources. Nevertheless, one question remains. How could these concerns have been mitigated through early identification and the implementation of targeted action plans designed to respond to such exposures?

How does ERM apply to law firms?

Increasingly, successful law firms employ systems and processes to track and trend key performance indicators similar to other industries, rather than operating as a group of professionals in a shared services organization. Decision-making authority and governance is then delegated by professional managers and operational committees, rather than residing with individual partners. In this context, ERM becomes an important mechanism for determining those risks that require firm governance, in lieu of remaining under the control of individual partners.

Some law firms, particularly those in the U.K., are currently utilizing ERM as an integral element of their management operations. Others are learning about the advantages associated with ERM. Lawyers are not immune from unexpected events with a significant financial, operational, and reputational impact upon their firms. In addition to fraud and unethical conduct, a multitude of risks have led to the dissolution of major law firms. These include disputes regarding compensation and retirement related to poorly drafted partnership agreements, inadequate diversification by industry or geography, partner defections and fiscal mismanagement. As a result, increasingly, law firm management teams are under partnership pressure to create a firm culture that will enhance revenue. Of equal importance, law firms also must implement measures to comply with data security and privacy requirements, and avoid potential conflicts of interest.

What are the principal areas of risk to which law firms are exposed?

Four broad risk exposures should be examined: Reputational/Business Risks, Regulatory Compliance Risks, Operational Risks, and Financial Risks.

Reputational and Business Risks:

- **Reputational**
    - Client dissatisfaction – Client dissatisfaction may arise from inadequate and/or ineffective communication, resulting in the inability to manage client expectations, and ill-defined parameters surrounding the scope of an engagement.
    - Attorney proficiency – Reputational harm may be affected through assignment of attorneys with a lack of specialized knowledge and experience relating to matters involved with an engagement, which also may encompass the ability to identify potential business and legal conflicts, observe information security parameters and pose data breach issues.
    - Public perception – What is the reputation of the law firm within the local community and beyond? Is the firm respected in its specified areas of practice? Have misconceptions arisen relative to the management of client matters, disciplinary actions, lawsuits filed by the firm, or negative publicity?
    - Employee perception – How do employees perceive the firm's reputation? Do employees view the firm as well-established, credible, and stable or do they perceive the environment as unstable?
    - Social media – What reputation has been established within social media? Do employees or clients post positive or negative comments about the firm in emails and blogs, or on Twitter® or Facebook®? What messages are being conveyed within these forums?
- **Business Risks**
    - Lateral hires
    - Mergers
    - Geographic expansion
    - Vendor usage
    - Lease agreements and warranties made to banks to induce them to provide working capital

Regulatory Compliance Risks:

- Regulatory risks include the breach of international, federal and state laws and regulations, resulting in governmental actions and/or litigation. Firms are thus susceptible to violations of money laundering rules, prohibited payments to parties on government restricted lists (Office of Foreign Assets Control), Foreign Corrupt Practice Act violations, bribery, ethical breaches, insider trading, criminal acts, and government enforcement actions pursued by U.S. agencies such as the Securities and Exchange Commission, the Internal Revenue Service, the U.S. Department of Justice and in the U.K., the Solicitors Regulatory Authority (SRA), as well as judicial sanctions and bar disciplinary actions.

Operational Risks:

- Partner/employee relations
    - Internal dissension caused by lack of faith in management or poor culture at the firm, such as lack of coherent uniform values
    - Partner defections, inequitable compensation or compensation that may result in professional conduct issues, as well as concerns about job security and earnings
    - Hostile work environment, including lawsuits based upon sexual harassment, discrimination, and other potential employment-related allegations

Financial Risks:

- Professional liability and other insurable risk exposures, especially insurance costs, uninsured losses due to lack of insurance and amounts payable within a self-insured retention
- Inadequacy of capital and profit margins, as well as uncollectible receivables
- Weak internal financial controls
- Fraud and embezzlement of firm and client assets
- Poor investment decisions

How does a firm approach ERM?

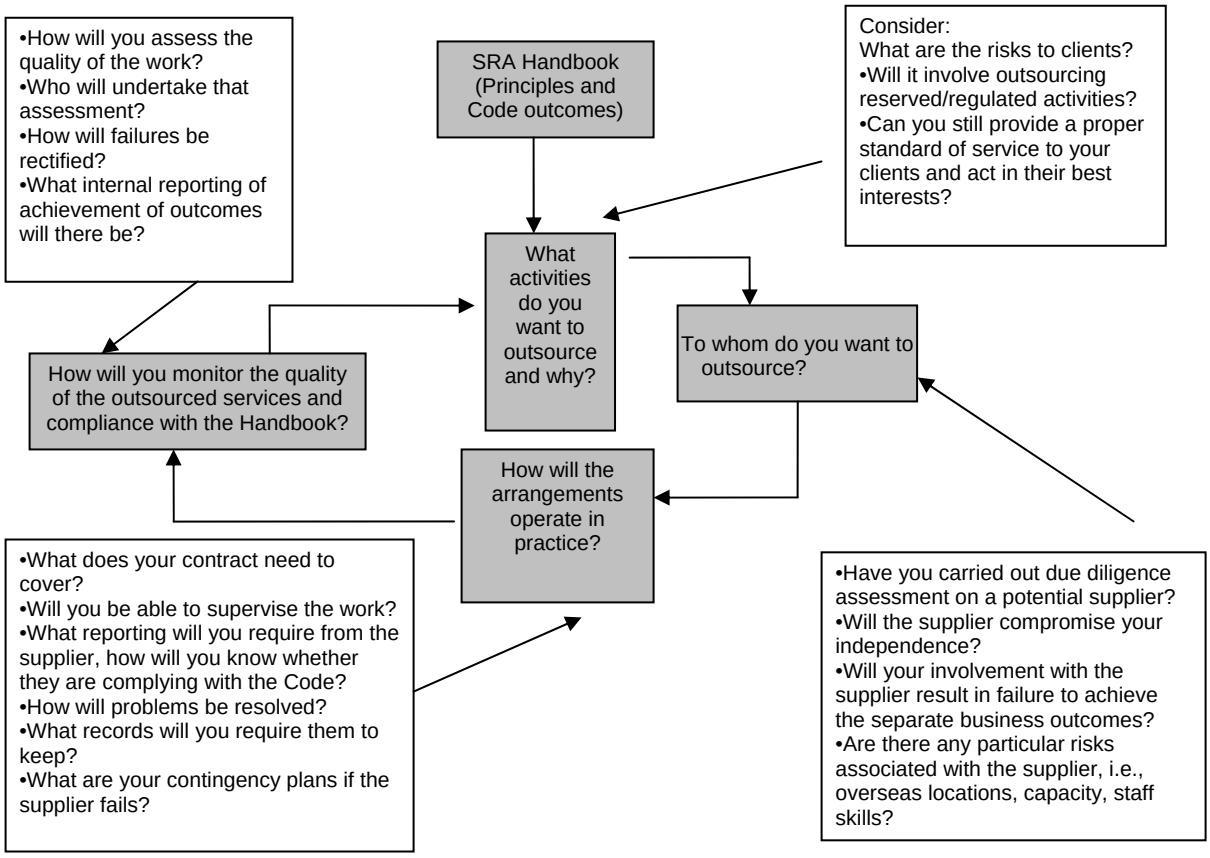
Organizational managers have initiated ERM to address various situations. First, they may adopt a reactive mode to a situation causing unintended consequences in an effort to preserve the institution on a going-forward basis. Second, management may perceive that a silo approach will enable it to identify and manage risk, as well as provide an opportunity for better communication and reduction in operating costs. Third, the use of available technology may optimize the implementation of an integrated approach. Finally, management may seek to formulate enhanced goals and objectives that encourage the creation of strategies to address operational concerns.

Most firms have a foundation of governance, including legal, risk management and financial controls. In addition, addressing the following questions and issues will assist you in achieving integration of current procedures and processes into a dynamic ERM model that will adapt to future exposures:

A. Who should be assigned to the study group, and ultimately, the risk control committee, responsible for design, implementation, and operation of ERM? Candidates to consider include the firm's general counsel, chief compliance officer, chief financial officer, chief risk officer and/or chief information officer, as well as a management committee member and practice leader(s). Often, an external consultant with experience in designing and implementing an ERM program can offer additional expertise.

B. Most organizations compile an inventory of current processes, responsibilities, policies and controls related to the risks outlined above, as well as the current costs involved. A useful technique may include the creation of a "map" outlining current responsibilities. Optimal practices already deployed should be highlighted in order to encourage those involved with the process. The enterprise also should confront the challenge of optimizing current resources in order to lower the cost of initiating the new ERM model.

Below is an example of mapping applied to outsourcing as outlined by the SRA.*



** Solicitors Regulation Authority "Outcomes-focused regulation at a glance" 10 Oct. 2011. Web 20 Jan. 2012*
https://sra.org.uk/solicitors/freedom-in-practice/OFR/ofr-quick-guide.page

C. What are the key risks that must be addressed, specifically those risks that can be monitored and measured? These exposures should be identified, as illustrated by the following examples:

- Client selection – What is a high-risk or low-risk client based upon the firm's definition (size, nature of business, nature of engagement)? Are high-risk clients monitored and are background checks of client management obtained?

- Lateral hires – How successful have they been, and how are they integrated into the firm?

- Partner compensation – What steps has the firm taken to ensure equitable partner compensation?

- Confidentiality – How can the firm provide assurance to clients that their information is maintained in a confidential manner?

How would success be measured and evaluated?

A critical element of ERM requires defined risk measurements resulting in the creation of systems to monitor results. In addition, an annual risk assessment prepared by the Risk Committee, and reviewed by the management committee or other interested parties, represents a major component of this effort. In order to successfully implement a comprehensive ERM program, the organization should create a structure, embracing management, partners, associates, and staff, strategically aligned to focus on effective procedures, practices and incentives targeted to the identification and management of risk. By implementing ERM throughout the organization, a universal knowledge and understanding of the potential risks will develop unified core principles, which reduce impediments to viable and pragmatic ERM implementation.

A. Measures:

Regarding client intake risk, verifiable measures should focus upon:

- whether there has been a conflict of interest check
- if needed, a client background check pertaining to financial and/or criminal matters
- whether there is an engagement letter on file
- whether the assigned attorney holds a financial interest in the proposed client
- whether the attorney will occupy a management position in a client's business transaction, and, if so, whether it was approved by law firm management
- the percentage of clients declined and the reasons for the declination
- whether billing codes were assigned to a client without customary approvals and, if so, why?
- routine file review to ensure compliance with established protocols and procedures

Regarding risks for lateral hires, measures should include:

- ensuring appropriate background checks have been conducted
- whether new engagement letters were executed

Regarding financial risks, measures should target:

- the percentage of accounts more than 90 days overdue for payment
- the number of partners who have departed from the firm (especially if covenants to banks have been executed)

B. Evaluation - Annual Audit:

An annual audit should be coordinated by the committee responsible for reporting on how the firm performed against designated measures. Such a review will assist in eliciting information relative to success or failure, including

designated activities the firm may undertake to achieve its goals. Additionally, comparisons with other firms, where the information is public, would also provide useful information to a risk committee.

The ultimate goal

An effective ERM program may make an enterprise a more attractive place for partners and employees to work. It will also provide value to clients by creating an atmosphere in which decisions are made based upon the best interests of both the client and the law firm. Additional benefits include making the firm a more desirable risk for insurers regarding terms and conditions of coverage, as well as conveying to regulators, investors, and lenders that the firm is appropriately managed and fiscally sound.

Summary

An ERM program is intended to enhance enterprise value in order to optimize the quality of professional services and business operations for both the client and the firm. By achieving a balance between the goals of the organization and its related risks, such initiatives will realize optimal effectiveness.

A comprehensive ERM program should:

1. Coordinate goals, strategy and risk appetite pertaining to the amount of retained risk a firm wishes to assume.

2. Identify risks a firm is willing to assume, those it believes may be mitigated, those it should not assume, and those that may become an appropriate subject of risk transfer.

3. Enable the firm to establish a framework to respond to anticipated events, such as recovering from a disaster or managing incidents or circumstances that may give rise to a claim.

4. Ensure the financial stability and growth of the firm.

While ERM is utilized as a risk management model in many industries, professional service firms typically have been reluctant to adopt a risk control framework that meets their compliance obligations while coordinating with the broader strategic goals of the enterprise. Law firms considering ERM should develop a risk management framework that pervades the firm culture in which all employees are accountable. They also should formulate internal controls that measure success against established benchmarks and, which assist partners in managing risk, encourage collaboration and enhance the reputation of the firm.

Stuart Pattison
Vice President, Underwriting
May 16, 2012