Chapter 1: An overview of law firm risk management

By David B. Cunningham

Introduction

Risk is the uncertainty caused by the occurrence of an event that might affect the achievement of objectives. The management of a law firm's risks involves decisions that are not simply about avoiding a negative impact, but also about pursuing a positive (but un-guaranteed) impact on business opportunities. Consequently, effective risk management not only mitigates losses, but can also positively contribute to the competitive standing of a firm. This tension between adverse risks and desirable business opportunities makes risk management an essential element of firm governance.

For most firms, the management of risk is an evolving discipline whose elements are at varying levels of maturity. The primary areas of risk relevant to a law firm are:

- Information technology (IT) risks;
- Financial risks;
- Practice management risks;
- Operational risks;
- Strategic risks; and
- Environmental risks.

While departmental and practice leaders have appreciation for risks in their own areas of responsibility, the view of a firm's full portfolio of risks is often fragmented. This chapter focuses on a holistic approach to managing risks, while subsequent chapters provide deeper examinations of particular areas of risk.

Benefits of effective risk management

Studies show that investors will pay a premium for public companies that are well governed. Despite its private ownership, the reasoning is no different for a law firm. Premiums come not only in the form of financial rewards, but also in attracting and retaining clients and high caliber talent.

Risk management as an element of good governance is still relatively new in law firms. Jim Jones, managing director of Hildebrandt and chairman of Hildebrandt Institute, notes that, "Ten years ago there were very few general counsels. Now, the overwhelming majority of AmLaw 200 firms have general counsels, and most of the AmLaw 100 roles are full time. And, their plates are very full."[1] In large, progressive law firms, other risk-specialist roles have appeared with responsibilities for loss prevention, security, and business continuity. In most firms, however, risk responsibilities have simply been added to the plates of existing leadership roles. These investments in directed effort reflect a growing acknowledgment of the business implications of risk management.

The benefits of effective risk management include fewer surprises, improved planning, improved information for decisions, enhanced reputation, protection for lawyers, and personal well-being. Specific benefits for firms can include the following.

Loss prevention

Loss prevention is the traditional focus of law firm risk management, notably mitigating

legal incidents, preventing malpractice claims, and ensuring the security of IT systems. This focus on avoidance of claims will continue to grow in importance, as evidenced by the American Bar Association's (ABA) *Profile of Legal Malpractice Claims: 2004-2007,*[2] which demonstrates that the largest claims are growing in both frequency and in dollar amount. These trends are expected to continue, as reflected by one law firm chief information officer (CIO) who observed that lawyers often overlook risk procedures in their scramble for work.

Cost savings

Beyond mitigating potential losses, effective risk management can also lower costs, in terms of professional liability insurance premiums, costs of and access to capital, and time commitments from committee members and risk staff. As Stuart Pattison, vice president of insurer CNA Global notes, "Many firms have high deductibles on their professional liability policies so reducing the number and size of claims has a direct effect on their bottom line."[3]

Departmental efficiencies

Proactively addressing risk areas can improve operational efficiency in business areas such as IT. Baker Robbins & Company's studies indicate that well-run IT departments not only address risks well but also maintain lower-than-median levels of staffing. Best of all, these well-run departments spend thousands of dollars less per lawyer per year than many of their less well-run peers.

Competitive edge

Perhaps the risk management holy grail is to address risk situations so well as to have a direct impact on the firm's competitive advantage. The downshift of the economy has fostered just such opportunities:

- **Growth in lateral talent** – Ability to attract and retain high caliber-talent; ability to clear conflicts appropriately and expeditiously (see later chapters for more detail); proper handling of new lawyer electronic materials; and reducing liability for matters brought to the firm by laterals.
- **Growth and retention of clients** – A minority, although a growing number, of corporate legal departments now request information on firm risk procedures. In a few recent situations, corporations have sent their own risk auditors to verify (not just ask about) the quality of law firm procedures. Increased corporate regulatory pressure, along with greater involvement from corporate purchasing departments, will continue to grow the opportunities for law firms who pay attention to the trend.
- **Quality of client relationships** – According to the Association of Corporate Counsel's Value Challenge,[4] legal departments have made it clear that firm matter management and communications are often below their expectations. These basic control elements, including budget reconciliations and status communications, are simple to implement and reap legal department loyalty.
- **Alternative fee arrangements** – Some legal departments are pressuring law firms to participate in the risks and successes of matters, spurring success-based fee arrangements. Indications show that firms that address their budgeting, staffing, and scope management processes will win more work, thus turning risk management into premium fees.

Quality of working environment

Higher-quality and more timely decision making, faster ability to respond to and

recover from crises, fewer conflicts, and lower stress levels contribute to an improved community and more engaged workforce.

Reputation

As John Shutkin, general counsel of Clifton Gunderson LLP (formerly general counsel of Shearman & Sterling), notes, "By far, the greatest risk to a professional services firm is to its reputation; that is its ultimate asset."[5]

Areas of risk in law firms

A common categorization of risk types helps in the understanding of risk. Agreement on definitions, scope, and categorization of risks enables a firm to take a portfolio view of its situation. The corporate risk management community has provided numerous risk models to categorize risks, although none are universally agreed upon across industries. Based on input from law firms, the risk categorization in Table 1 is adapted for a legal environment.

These risk areas can be directly mapped to leadership roles across the firm, along with broad responsibilities of a chief operating officer (COO) and general counsel. A general counsel (or designated risk partner) can be expected to be involved in any area when relevant issues and

Risk type	Example risks	Key roles
IT	*Systems:* Continuity, recovery, security, and access management *Data:* Confidentiality, integrity, ethical walls, retention, data protection, data transfers, hosting of third-party or client data *Third-party suppliers:* Maintenance/ support, contracts and outsourcing	CIO, general counsel
Financial	Audit, financial internal controls, financial transparency and disclosure, anti-money laundering, counter-terrorist financing, credit, firm investments, currency, and portfolio risks	Chief financial officer (CFO)
Practice management	Client relations, laterals, professional responsibilities (including malpractice, conflicts, records, and litigation support), and professional development risks	Practice leaders, general counsel, directors of conflicts, records, litigation support, library, and knowledge management
Strategic/corporate	Firm governance, risk management governance, reputational, marketing, and market risks	Managing partner, marketing director, general counsel
Operational	Employment, recruiting, fraud, damage to assets, and insurance mediation risks	Human resources (HR) director, COO, general counsel
Environmental	Natural disasters, epidemics, and resource access risks	COO, business continuity team

Table 1: Types of law firm risks

Role	Traditional risk responsibilities	Newer and emerging responsibilities
General counsel (GC)	This role now exists in the majority of AmLaw 200 firms. Risk partners and risk committees fill this role where the GC role does not exist.	Increasingly assuming a leading role in aggregating firm-wide risks and taking a proactive stance in identifying, treating, and monitoring risk areas. Close working relations with risk directors and CIO.
Risk directors (conflicts, records)	Clerical set-up roles for attorney decision making.	Significant administrative departments, with dotted-line responsibility to the general counsel. Working as part of a team to decide conflicts rather than simply process the information.
CIO or IT director	Technology uptime, disaster recovery, security, and IT contracts.	Traditional responsibilities, along with significant data management risks, including data transfer agreements, ethical walls, data protection, and legal holds. Increasingly risks and professional development in relation to knowledge management, e-discovery, conflicts, e-records management, new business intake, and search. In progressive firms, significant role alongside general counsel for enterprise risk management.
Director of security	Not traditionally present in law firms.	A limited number of these roles now exist in US law firms, many with a portfolio view, including IT, facilities, policies, human resources, and data management.
Chief risk officer (CRO)	Not traditionally present in law firms.	Although one of the fastest growing titles in corporate America, DLA Piper is the only law firm known to have a CRO on staff.
Business continuity planner (BCP)	Generally associated with the IT department, with a primary focus on IT continuity and recovery.	Often addressed via a virtual committee, BCP maintains its traditional elements while also contending with risks (such as H1N1, also known as swine flu) that may force the firm to continue operations for extended periods without physical proximity to other firm members. Only the largest firms have a dedicated BCP role. These roles are evolving from an IT focus to a firm-wide business focus.

Departmental directors	Risk management roles have been specific to each departmental scope, notably finance and HR risks.	Part of a firm-wide risk team, addressing cross-departmental risk issues including laterals, business continuity, and data confidentiality.
Insurance underwriters	Vary in the depth of assessments.	Some are taking a more active role in encouraging firms to undertake risk assessments and, in limited cases, providing a fund for doing so.
Clients	Traditionally passive on a firm's risk processes.	Increasingly active in asking questions about risk procedures. In very limited cases, taking an active role in auditing their biggest law firms.
Partners/lawyers	Active conflicts decisions, participant in paper-based records process, and minimal matter budgeting.	Conflicts decisions becoming more centralized, while records management has decentralized to the lawyers via e-mail. Matter scoping and cost controls becoming more prevalent. Some practices employing business managers.

Table 2: Law firm risk roles

exceptions arise. These roles are further outlined below.

The firm's exposure to these risks and the maturity in understanding them will vary not only by risk area, but also by office, department, practice area, and cultural boundaries.

Roles in risk management

As firms address the expanding breadth of issues and the coordination necessary across risk areas, roles and responsibilities are evolving. Table 2 outlines traditional responsibilities and the changes occurring in these roles.

A successful risk management environment

Unlike disciplines such as IT and human resources, law firm risk management rarely has its own department and departmental leadership. The general counsel or risk partner, as the focal point of legal risks, and the CIO might take the primary roles in leading a virtual team of firm risk stakeholders. When structured progressively, this team will take an 'enterprise' perspective of risk. Building a successful risk management environment provides a foundation for the subsequent assessment and treatment of risks.

Communicate and consult

Communications are a critical element of any successful risk management program. In a professional services environment, stakeholders include not only the firm managers but also the lawyers, secretaries, and departmental staff closest to the business transactions of the firm. An early responsibility in establishing a risk management program is to identify these stakeholders as they will be affected by risk incidents, will serve as eyes for identifying

risks, and may be constrained by risk mitigation measures or controls.

Communications and consultations aim to make risk management explicit, demonstrate how it adds value to the organization, and build trust that the multiple perspectives of the firm stakeholders are being considered. To accomplish these aims, proactive communications become a leading role for those in active risk management roles including policy advocacy and lawyer and staff education.

Establish the context

In establishing the risk management context, the firm needs to define the scope of its risks and the parameters in which to address them. It is impractical to undertake a full-firm assessment of all risks in a single gulp. By triaging the scope of the effort, a firm can select not only particular areas of risk, but particular geographic regions, groups of stakeholders, or business departments.

For example, a recent study of UK law firms by Marsh identified the top five risks facing law firms in order of severity as:[6]

- The bankruptcy or acquisition of significant clients;
- IT security;
- Pressure on fees and the need for 'instant' advice leading to claims;
- Conflicts of interest; and
- Errors made by staff/lawyers on complex, high-value transactions.

Based on client pressure, some law firms have prioritized the achievement of ISO 9001 or 27001 certification to address the risks and quality of their data management across the organization.

Promote self-assessment

To triage limited resources, a firm should embrace the discipline of risk self-assessment and delegate the workload to those closest to the risks. Risk self-assessment drives the responsibility and accountability of risk management to individual business process owners and lawyers and reinforces their responsibility and accountability for the risk areas they 'own.' An effective risk management program promotes 'diligent action' over increasing levels of assessment and establishes a report mechanism from process owners and lawyers upward in the firm.

Monitor and review

Ongoing review is necessary to ensure the firm's analysis remains relevant and its treatments are meeting expectations successfully. The firm should react to lessons learned and feedback from those who live with the risk measures on a daily basis.

Firms face a reality that upfront investments in risk assessment and treatment require continuing investments in education and compliance monitoring. To contain these ongoing efforts, considerations during risk treatment should include the degree to which compliance is automatically assessed or gated (where one cannot proceed until a quality condition is met) by the technology in place to support a risk process. Later chapters consider the role of technology and automation in greater detail.

Risk assessment process

Guidance on the management of risk is available related to sources such as the International Organization for Standardization (ISO) and Sarbanes-Oxley, although no standard is directly focused on the unique situations of professional service firms. While seemingly an obscure source, it is beneficial to look to the Australia/New Zealand AS/NZS 4360 standard for guidance;[7] it is acclaimed as the gold standard for a practical, easy to use, *risk-*

Figure 1: The risk assessment process

focused methodology. It is described more fully in the following pages. (An opposing *control-based* methodology seeks to identify missing or ineffective controls but can create a focus on an increasing level of controls rather than a focus on the business risks they were designed to mitigate.)

Risk-based approaches can be described as those producing significant amounts of information about risk events and their type, frequency, level, impact, and root cause. With the capture of proper risk information, a risk-based approach provides management with a perspective of the significance and likelihood of risk events and enables management to prioritize the materiality of mitigating controls.

The AS/NZS 4360 standard establishes three core aspects of the risk assessment process, as shown in Figure 1.

Identify risks

The objective of risk identification is to create a comprehensive list of the sources of risks and events that might affect the achievement of business objectives. Associated with each risk should be a source of risk, an incident, a consequence, a cause, existing controls, when the risk could occur, and where it could occur.

The approach to developing a comprehensive list can be any one or a combination of:

- Existing materials, such as strategic plans, audit reports, industry checklists, expert judgment, and personal experience;
- Team-based brainstorming or facilitated workshops; and
- Structured flow charting or system analysis.

The people involved must have detailed experience in the particular business discipline while also being able to step back and think creatively. An intrinsic aspect of identifying risks is to have an understanding of the firm's assets at risk and their corresponding value to the organization (stated financially or subjectively on a scale). If such an inventory does not exist, it should be created as a predecessor to the risk assessment.

Analyze risks

Risk analysis creates an understanding of the level and nature of risks, and the consequent priorities in addressing them. While risks can be evaluated using either a quantitative or a qualitative approach, quantitative assessments are atypical in law firms and should not be assumed to be superior. Qualitative assessments use scoring methods and the experience of staff and consultants

The risk: What can happen and how can it happen?	The consequence of an event happening		Adequacy of existing controls	Consequence rating	Likelihood rating	Level of risk	Risk priority
	Consequence	Likelihood					

Table 3: Example risk register

to arrive at a risk score. Although termed a qualitative approach, this method typically involves assigning a numerical value or relative ratings of the consequences and likelihood of risks.

Once the risk assessments are scored using a table formally termed a risk register (see Table 3), they should be sorted from highest to lowest. This allows organizations to address the highest risks first. This sorting is more practically done by area of risk and by business department, although the general counsel and peers should review the list from a firm-wide perspective.

Risk analysis can be conducted as part of a broad review, but also at the initiation of a new project or annual planning exercise.

Evaluate risks

The purpose of the risk evaluation is to make decisions, based on the outcomes of the risk analysis, about which risks need treatment and the priorities of these treatments. Risks are prioritized relative to the complete set and take into account known priorities and the supporting business requirements. A common approach is to divide risks into three categories: intolerable risks (no matter the potential opportunities, risk measures are necessary), grey-area risks (costs of risk measures and benefits of opportunities must be weighed), and negligible risks (no risk measures are necessary).

Risk treatment process

The objective of risk treatment is to change a risk to a level where the benefit outweighs the total cost of treatment, taking into account that costs and benefits have both monetary and intangible aspects.

Identify options

Identification of options begins by considering the existing guidelines for addressing a risk, if any exist. Law firms can refer to a wide variety of sources such as the ABA Model Rules of Professional Conduct,[8] the IT Infrastructure Library (ITIL),[9] and libraries of assessment materials from their professional liability insurers.

Since risks can have either negative or positive outcomes (which are not mutually exclusive), treatment considerations vary – see Table 4.

A comprehensive understanding is necessary of not only the *immediate* cause of the risk but also its underlying *root* cause. Addressing the root cause (including cultural issues) can be more effective than mitigating the risk itself.

Contingency planning is an important complement to these options, as it aims to help the firm recover from consequences within an agreed timeframe.

Evaluate and select options

The selection of treatment options depends on the clarification of treatment objectives. The objectives define the risks that are to be treated, the causes that the treatment should address, what the treatment should do, and the required performance. To determine which treatment options best meet the objectives, a firm might undertake a cost benefit analysis, although it is reasonable to do so in a qualitative manner.

A firm can also consider options that represent varying trade-offs between costs and benefits, as below:

- The best achievable result;
- A satisfactory (but not optimum) solution;
- The most cost-effective solution;
- The accepted practice (industry norm, which may or may not be good business practice); and
- The absolute minimum.

Risks with positive outcomes (opportunities)	Risks with negative outcomes
Actively seek the risk	Actively avoid the risk
Change the likelihood	Change the likelihood
Change the consequences	Change the consequences
Share the opportunity	Share the risk

Table 4: Responding to positive and negative risk outcomes

The evaluation of treatment options is focused on establishing new treatments, although it is also useful for reconsidering the effectiveness of existing measures.

Prepare and implement treatment plans

Treatment plans should identify responsibilities, the expected outcome of treatments, budgets, performance measures, and the review process. The plan requires communications and management involvement to create accountability and engagement amongst those affected.

As noted earlier, the treatment plan sets in place a cycle of monitoring and 'continuous improvement' review.

The predicament of legal risk standards

Risk assessment involves the identification, evaluation, and estimation of the levels of risks involved in a situation, their comparison against benchmarks or standards, and determination of an acceptable level of risk.

In the legal environment, however, risk benchmarks and standards are scarce, so anecdotal peer comparisons, friendly discussions, and periodic limited-distribution surveys provide practical substitutes. Law firms recognize that they face a predicament. As risks become more complex and risk management continues to mature, generally accepted principles or standards are more valuable across the industry. To remain competitive, however, most insurers generally do not want to impose tougher standards compared to other underwriters. Law firms, likewise, recognize the potential benefit in the definition of best practices, but resist defined standards for fear of incurring liability for any gaps they fail to address.

The most thorough risk standards today are those created by a handful of leading firms, by insurers such as MPC Insurance, Ltd., and by the very limited number of clients that audit their law firms directly. This increased willingness for clients to ensure firms are meeting their corporate risk measures and insurers' advancing diligence in risk assessments, combined with firms' continuing improvements in risk expertise, create a slow but fundamental shift toward industry-wide risk guidance.

As Adam Hansen, director of security for Sonnenschein, Nath & Rosenthal, reflects, "Firms are no longer exempt from meeting the risk management expectations of our biggest clients."[10]

David B. Cunningham is managing director at Baker Robbins & Company. He can be contacted at dcunningham@brco.com.

References

1. From the author's personal interview; quoted with permission.
2. Standing Committee on Lawyers' Professional Liability, Profile of Legal Malpractice Claims: 2004-2007, American Bar Association, 2008.

3. From the author's personal interview; quoted with permission.
4. See www.acc.com/valuechallenge/index.cfm.
5. From the author's personal interview; quoted with permission.
6. Marsh/*Legal Business*, 'Law firms risk management survey 2009'. Available at http://www.marsh.co.uk/research/2009/lawsurvey.php.
7. See www.riskmanagement.com.au for further details of the standard.
8. Center for Professional Responsibility, Model Rules of Professional Conduct 2009, American Bar Association, 2009. Also see http://www.abanet.org/cpr/mrpc/model_rules.html.
9. See www.itil-officialsite.com/.
10. From the author's personal interview; quoted with permission.