A Proposed Law Firm Information Security Assessment Framework

Work Group 3 Report
Law Firm Information Governance Symposium

IRON MOUNTAIN®

Contents

WORK GROUP 3

Executive Summary

This Work Group authored an eight-step Law Firm Information Security Assessment Framework to help guide firms in the development of IG standards that meet the requirements and expectations of the client — and still allow the flow of information within the firm.

- It is this Work Group's belief that this framework may be used to address such prevalent issues as:
  - Responding to clients, insurance carriers, and other third-party requests to understand how the firm protects client information
  - Determining guidelines regarding taxonomy in firm document management systems (DMS)
  - Assessing feasibility of new technology in the firm environment, such as cloud storage solutions
- The first phase of the framework discusses the importance of scoping the project, identifying a sponsor, and engaging stakeholders.
- Steps two through four are designed to help law firms analyze their risk exposure, determine what their risk tolerance is, and develop a risk mitigation strategy for any severe risks that have been identified.
- Steps five through eight offer best practices for developing a sound implementation plan and then executing and enforcing it. Firms can accomplish this by regularly auditing their processes and reassessing risk.

WORK GROUP 3

A Proposed Law Firm Information Security Assessment Framework

WORK GROUP PARTICIPANTS

Chair: Brianne Aul, Firm-wide Records Manager, Reed Smith LLP

Beth Faircloth, Director of Conflict Services, Jenner & Block LLP

Shawn Knight, Director of New Business Intake and Records, Vinson & Elkins LLP

Mark Lagodinski, CRM, Director of Records Management, Sidley Austin LLP

Brian Lynch, Director – Risk Practice, IntApp

Eric Mosca, CRM, Director of Operations, In Outsource

Paul Singleton, Director of Risk Management, Bingham McCutchen LLP

Susan Trombley, MLIS, Director, Consulting, Iron Mountain

INTRODUCTION

There is no one-size-fits-all approach to building a successful IG program, but the reasons and necessities of doing so are universal. Information within law firms is growing at an exponential rate, and there is an obligation to protect client information – as well as administrative information – and maintain confidentiality by restricting access to select individuals as appropriate.

However, the effort to protect and maintain information – physical and electronic – is not the responsibility of one individual or department, but rather a combined effort from every lawyer and each department within the firm. This is particularly true in today's mobile cultural, where new devices, the latest technology, and anytime-anywhere access to information is the expectation. The ability to manage these new security risks is paramount to the long-term health of the organization.

Some firms have a checklist on the intake process to include what security steps it will take, depending on the nature of a matter, and the types of documents that will be received. Other firms leverage ISO 27001 requirements and work with the General Counsel (GC) to come up with a standard for the firm. It is, however, generally accepted that security preparations need to begin at matter inception, and there needs to be a process established to manage access and control requests for information.

Firms must have formal documentation that defines the steps taken to protect common information. It needs to be flexible enough to accommodate for change, but thorough enough to address various contingencies.

While some clients may not know exactly what the measures should be, they believe their law firms will, or should, know what steps are needed to secure their information. Other clients have specific requirements for how their information should be handled. As such, it is important that a firm's Information Security strategy is documented in a way that it may be presented to a client, should they request it.

To do this, law firms need a consistent method, or framework, to help develop and organize the various departments and individuals required to adopt such a strategy. This Work Group established an eight-step Law Firm Information Security Assessment Framework (Figure 1) to help guide firms in the development of IG standards that meet the requirements and expectations of the client – and still allow the flow of information within the firm. The full framework outlined below includes detailed descriptions for each step in the process and offers law firms a practical guide for developing and tailoring an Information Security strategy for governing client and firm information.

It is this Work Group's belief that this framework may be used to address such prevalent issues as:

- Responding to clients, insurance carriers, and other third party requests to understand how the firm protects client information
- Determining guidelines regarding taxonomy in firm document management systems (DMS)
- Assessing feasibility of new technology in the firm environment, such as cloud storage solutions

However, it is important to keep in mind that this framework is not limited to such issues. Its structure provides significant flexibility so that it may be used for multiple security assessments across the firm environment.

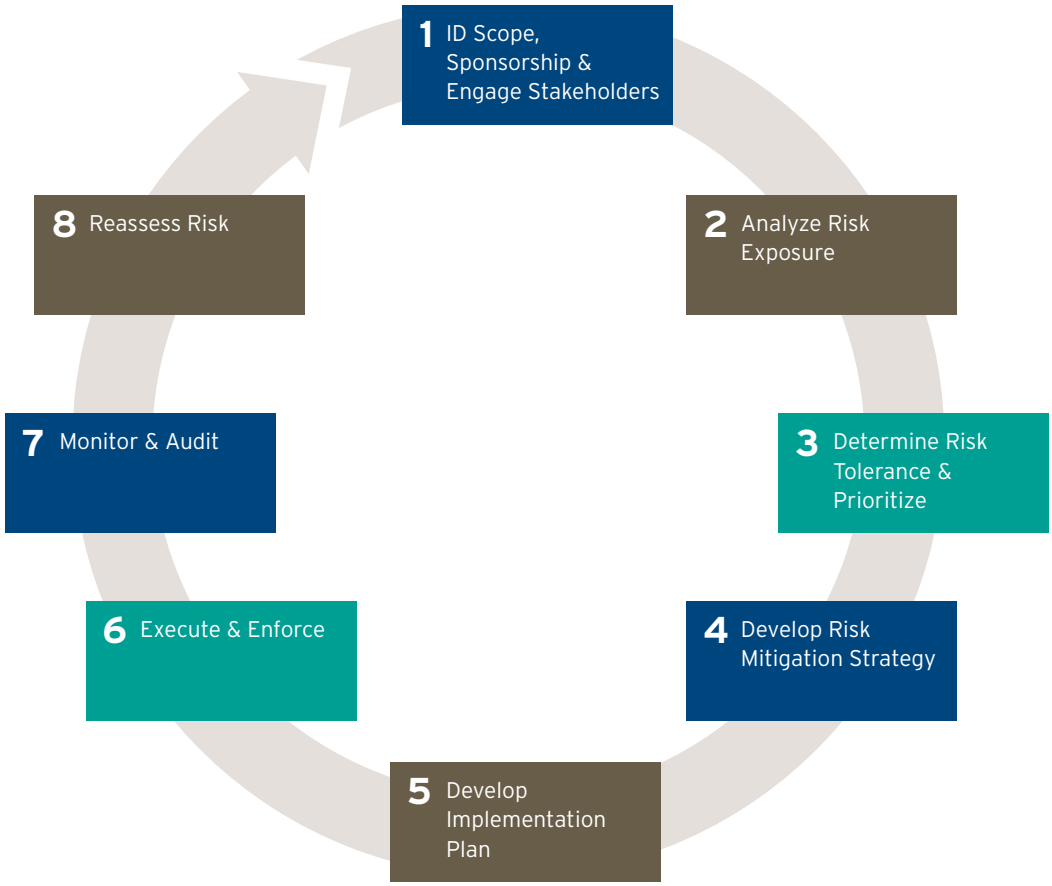

Figure 3.1: The Information Security Assessment Framework.

IDENTIFY SCOPE AND SPONSORSHIP AND ENGAGE STAKEHOLDERS

Step 1 of the Information Security Assessment Framework is to define the Information Security program objectives and scope of work. At this stage, the project Sponsor should be identified. The Sponsor will have primary responsibility for supporting and justifying the proposed change, whether it be new technology, process, etc., in the law firm environment ("the Proposed"). The role and responsibilities of the Sponsor will vary depending on the type of initiative.

DEFINING THE SCOPE

Defining the scope of work is critical to the success of the project, as it will lay the foundation for the remainder of the effort. As such, one should expect to invest the required time to plan and map out what security measures will be covered in the strategy, so as to ensure most, if not all, areas of potential risk are addressed.

This framework can be applied to an overall effort to gauge the firm's compliance with appropriate information security concerns, or it can be used to analyze specific issues (e.g., cloud computing solution or "bring your own" mobile devices policy.) A number of specific security questions are common among law firms and should be considered during the Step 1 discussions, including:

- What behavior is the firm attempting to control or address, and is this driven by client request, outside regulations, new technology, new policy or something else?
- Does this issue affect existing information across firm repositories or is this only an issue to be considered for the future?
- Does the issue or issues affect only a specific client's information, or all firm clients?
- Lawyers are expected to be on-call at anytime, from anywhere, so how does this issue impact lawyers working inside and outside of firm systems?
- Clients expect access to information at their fingertips, so how does one address or manage that expectation?
- Partners and teams need access to information, but not necessarily ALL partners and ALL teams. So, what is the best way to control access?

WHAT PARTIES SHOULD BE AT THE TABLE?

Step 1 should also identify the key internal stakeholders who would participate in the assessment and analysis and define their level of engagement and commitment to the project/program.

Roles crucial to managing Information Security include:

- **IT:** As the engineers of the firm's technological infrastructure, IT's understanding of how systems work within the current environment provides the logic and feasibility to justify or refute the Proposed.
- **Records and Information Management:** Records and Information Management (RIM) holds the responsibility for managing information through its expected lifecycle within the firm and can pose questions or concerns should the Proposed jeopardize the current information controls and retention in place.
- **Risk Management:** Risk Management understands the policies, procedures and legal regulations the firm is required to address. Typically serving as the liaison between the firm and its insurance carriers, Risk Management can evaluate the Proposed based upon the internal and external requirements.

- **General Counsel:** The GC's legal guidance and support is crucial to the approval of any new system or process. While he/she may not be involved with all of the discussions, his/her approval (or lack thereof) will likely determine the ultimate viability of the Proposed. The GC also represents the firm's ethical obligations and understands the firm's risk tolerance.
- **Knowledge Management:** KM promotes the collaboration and sharing of internal and external information amongst individuals in the firm — from staff, to partner, to client. KM can outline the benefits, or hindrances, to the Proposed regarding the expected flow and ease of access to information.
- **Project Management:** The Project Manager understands what other approved projects are on the timeline for a given period and can provide information regarding resources, budgets, and conflicting priorities.

ANALYZE THE FIRM'S RISK EXPOSURE BY PRACTICE AND JURISDICTION

Step 2 of the Information Security Assessment Framework is designed to determine a firm's risk exposure across the organization to ensure the Information Security strategy being developed is comprehensive and adequately protects the organization and its clients. It should cover all practices and jurisdictions, as appropriate.

Below is a checklist of risk exposure and regulations a large firm may consider when adopting the control measures needed within the framework:

- **Ethical Guidance:** What guidance has the ABA, state bar associations or a similar organization provided regarding the Proposed?
- **Client Requirements:** Has a client provided a clearly defined expectation regarding how its information needs to be maintained and secured?
- **Regulatory Compliance:** What laws or regulations regarding information privacy impact the Firm's defined practice areas and/or clients?
- **Standards:** Does the Proposed align with such published standards as ISO 27001?
- **Lawyer/Employee Access:** Should employee access be a one-size-fits-all approach, with security being dictated by ethical walls and the like, or should access be provided to certain groups or individuals on an as-needed basis?
- **Peer Approach:** What have other firms done, and has it been successful?

In considering the above, the project team should be able to review and determine the following:

- **Responsibility:** Who will be responsible for ensuring the Proposed will adhere to the guidelines set forth by the above?
- **Permissions:** What permissions should be granted/restricted in the systems?
- **Policies/Practices:** What policies or practices need to be adopted to align the Proposed with the above control measures?
- **Contracts and Agreements:** What security controls need to be clearly stated and agreed upon with vendors, clients, etc.?
- **Accessibility:** Who will have access to the Proposed (if new technology), and what type of access will they require?
- **Environmental Assessment:** Are there any other systems or practices in place that may conflict with the Proposed?
- **Tracking Audit History:** Will there be a record of user access and modification on the Proposed?
- **Breach Notification:** What requirements and procedures will be conducted in the event of information loss or unauthorized access to information?

- **Vulnerability Assessment:** Does the firm environment or infrastructure hinder the implementation of the Proposed?
- **Vendor Viability Assessment:** Does the vendor possess the appropriate qualifications, certifications, and credibility to sustain the Proposed throughout its lifecycle with the firm?
- **Disposition Methods Strategy (return, delete and transfer):** Does the Proposed allow for various disposition methods to occur in a manner that is defensible and secure?
- **Cultural Acceptability:** How will the Proposed be integrated in the firm's current environment? What are expected areas of resistance, and how can they be addressed proactively?

DETERMINE RISK TOLERANCE AND PRIORITIZE OPTIONS

Step 3 of the Information Security Assessment Framework is designed to identify and understand the firm's level of risk tolerance (whether that is formalized or not) and is necessary to determine specific risks and prioritize options for consideration.

While each firm's risk tolerance level is different, it's important to understand the "worst-case scenarios" with the Proposed, and determine potential effects if those scenarios become reality. In evaluating the risk tolerance, consider:

a. Identification of the risk

b. Probability of the risk occurring

c. Severity of the impacted risk to firm environment

d. Mitigation of the risk (if applicable), including:

   i. Cost of mitigation

   ii. Impact on lawyers and end users

   iii. Efficacy of mitigation technique

Once information has been identified, then the desired outcomes and benefits of the Proposed should be measured against those risks, and a decision should be made as to whether to move forward. Ultimately, each risk should have an "owner" assigned who has accepted the responsibility for preparing and handling the risk should it occur.

DEVELOP RISK MITIGATION STRATEGY

Step 4 of the Information Security Assessment Framework is designed to document a plan for mitigation of the risk identified in Step 2 and prioritized in Step 3, by considering the various elements included in a risk mitigation strategy.

Key elements to consider when developing a risk mitigation strategy include:

- **Access or Control Addressed:** Detail the type of access being granted or restricted, or the user behavior being enforced. General categories should include: New Technology, New Regulation, New Client Requirement, and New Leading Practice. Note the scope of access or control being limited and the desired outcome.
- **Policy:** Indicate updated policy documentation needed, including high-level policy points and necessary procedural documentation. Provide an estimate of time required for drafting and review of new documentation.
- **Training:** Detail the methodology for communicating new policies and procedures to end users, training required for each type of user and administrative role, and approximate duration of each training session. Detail the collateral documentation needed, such as Quick Reference Guides, training videos, or other documentation.

- **Infrastructure:** Detail the changes to Firm infrastructure necessary to implement control or technology. This may include physical hardware, software, deployment methodologies, tracking and reporting tools, or new administrative positions.
- **Resources (physical and other):** Document the resources that will be brought to bear on this risk mitigation approach. Resources may include research tools or subscriptions, outside auditors, or persons dedicating time to this effort. Note the expected time commitment weekly and/or on an ongoing basis, as well as any costs associated with utilization of this resource and the impact to existing job responsibilities.
- **High-Level Cost Analysis:** Provide a high-level analysis of all costs associated with implementation of risk management control. Include capital expenditures, personnel costs, operating expenses, software and hardware costs, etc.
- **Approval Needed:** Indicate the approval necessary to move forward with implementation of this risk management control. This may be internal or from an outside auditor or client.

It is assumed that conditional approval of the above items is provided before proceeding to Step 5: Develop Implementation Plan.

DEVELOP IMPLEMENTATION PLAN

Step 5 of the Information Security Assessment Framework is designed to help firms develop an implementation plan to roll out the Information Security strategy. This entire exercise should be done with the intent and the level of detail necessary to seek final approval to proceed with the implementation.

Key aspects to consider when developing the implementation plan can include:

- **Detailed Cost Analysis:** What is the breakdown of costs for new technology? Will there be a requirement for external consultants, or can this be performed in-house? What are budget restrictions?
- **Workflow Definition:** What new processes will be generated as a result of the Proposed?
- **Automation/Technology Considerations:** Can current technology support the Proposed, or will systems need to be purchased/updated/decommissioned as part of the process?
- **Identify Costs/Commitments and ROI:** Based upon the initial costs, as well as potential maintenance costs, etc., when will the expected ROI be realized by the firm?
- **Training and Adoption Plan:** What educational tools exist or need to be developed in preparations for the Proposed?
- **Develop Control Procedures:** What administrative-level functions are available with the Proposed, and who will be responsible for auditing and maintaining proper usage of the system?
- **Develop Metrics for Success:** How will the firm measure whether the new control has been successful in achieving the stated goal?

EXECUTE PLAN AND ENFORCE COMPLIANCE

Step 6 of the Information Security Assessment Framework is designed to help the project team track plan execution and enforce adherence to and compliance with the Information Security strategy. The following are two key areas to consider during the execution stage of the Information Security strategy:

COMMUNICATIONS PLAN

A well-crafted communications plan aims to integrate all aspects of the Information Security strategy into an orchestrated education and advocacy effort. This provides the foundation for proactive implementation allowing for efficient deployment of resources highlighting synergies and shared opportunities. Most importantly, a comprehensive and well executed plan has the power to transform the strategy from documented procedure into tangible practice, while building credibility and involvement from all members of the firm.

There are a number of key components to keep in mind when developing the plan:

- **Goal:** Having a firm grasp on the strategic goals of the Information Security program is crucial to the communications plan. Understand why you are launching the communication effort and what it is that you want from this goal. Briefly describe the Information Security program component, security risk or issue that needs to be communicated.
- **Spokesperson(s):** Establishing at the beginning the individuals who will be the chief authors and spokespersons will lead to consistent communication of content. The purpose of the exercise is to capture and maintain the audience's attention. Messages of shifting style or, worse, wavering subject matter will quickly confuse the audience and lead to mistrust.
- **Audiences:** Who is the primary target audience? Is it all lawyers, lawyers in a particular office or practice group? List the primary and secondary groups you are targeting. Do a thorough analysis of the people who will receive the messages. A good plan must know why a particular audience should hear the message. Understanding the background and characteristic components of the audience should lead to a clear appreciation of why the audience would want to hear the message and how they will be able to benefit from it.
- **Message:** Define the messages to be communicated to the various audiences. The key messages should be two-to-three overriding messages that you want to convey. The message may change depending on the audience, but there should be a few bullet points that get included into every conversation. Supporting messages may be more specific based on the audience or timing. A good communication plan will present messages several times. Each message might build upon the previous message and provide a little more information. (This "piqued interest" approach can keep the audience anticipating the next information installment.) Try to avoid explaining all details in any one message. This leads to lengthy content, and the audience will become bored, overwhelmed, or both. Good messages will frame the information security risk/challenge, present a solution, and offer actions. Give thought to branding. A consistent look and feel to your written communications creates a sense of dedication and professionalism.
- **Communication Tools and Channels:** Identify the tools and channels that you might use to communicate the message. Give consideration to your firm's existing communication infrastructure and leverage the available resources, including an intranet, newsletters, lunches, meetings, broadcast emails, town halls, or training sessions. Select those tools and/or channels that will have the greatest impact on your target audience(s). For example, short, pithy videos can capture quicker and stronger attention than email messages.

- **Milestones:** Keep in mind that an audience — who may be relied on to be active supporters, even participants — can quickly become overwhelmed or resistant when inundated with new content. This can be controlled by outlining realistic, yet achievable, project milestones in the communications plan.
- **Intended Result:** Identify the information security goals to be achieved. Why communicate? What do you want partners, associates, legal staff, or administrative staff to do as a result of hearing the message? What changes in behaviors are desired? Be certain the target audiences know what the result is and what the benefit will be. Being able to address the question "What's in it for me?" can reap quick rewards in the implementation.
- **Feedback:** Does the plan allow for feedback (suggestions, comments, etc.), or is it only intended to provide information?
- **Evaluation:** Assess how well the plan worked; this will help with future plans. How many people were reached? Who was reached? Were there any positive actions taken as a result of the communications plan? Identify ways to evaluate, and make sure some of those evaluation indicators include numbers and stats.

MEASURE AND REPORT

The project team should measure and report project progress to stakeholders and/or a steering committee — including project status, delays, issues log, and success/control procedures. In addition, the project team should complete an after-action review and capture the lessons learned during the process.

MONITOR AND AUDIT

Step 7 of the Information Security Assessment Framework will help firms monitor the usefulness of their controls, while auditing the effectiveness of their risk mitigation efforts. If controls are failing or circumstances change, firms may need to circle back to Stage 4 to revise the process.

The audit process at each firm will be different, so it's up to the culture of the company to define how they want to establish that process.

The frequency of audits should be determined by the value of documents and their circulation activity. Regardless of frequency, however, RIM should be involved to ensure the documents are properly handled over their lifecycle (Note: many firms are defining the electronic copy as the official copy).

RE-ASSESS RISK

The eighth step in the process is re-assessment. At this point, law firms should be systematic in tracking changes in the environment that will impact their risk strategy. Areas to monitor for changes include:

- New regulations
- New policy
- New offices/jurisdictions
- New technologies

Firms should establish automated notifications and schedule reminders to review their Information Security strategy, ensure it's still applicable, and that it's adequately meeting the expectations of the firm and its clients. If changes are required, circle back to Stage 1 and repeat the eight-step process.

745 Atlantic Avenue
Boston, MA 02111
800 899 IRON (4766)

ironmountain.com

ABOUT IRON MOUNTAIN. Iron Mountain Incorporated (NYSE: IRM) provides information management services that help organizations lower the costs, risks and inefficiencies of managing their physical and digital data. Founded in 1951, Iron Mountain manages billions of information assets, including backup and archival data, electronic records, document imaging, business records, secure shredding, and more, for organizations around the world. Visit the company Web site at www.ironmountain.com for more information.

US-LAW-EXT-WP-082412-003.3