A Proposed Law Firm Information Governance Framework

Work Group Reports
Law Firm Information Governance Symposium
Introduction and Background

Law firms are at a critical juncture: Clients have a spotlight on our information management, digital media is growing exponentially, and lawyers and clients and their information are increasingly mobile. Those of us who would ultimately form the Steering Committee recognized that the industry as a whole would benefit from collaborating on an Information Governance (IG) framework, rather than working individually in our silos. With the support of Iron Mountain, we set out to create an ongoing platform for collaborating on a law firm IG framework.

More than 20 law firm information management leaders converged in Chicago for the inaugural Law Firm Information Governance Symposium in May of 2012. For two days, we worked on drafting definitions, leading practices, templates, and strategies in the following Work Groups:

- **Work Group 1: Defining an Information Governance Framework** - What is it and how does it work in the law firm environment?
- **Work Group 2: It Takes a Village: Managing Information Governance** - How can departments work together to develop and run IG processes?
- **Work Group 3: A Proposed Law Firm Information Security Assessment Framework** - What are the best ways to assess and manage information risk and compliance?
- **Work Group 4: How to Move Forward with an Information Governance Program in a Law Firm** - How can firms develop strategies for communicating with lawyers about IG, developing staff proficiencies, and garnering resources for the journey?

The Symposium Steering Committee, Work Group participants, and Iron Mountain are pleased to provide the legal community with this proposed framework for law firm IG. This is by no means a definitive, final law firm IG framework. Rather, it is a first step in a journey to develop clarity and guidance on how to approach IG in the context of law firms. We encourage you to use this framework for strategic discussions at your firm on why and how to invest in IG. We also invite the broader legal community to join us in a dialogue to refine and develop this proposed framework.

---

### SYMPOSIUM STEERING COMMITTEE

- **Brianne Aul**  
  *Firm-wide Records Manager, Reed Smith LLP*

- **Bryn Bowen**  
  *Director Records and Information Management, Greenberg Traurig*

- **Leigh Isaacs**  
  *Director, Records and Information Management, Orrick, Herrington & Sutcliffe LLP*

- **Charlene Wacenske**  
  *Firm-wide Records Manager, Morrison & Foerster LLP*

- **Rudy Moliere**  
  *Director of Information Governance and Records Management, White & Case LLP*

- **Carolyn Casey**  
  *Sr. Manager, Legal Vertical, Iron Mountain*  
  **Symposium Leader**
EXECUTIVE SUMMARY .......................................................... 4
WORK GROUP 1: DEFINING AN INFORMATION GOVERNANCE FRAMEWORK
1.1 Overview .......................................................................... 6
1.2 Proposed Definition............................................................ 6
1.3 An Information Governance Advisory Board ................... 7
1.4 Information Governance Principles .................................... 7
1.5 Information Governance Processes ...................................... 8
  - Administrative Department Information
  - Client Information Requests
  - Document Preservation and Mandated Destruction
  - Firm Intellectual Property
  - IG Awareness
  - Information Security
  - IT Systems Administration
  - Matter Lifecycle Management
  - Matter Mobility
  - Mobile Devices/BYOD
  - RIM
  - Retention/Disposition
  - Third-Party Relationships
1.6 Information Governance Benefits ......................................... 9
WORK GROUP 2: IT TAKES A VILLAGE: MANAGING INFORMATION GOVERNANCE
2.1 Project Scope .................................................................... 10
2.2 Defining Roles and Responsibilities ...................................... 10
2.3 Defining a Process ............................................................. 13
2.4 Achieving Collaboration and Creating Partnerships .......... 13
2.5 Electronic Information Challenges ...................................... 16
  - Outside Influences
  - Internal Processes
  - Transfers
2.6 Moving Unstructured Information to a Structured Repository Environment .................................................. 18
  - Paper vs. Electronic
  - Transitory Files
2.7 Key Processes for Consideration ......................................... 20
  - Matter Mobility
  - Document Preservation and Mandated Destruction
  - Administrative Department Information
  - Third-Party Relationships
WORK GROUP 3: A PROPOSED LAW FIRM INFORMATION SECURITY ASSESSMENT FRAMEWORK
3.1 Introduction ...................................................................... 26
3.2 Identify Scope and Sponsorship and Engage Stakeholders .................................................. 28
  - Defining the Scope
  - What Parties Should Be at the Table?
3.3 Analyze the Firm’s Risk Exposure by Practice and Jurisdiction .................................................. 29
3.4 Determine Risk Tolerance and Prioritize Options .......... 30
3.5 Develop Risk Mitigation Strategy ......................................... 30
3.6 Develop Implementation Plan .............................................. 31
3.7 Execute Plan and Enforce Compliance ................................. 32
  - Communications Plan
  - Measure and Report
3.8 Monitor and Audit .............................................................. 33
3.9 Re-Assess Risk ................................................................. 33
WORK GROUP 4: HOW TO MOVE FORWARD WITH AN INFORMATION GOVERNANCE PROGRAM IN A LAW FIRM
4.1 Overview and Introduction .................................................. 34
  - Information Governance Moving Forward
4.2 IG Organizational Structure and Collaboration ............ 35
  - Roles of Other Groups
4.3 The IG Professional in Law Firms ......................................... 37
  - The Emerging Role of the IG Professional
  - Records Department Development
  - Within Records
  - Available Tools
  - IG Leadership Profile
4.4 Marketing .......................................................................... 40
  - Selling to Other Supporting Groups
  - Selling to Management
  - Selling to End Users
4.5 Communications ............................................................... 44
  - Setting Expectations
  - Messaging of IG Program
4.6 Metrics ............................................................................ 46
  - How Are We Doing It Now?
  - Value of Metrics
CONCLUSION ........................................................................... 49
Executive Summary


**WORK GROUP 1: DEFINING AN INFORMATION GOVERNANCE FRAMEWORK**

This Work Group's report provides an initial definition of Information Governance (IG) in a law firm and sets forth an overall framework. It presents IG as an evolving discipline that expands beyond the notion of traditional Records and Information Management (RIM), with a goal towards generating awareness of IG applications in the law firm environment.

- Proposes a definition and overall framework for law firm IG
- Recommends establishing an Advisory Board of firm leadership from across multiple functions to spearhead IG development and implementation
- Emphasizes an integrated, holistic IG program that uses policy-driven methods and applies IG principles consistently to key processes
- Presents 11 IG principles to guide all aspects of information creation, use, retrieval, maintenance, storage, and disposition by the firm
- Identifies 13 key processes that should be informed by the IG principles
- Asserts that a good IG program will help firms improve client services, mitigate risks, and reduce costs.

**WORK GROUP 2: IT TAKES A VILLAGE: MANAGING INFORMATION GOVERNANCE**

Work Group 2 tackles the intersection of departments at the firm in the IG program. Their report offers strategies for aligning Information Technology (IT), RIM, and Risk Management to work together, while defining processes that cross the traditional boundaries of these departments. This Work Group focused on identifying the role each department plays in IG – determining best practices to ensure all department goals are met, improving processes to provide the best client service, and reducing firm risk.

- Discusses the Advisory Board in depth, and the evolving role of the RIM professional in law firms
- Suggests strategies and tools for collaborating across departments
- Examines strategies and leading practices for electronic information challenges, including mobile devices, cloud-based storage, collaboration, and email retention
- Offers leading practices for moving unstructured information to a structured repository environment
- Provides strategies for managing document and email retention, transitory files, and electronically stored information
- Looks deeper at the key processes that must be guided by IG principles
- Offers leading practices for legal holds, transferring files in and out of firms, destruction practices, and administrative file management
WORK GROUP 3: A PROPOSED LAW FIRM INFORMATION SECURITY ASSESSMENT FRAMEWORK
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 4: HOW TO MOVE FORWARD WITH AN INFORMATION GOVERNANCE PROGRAM IN A LAW FIRM
Planning and executing an IG program are enormous steps for any law firm, but they are only the beginning. This Work Group report identifies and discusses ways law firms can best move forward with a new IG program to make it an ongoing process and part of the firm’s culture. The group makes use of visual maps in its presentation.

- Examines an ideal collaborative structure of an IG organization
- Discusses the emerging role of the IG professional in today’s law firms
- Maps stakeholders and audiences and offers best practices for marketing and communicating the IG program to specific audiences
- Explores metrics for an IG program and how to leverage them to make adjustments to the program and enable informed decision-making
1.1 OVERVIEW
This Work Group’s report provides an initial definition of Information Governance (IG) in a law firm and will set forth specific IG principles. It presents IG as an evolving discipline that expands beyond the notion of traditional Records and Information Management (RIM), with a goal towards generating awareness of IG applications in the law firm environment. The concepts in this Work Group 1 Report set the overall framework for IG in the law firm. Reports from Work Groups 2, 3, and 4 are components of this framework.

We envision our peers at law firms using this IG definition and framework to foster communication and strategic discussions in their law firms on what IG is, what benefits are gained, and why their firm should consider investments in IG.

1.2 PROPOSED DEFINITION
IG is an enterprise-wide approach to the management and protection of a law firm’s client and business information assets. An effective IG Program:

- Enables lawyers to meet their professional responsibility regarding client information,
- Recognizes an expanding set of regulatory and privacy requirements that apply to firm and client information,
- And relies upon a culture of participation and collaboration within the entire firm.

With IG, firms are better able to mitigate risk, improve client service through increased lawyer productivity, and reduce the cost of managing the information needed to support the efficient delivery of legal services.
1.3 AN INFORMATION GOVERNANCE ADVISORY BOARD
IG relies upon a core set of principles defined by the firm through an IG Advisory Group comprised of firm leadership and select stakeholders from the following disciplines:

- Administrative Management (HR, Finance, Marketing, etc.)
- Business Intelligence
- Information Security and Privacy
- Ethical/Legal Compliance
- Firm Intellectual Property
- IT System Administration/Infrastructure
- Knowledge Management
- Litigation Support
- Records and Information Management
- Risk Management

The support of senior executives is essential to the success of the IG principles that guide all aspects of information creation, use, retrieval, maintenance, storage, and disposition by the firm.

1.4 INFORMATION GOVERNANCE PRINCIPLES
Firms will need to establish a set of core principles that will permeate their IG program and processes, including:

- Educate all firm citizens regarding their IG duties and responsibilities.
- Confirm the authenticity and integrity of information.
- Recognize that the official record is electronic (assuming jurisdiction does not specify paper).
- Store information in a firm-approved system or record-keeping repository.
- Classify information under the correct client/matter/administrative code.
- Control the unnecessary proliferation of information.
- Disposition information when it reaches the end of its legal and operational usefulness.
- Secure client and firm confidential/personally identifiable information.
- Comply with subpoena, audit, and lawsuit requests for information.
- Conform all lines of business systems and practice group applications to IG standards.
- Ensure third parties who hold client or firm information comply with the firm’s IG standards.
1.5 INFORMATION GOVERNANCE PROCESSES

An integrated, holistic IG program uses policy-driven methods and applies IG Principles consistently to the following core law firm business processes:

- **Administrative Department Information**: The process of managing the law firm’s internal strategic and operational business information, including the preservation of vital records to ensure business continuity.

- **Client Information Requests**: The process of responding efficiently, consistently, and appropriately to client requests regarding IG, including Request for Proposal (RFP) responses, questionnaires, surveys, outside counsel guidelines, and audits.

- **Document Preservation and Mandated Destruction**: The process of preserving potentially responsive information, ensuring the suspension of scheduled disposition, and certifying custodial legal hold compliance during the discovery phase of litigation, investigations or audits. Also the destruction of information as mandated by the court or by agreement among parties.
- **Firm Intellectual Property**: The process of capturing and preserving the firm's knowledge and operational, creative, and historical artifacts that hold commercial, business, or strategic value (e.g., marketing and branding materials; KM Resources; contact information; firm initiative planning information; business development strategies; firm strategic plans; case management strategies; lateral lawyer growth records; financial information; firm policies and procedures).

- **IG Awareness**: The process of providing guidance, proactive education, and training to frontline support and local office administrators.

- **Information Security**: The process of controlling access to information, for example, via ethical walls and confidential access controls. It includes the protection of personally identifiable information (PII or PHI) and confidential client information and remote access to systems.

- **IT Systems Administration**: The process of providing guidance on systems selection and implementation, database administration, commissioning/decommissioning/developing systems, and information migration.

- **Matter Lifecycle Management**: The process of capturing new client or new matter information that is organized by areas of law and/or practice groups, including client engagement documentation and perpetuating the collection/distribution of firm authoritative information. The process of systematically deactivating matters in firm systems at the conclusion of formal representation (matter closing) is also part of this umbrella process.

- **Matter Mobility**: The process of moving matters and their associated information into and out of law firms; triggered by lateral moves, client terminations, and other events.

- **Mobile Devices/BYOD**: The process of providing guidance on compliance with firm policies/procedures with respect to acceptable use and security of firm-issued and personally owned devices (i.e., “bring your own device” or BYOD).

- **RIM**: The process of creating and periodically revising operational guidelines for managing information assets at the law firm, including file folder structures and taxonomy.

- **Retention/Disposition**: The process of applying lifecycle management practices to client and firm information, enacting disposition as authorized, and applying defensible disposition to legacy information.

- **Third-Party Relationships**: The process of ensuring consistent contracting language and defining Service Level Agreements that are compliant with firm policies regarding information access and protection.

### 1.6 INFORMATION GOVERNANCE BENEFITS

- **Improved Client Services**: IG provides rapid access to information that improves lawyer productivity, enhances knowledge sharing and collaboration, and results in faster service delivery to clients.

- **Risk Mitigation**: IG provides defensible policies, protected information, and compliance with legal and ethical requirements, thus reducing firm malpractice exposure and potential harm to reputation.

- **Cost Containment/Reduction**: IG provides opportunities for cost reduction in the areas of real estate, human resources, discovery, litigation, physical and electronic storage, insurance, technology, and legal and regulatory penalties (e.g., discovery penalties, malpractice awards, etc.).
WORK GROUP 2
It Takes a Village: Managing Information Governance

2.1 PROJECT SCOPE
The areas of Information Technology (IT), Records and Information Management (RIM), and Risk Management have all been speeding towards a common goal of Information Governance (IG). The challenge is finding a way for these groups to work together, while defining processes that cross the traditional boundaries of these departments. While some goals may be different between departments, all are seeking to provide seamless service to clients, ensure the integrity of information, and most importantly, minimize the exposure of their respective law firms.

This Work Group focused on identifying the role each department plays in IG — determining best practices to ensure all department goals are met, improving processes to provide the best client service, and reducing firm risk.

2.2 DEFINING ROLES AND RESPONSIBILITIES
IG is most typically comprised of a cross-functional Advisory Board including senior executives from the following groups:

WORK GROUP PARTICIPANTS
Chair: Charlene Wacenske, Firm-wide Records Manager, Morrison & Foerster LLP
Maureen Babcock, IT Business Operations Manager, Snell & Wilmer LLP
Patricia Fitzpatrick, Director of Practice Management, Katten Muchin Rosenman LLP
Matt Kivlin, Director of Product Management, Records Management, Iron Mountain
Dana Moore, Information Governance Compliance Manager, Foley Lardner LLP
David B. Steward, CRM – Director of Records, Husch Blackwell LLP

Figure 2.1: Key groups from which the cross-functional IG Advisory Board should be sourced.
In many firms, such programs as IG that require both compliance and auditing are formed under the direction of Legal Counsel, so that communications regarding reportable occurrences and events can be protected under privilege. It is common to have C-level executives as members of the IG Advisory Board delegate functional responsibility for the execution of the IG program to their direct reports across the organization. This practice is in line with the Principal of Accountability as defined by ARMA in their Generally Accepted Recordkeeping Principles (GARP).

In larger firms, the members of the IG Advisory Board may be expanded to include multiple members from the following broad categories:
- Legal Counsel
- General Counsel (in house)
- Professional Responsibility (advisory board members)
- Directors of Risk Management/Loss Prevention/Compliance
- RIM
- Director of Records and Information
- IT
- Chief Information Officer
- Chief Technology Officer
- Chief Security Officer
- Firm Management
- Chief Executive Officer
- Chief Operating Officer
- Executive Director
- Practice Area Chairs/Department Heads

Ultimately, someone from one of these groups needs to be in charge and assume the role of the “Information Governor.” This will be the person responsible for making sure the IG Advisory Board meets regularly, setting the agenda, and ensuring meeting minutes are memorialized. The Information Governor may also assign specific tasks to individuals on the Advisory Board based upon their areas of expertise. In a large firm, the Information Governor may be a dedicated position created specifically to fulfill this need. In smaller organizations, an existing executive on the IG Advisory Board could fulfill the role.

The members of each functional area will have designated responsibilities within the IG Advisory Board. Legal Counsel will provide professional opinions and guidance on ethical, legal, and regulatory provisions of the firm's IG policy. Reportable events that are a result of the compliance and auditing activities will need to be reviewed by Legal Counsel, so they can determine the appropriate actions to be taken.

IG is an accountability program designed to enforce a desired behavior. Firm Management will need to set the “tone from the top” by fully supporting the program as it is administered. In addition, Practice Area Chairs will need to make their lawyers mindful of the IG policies and the fact that all information, regardless of media or format, needs to be properly managed.
Traditional records departments are morphing into RIM groups and working more closely with their counterparts in IT than ever before. Historically, RIM focused solely on the management of unstructured information (i.e., paper files in most law firms). As the digital age has evolved, however, records professionals are being forced to learn new technologies and broaden their skill sets to allow them to participate in the management of structured information repositories (e.g., document management systems (DMS), email systems, information warehouses, etc.). This intradepartmental activity begins to blur the line in terms of who “owns” and “supports” these systems in most firms.

Some firms have attempted to solve this dilemma by establishing both a CIO and CTO position and dividing responsibilities between the two. When this happens, the RIM group typically reports up through the CIO. In these situations, the CIO develops an overarching strategy for the management of all information, business processes, and information lifecycle practices. Considerations must be given for how to handle each of the following:

- Metadata Management
- Personally Identifiable Information (PII)
- Retention and Disposition
- Knowledge Management
- Ethical and Legal Regulations
- eDiscovery Requirements
- Confidential Client Information
- Information Privacy and Security
- Intellectual Property (and digital rights thereof)
- Business Intelligence
- Storage Optimization and Archiving (across multiple platforms)

The CTO is given responsibility for the execution of system-related tasks, including:

- System Selection/Development
- System Implementation and Training
- System Maintenance and Support
- Decommissioning
- Monitoring for Information Breaches and Leakage
- Project Management

In many firms, the records department remains independent of the IT group. Regardless of whom Records reports to, the existing records staff needs to undergo a transformation in order to be able to fully support the official client file in an electronic format. This requires directors and managers of this group to educate their staff and assist them in developing new technical skills. Records professionals today need to be able to move and analyze information and to support any electronic information that the lawyer may bring to the firm with them.
The Information Governor also has responsibility to ensure client information is properly managed, and that all administrative departments within the firm are included in the IG policy framework and fully participate in the program. This will require ongoing communications with each supporting area and a full understanding of the various types of records generated by each group. Ongoing training, communications, and monitoring need to be in place in order for the IG program to be successful.

2.3 DEFINING A PROCESS

Having a clearly defined process is paramount to the application of a successful IG program. The scope of IG is broad, covering the management of all facets of information during a record’s lifecycle. All processes must be clearly defined and communicated in any successful IG program.

Knowing what information you have and where it resides are essential, especially if/when you are served with a direct or third-party subpoena to produce information. The Federal Rules of Civil Procedure (FRCP) describe the importance of this in detail and offer guidance on preparing your firm to produce electronically stored information (ESI) as part of discovery proceedings. For this reason, it is worthwhile to invest as much time as is necessary to identify and document in writing all current information repositories at your firm.

This ESI Data Map should be updated periodically to include new technologies as they are brought into the firm, and careful consideration should be given to information privacy, security, retention, and the other concerns previously described. This should be a collaborative discussion within a committee or group responsible for the consideration of IG within the firm.

Having clearly defined processes for other common events is also essential. Many firms develop electronic workflow systems that automate the review and approval of requests before any action is taken on events, such as legal holds, client file releases, invoking of retention rules, and confirmation of destruction orders.

2.4 ACHIEVING COLLABORATION AND CREATING PARTNERSHIPS

In today’s business environment, gaining a competitive advantage with new technologies or applications is critical to success. However, the need to balance new technologies with existing workloads can exert tremendous pressure on the entire organization.

The pressure is even greater when the requests come from lawyers who expect IT to do what it takes to make the latest technology a reality. This is especially true if the request comes directly from a client. The result is “application creep” – some estimates put the average number of applications per firm at 500.

Increasingly, IT is circling back to RIM and asking them to participate in the process, so information can be more effectively managed – no matter what technology platform lawyers or practice groups want to use. However, an informal alliance that may form between IT and RIM will not necessarily set firm policy when it comes to implementing new technologies. Rather, a firm’s policies and procedures are more often determined by the firm’s culture.

Generally speaking, the management styles of practice leaders shape company culture. These styles fall into two broad categories: firm-centric and fiefdoms. Although both categories have the same end goal of growing the group to provide revenue for the firm, their approaches may be quite different.
For practice groups that take a firm-centric approach, clients belong to the firm and the RIM policies are inclusive, allowing, in some cases, firm personnel to view all documents in the DMS. On the other hand, practice groups divided into fiefdoms tend to operate in silos and focus more on the individual practice of each lawyer than their firm-centric peers.

There has always been a struggle between ease of access and appropriate levels of information security. Law firms typically have a need to provide access to material for the purpose of knowledge management (KM). This includes the ability to retain continuity of retrieval for information as the people involved with a case change roles. Consideration must be given to preserve client confidentiality, as well as adhere to such compliance constraints as ethical walls and protective orders. Additionally, privacy rules may vary between jurisdictions, particularly for those firms that engage in international law.

Access to information within any environment is a continuum. On one end, retrieval of any document is restricted to only those few individuals with demonstrated need to know – a need that may expire as events change. On the other end, unfettered access is granted to the majority with few exceptions.

Most law firms tend to be somewhere in the middle of this continuum. Certain documents, folders, and matters may have restrictions on access, while the majority are “visible” should the individual choose to look. Restrictions may be applied by individuals to their own content or by a department responsible for entire collections.

There is a shift in the legal industry from information retention in the form of physical documents to electronic formats. This, combined with the power of enterprise search and retrieval, enables individuals broad and immediate access to firm and client information. Firms may discover that minimal restrictions on document security and powerful search tools may lead to embarrassing – and even unethical – situations. Each firm has to weigh client privacy and security needs with its own KM requirements in order to determine the level of information access it can tolerate.

Collaboration is key, particularly between IT and RIM. Successful collaboration is critical in the support of IG within the firm. Continuity in the firm’s IG approaches and policies presents a united view of information management to everyone in the firm; therefore, RIM and IT must be consistent in showing support of firm IG policy. More importantly, GC and firm leadership must agree to and support a strong IG position.

What’s more, IG policy must be enforced consistently. Firms must decide how and when to audit compliance, keeping in mind that it is better to monitor proactively for compliance, rather than wait for an incident to spur action. Timely and consistent audits will reveal areas for improvement, as well as demonstrate the firm’s commitment to excellence in the governance of information.
IG could be the way to break down department, practice group, and other information silos within a firm by focusing on the common goals of client service, information integrity, and security and minimizing firm exposures. A strong IG program will not only reduce risk, but also provide compelling business advantages by reducing physical and electronic storage costs, adding efficiencies to search and retrieval processes, and, ultimately, building a firm’s competitive advantage.

To reinforce the notion of collaboration, some leading-edge firms utilize force field analysis to help make decisions. Force field analysis is a framework for identifying the factors or forces that influence decision making. For example, when lawyers want a new technology fast, but IT already has a variety of key projects lined up, it can be helpful for the department to document the various elements of pressure that may influence priorities and sway the decision-making process.

Figure 2.2: A force field analysis of elements that push a firm toward change and those that hold a firm from change. Note that it is possible to apply weight to such an analysis. For example on a scale of one to five, Compliance may be a five, whereas Unrestricted Research might be a three. Adding the weighted elements can further benefit change management by illustrating not only what pushes or restricts, but how powerfully these forces affect the desired outcome.
2.5 ELECTRONIC INFORMATION CHALLENGES

Many firm lawyers and support staff use their email account as a repository, creating mailboxes far above acceptable size limitations, which drastically inhibits performance. Some firms have developed solutions and introduced policies that attempt to manage mailbox sizes, including everything from archiving and auto deletion to stopping the receipt of email when the mailbox has exceeded size limitations.

Other firms have tried to counteract the practice of using email as a filing system by implementing the use of the DMS as a central repository for client information, often as part of a “matter-centricity” implementation. The DMS provides the capabilities to secure documents, whether at the custodian level or as a default setting. In addition, the DMS provides better collaboration amongst teams working on the same matter, as well as easier avenues for locking down information for compliance activities, such as ethical/confidential walls, legal holds, and retention and destruction orders.

All firms will rely on continuous communication and education to drive adoption of new policies and procedures that will govern the use and storage of information.

- Information Types: In addition to client representation records, the firm generates a great deal of administrative information from key business units (e.g., HR, Accounting, Marketing, Conflicts, Firm Management, etc.).

- Information Locations: Some firms have designated official repositories for client records, be it a DMS or shared drive that is organized in some meaningful way (i.e., law department, client, matter). Others may leave the organization of information to the individual custodians, or acknowledge that their information is like the “Wild West” and is in dire need of a structured, multi-year plan to address it. Increasingly, this effort falls under the purview of those responsible for the RIM function.

OUTSIDE INFLUENCES

New Technology

Since clients often request the use of specific technologies or applications that may have a definite impact on the RIM program, collaboration between IT and RIM is necessary to address potential impacts on firm IG policy. This is because new technology can force a modification of current policy. For example, a technology such as Lync – a messaging application packaged with Windows – provides instant messaging (IM) functionality and can record IM conversation threads. As it is managed through email, this product may contradict existing IG policies, triggering modification of existing policy or the development of a new one.

Mobile Devices

Today’s increasingly tech-savvy associates and partners want access to information from any mobile device, which creates security challenges and concerns. While some firms establish policies that don’t allow employees to sync their smartphones, others do with provisions, including the ability to remotely “wipe” all information if the device is reported lost or stolen.

Cloud-based Storage and Collaboration

There is also an increasing push to leverage cloud-based services. The cloud creates an environment where firm and client documents reside outside of the firm’s network – a situation that can divorce the management and protection of a firm’s information from its own privacy and security policies. This becomes even more challenging if the firm doesn’t know exactly where the information is located (for example, if a cloud-based vendor does not have all of its servers located in the United States).
INTERNAL PROCESSES

Document Retention
How old is old? On one side, IT wants to delete information on the shared drive that has been inactive for years. However, from a RIM perspective, whether that file can be deleted depends entirely on what the information is related to and if the information has reached the end of its retention period.

First thing’s first: In order to delete information, you need to know its relationships. It is vital to develop an organized repository for firm information – both client and administrative – so it can be managed throughout its lifecycle. Then, develop a retention schedule that is ideally tied to the closed date of the matter for client records and the legal requirement or business need for administrative records.

Email Retention
Many firms view email more as a communication tool than a repository. Email retention is typically based on age; for example, email in the inbox or sent items may be retained for a pre-determined amount of time and deleted or archived if not filed into the official repository by that time.

Prior to implementing an email retention policy, it will be necessary to address legacy information and provide custodians an opportunity to file email records before they are permanently removed. Depending on the size of the firm, some forecast that auto-deleting email older than three years, for example, could free up more than a terabyte of space. Leading-edge firms are also beginning to adopt an automated matter-closing process – effectively applying retention policies across all repositories. This helps to keep firms compliant as clients and partners join and leave over time.

Transitory Files
There is growing concern regarding transitory files, such as voicemail, IM, and electronic dictation, as firms typically do not want to retain these file types for the long term. Some have set retention standards for the manual transcription of voicemail messages or implemented auto transcription technology for electronic dictation. With the increasing use of voice over internet protocol (VoIP) and voice and email integration, firms should plan a policy surrounding the retention of voice audio files in advance of implementation.

Retention schedules for the applications themselves are imperative. Retaining voicemail for up to 30 days before deleting automatically, or opting not to retain instant messages once the conversation window has been closed are just two examples of managing this type of information. Some firms use IM software that automatically saves conversations in the user’s mailbox, where they would be retained based on the email retention schedule. Once email is filed into a matter, the retention of these types of transitory files is typically managed at the matter level.

Backup Tapes
The back up of information is handled by the IT department in most firms and has associated procedures and policies that have probably been in place for some time. Whether the firm is using a tape or online backup solution, a system backup should be viewed as a disaster recovery resource to maintain business continuity, rather than a short- or long-term retention tool.

Most firms are using a combination of full, incremental, and differential backup for all information, however, the retention of these backups may differ depending on the database. For example, a monthly or yearly DMS backup may be retained for up to two years, while a backup of the email database has a retention period of just 30 days. Regardless of how your firm views it, the information in the backup may still be subject to discovery. Therefore, it is important to know what your backup and associated retention schedule is for all databases and review it every one to two years to ensure it is still meeting the needs of your firm.
TRANSFERS
Transferring electronically stored information (ESI) creates many challenges, many of which center around the collection and review of information relevant to the matters transitioning into or out of the firm.

When it comes to transferring information out of the firm, some adopt a policy that all of the related information, both physical and electronic, can be released and copies are not retained – thereby shifting the whole liability issue to the departing lawyer. Others retain a copy of the electronic information for the life of its retention or indefinitely where no retention policy exists.

There are also firms that take a stronger stance on information that is released. For example, a departing lawyer will be tasked with filing and organizing information and working with risk management to assess how in-depth a review needs to be, who will conduct the review, and if any exceptions to current processes can be made. This approach helps manage unreasonable demands of the departing lawyer.

It is essential to develop a systematic way to reduce materials that need to be reviewed and transferred. For example, when it comes to email some firms only focus on external messages, which can reduce the volume of email needing review by more than 50%.

It is equally important to develop an approach to review incoming ESI to ensure all information being loaded into firm systems is for active firm clients and is organized in accordance with firm guidelines. For incoming laterals, it is important to review firm applications and how they are used to manage information. Many firms have a meeting early on to talk about what new partners are bringing (format and content), discuss expectations for moving forward, and outline the policies so they are understood.

2.6 MOVING UNSTRUCTURED INFORMATION TO A STRUCTURED REPOSITORY ENVIRONMENT
Knowing where information is stored seems like a straightforward task. The reality is it’s one of the most complex endeavors for both IT and RIM professionals. Law firms have a history of unstructured information (i.e., electronic content that is not stored in a database or other fixed location, but on local or shared drives where this information is typically not organized or classified in any consistent way), and information repositories have grown organically based on the wants and needs of lawyers. Firms hoping to create structured repositories for unstructured information have numerous technical challenges and cultural hurdles they must overcome.

The first step is designing a new structured repository plan. This should include the following elements:

1. Selection of a business owner for each repository
2. Identification of document types for each repository
3. Creation of a searching structure for each repository
4. Creation of a lifecycle plan for each repository

Next is the identification of all known locations of the unstructured information. It may be commonly found on desktops or shared drives, email inboxes, or portable storage devices. To adequately identify the location of unstructured information, IT and RIM professionals must question the end users (e.g., lawyers, paralegals, and secretaries). Every lawyer practices in a unique fashion; therefore, where they store information may be unique, as well. From a cultural standpoint, they may be unwilling to participate in anything that will affect their current ways of managing the information within their personal practice.
Mapping the unstructured information to the new structured repository requires end user review. From an end user perspective, information review is never a popular prospect. After all, reviewing information from closed matters is not a billable task. The same goes for reviewing information from current matters when a lawyer would rather be actively working on it and billing time.

One way to handle this is to make a decision that information from all new matters must be incorporated into the new repositories in real time. Oftentimes, firms struggle to figure out the mapping component, which halts the project, but with this go-forward approach, firms can “stop the bleeding” of unstructured information. They can then devise a separate project to tackle the “old information.” Below is a list of considerations to help with their unstructured information challenges:

- **Recognize Changing Roles:** Lawyers have had to become increasingly self-sufficient due to increasing staffing ratios. The role of secretary is also changing, tending to focus less on document creation and more on billing and collections.

- **Engage Senior Managers:** It helps to get engagement from senior leadership. Firms where the GC is engaged actively tend to see that communication of firm policy and procedure gets to the lawyers and is noticed.

- **Establish Clear Policies:** Firms can no longer afford to say that people can save information wherever they want. From an IG perspective, firms must be able to articulate to the lawyers and HR where information goes and establish clear policies for a baseline.

**PAPER VS. ELECTRONIC**

Firms today operate in a hybrid environment of both paper and electronic documents. This section highlights a few key principles and leading practices related to governing all information, regardless of format:

- The same processes should be used for securing both paper and electronic information.

- Some firms are moving toward a common practice of encryption for all electronic documents. For these firms, encryption keys must be provided for all portable media storage and other transfer options, such as FTP sites, to maintain the protection of the original encryption. The necessity of having enforceable security procedures for USBs might be difficult to prove until an information security breach has occurred.

- Firm personnel must be educated on the dangers of information security breaches and the susceptibility of personal email for transferring or client information. In addition, information transfer sites that are not controlled and protected by the firm’s approved security measures (e.g., DropBox) can also expose firm or client information to outside parties and jeopardize client confidentiality.

- Vendors who manage the firm’s paper and electronic documents must have strict security protocols in place, which the firm should monitor from time to time.

**TRANSITORY FILES**

Transitory files, such as voicemail, IM, and electronic dictation files, are another growing concern, as they are files that companies do not typically want to retain long-term.

Increasingly, lawyers are communicating with clients using IM, which, depending on the software, could mean that it becomes discoverable evidence (especially in Lync, where IM chats are saved into the user’s email). For some firms, IM is only retained as long as the string is open. However, other firms operate a retention policy of keeping instant messages for 14 days – the same length as deleted email. The DM repository is much longer – up to one year. Other firms tie it into loss prevention once a year based on an 18-month rotation.
2.7 KEY PROCESSES FOR CONSIDERATION

MATTER MOBILITY
Incoming Lawyers and Clients

Attracting lateral partners with prestigious reputations and established books of business is the focus of every successful law firm. Likewise, attracting large clients with complex and/or ongoing legal needs produces strong revenue streams and is the mainstay for a firm’s longevity within the legal industry. But, both of these business drivers often result in challenges for those directly involved in IG.

When lateral partners are being courted by firms, the focus is on establishing a relationship and assuring the partner that he or she will be supported by the new firm. Firms often do not want to tarnish their initial discussions by talking about what materials the lateral partner can and can’t bring for fear of negatively affecting the partner’s view of the firm and its information-transition policies.

Years ago, firms that chose to broach this subject relied upon the cost of storing paper at off-site facilities to discourage lateral partners from bringing over an excessive amount of files. As IG has morphed to include an increasing volume of electronic files, however, that argument no longer carries the weight it once did. Many laterals have challenged this by claiming that electronic information storage is cheap, so it won’t cost nearly as much to store electronic records.

Some laterals may bring electronic information into the new firm on a flash drive or other type of storage device. Sometimes this is openly disclosed, other times it is not. Some firms ban the use of all external devices by locking down the USB ports, but this is an extreme measure that can prevent lawyers from working productively off-site — whether in a courtroom, at a deposition, or at a client’s location. All of these practices beg the question: What is a firm supposed to do?

Firms have a legal obligation to perform due diligence and clear potential conflicts for all new business. This includes brand-new clients for whom legal services have never been performed, as well as established clients for whom a new matter is being undertaken. Once potential conflicts have been cleared and/or waived, the client may instruct its former counsel to transfer existing files to the new firm. Most often this is communicated by the client to the prior firm in writing. Typically, the receiving firm gets a phone call alerting that a delivery is being made. The paper and electronic records are then integrated into the new firm by those directly involved in IG.

Firms also have a legal obligation to perform due diligence and clear potential conflicts for all lateral hires. This entails a comprehensive review of the candidates’ prior clients, the adverse parties involved in those clients’ matters, and the candidates’ prior employers (including law firms). Lateral hires should also be asked if they were exposed to any confidential information during their prior representations. Asking this question is essential to determining if they are bringing “imputed knowledge” into the new firm.

If the answer is yes, additional steps should be taken to ensure former client confidences won’t be breached. In these situations, it may be necessary to establish physical and electronic information barriers to protect the client information. This is where those involved in IG come into play. It is their job to ensure that all records, whether paper or electronic, are secured.

This is not meant to be a comprehensive list, but rather a deep dive into certain key processes that present particularly difficult IG challenges.
Many firms today use some form of wall software to enforce heightened security on information that is stored in the DMS and shared network drives (i.e., files shares used for electronic discovery), as well as to prevent requests that paper files be stored in the firm’s records management system (RMS). The wall software can also be configured to prevent those that should not be working on the matter from recording and billing time to it. Paper files may need to be labeled as “restricted” and segregated to prevent unauthorized access.

Whether it’s a new client, a new matter for an existing client, or a new lateral hire, all those involved in IG must work together to define a process that allows the firm to operate as a business, while maintaining a tolerable level of risk. RIM and IT will need to communicate with firm management and legal counsel to determine the level of acceptable risk. Some firms may be more willing than others to allow lateral hires to bring records of prior clients to the new firm. Oftentimes, those firms that do permit this make the argument that the imputed knowledge comes through the door with the lateral hire regardless of whether or not the paper or electronic file accompanies them. So, once you accept the lateral, you may be at no greater risk by allowing the records into the firm. Of course, the existence of that information and the ability of others to gain access to it should also be considered.

**Leading Practices**

- Create a global checklist across all administrative departments and an electronic workflow that has a point of responsibility for both incoming and outgoing legal and administrative staff. While the individual tasks may be different, the processes are actually very similar.

- Establish a segregated technical environment to do the review and transition of all information upon joining the firm, and identify what needs to be loaded onto the firm’s systems so conflicts can be identified and addressed.

- Acquire express, written authorization from the client before releasing any client information. Clients don’t need to give approval for new counsel to accept their information, as it’s implicit in the engagement letter with the new firm.

- When new partners join, only allow them to bring client information into the firm for those clients that will be transferred to the new firm. If a decision is made to bring in other (prior firm clients’) information, there needs to be a letter clarifying that there is no business relationship and a process outlining what’s going to happen to those files (electronic and physical) if the lawyer leaves the new firm. The prior firm clients should be entered in the conflict system and linked to the lateral partner as former clients from a prior firm (i.e., not as active clients of the new firm). Note that many firms, because of the imputation risk, do not allow this type of non-client information into the firm’s information systems in the first instance. As a result, alternate arrangements, including storing it offsite under a non-firm account, are often adopted.

- Information should be tagged and organized in (DMS) folders by client matter when incoming lawyers are coming aboard. It should also be organized using the new firm’s client matter number scheme. For clients that are being transferred to the new firm, Outlook folders from the prior firms could be transferred into their new firm email system as a temporary measure, until they can be absorbed in the firm’s DMS and/or electronic RMS.

- For personal matters, you should establish a work space on the DM. This space can also be used for client development and networking activities. Emphasize that this is not to be used for client material.

- Consider establishing a policy that one’s laptop or other external hard drive will be wiped 30 days after a person leaves.
Transferring Information in and out of the Firm

It doesn't matter if a client is transferring out of the firm or if a lawyer is leaving the firm; the process should be the same. No information (physical or electronic) should be transferred out of the firm without express authorization by the client. The firm's ethical and fiduciary duties are to the client, not to the partner. It is not enough for a departing partner to say that a client is moving with them. The client or the current firm must terminate the engagement (by disengaging the client or via court order).

Some firms are still very client-oriented and ask in the pre-meeting with new lawyers to organize their inbox before coming on board – not wanting them to dump their entire inbox into the system. The firm will audit a percentage of the email within the inbox in advance. If something is found that raises a red flag, then more email can be audited. Messages concerning partner compensation in the previous firm is one example of email that should not be accepted on the network of the new firm.

Other firms create an e-workspace where new partners have information on everything they need to do to get up and running within the first month. It's very open, so there's a lot of peer pressure, and there are typically dozens of tasks on the list – everything from getting a BlackBerry to acquiring business cards. From an IT perspective, having that list is important, as it allows the firm to see what still needs to be done.

Still other firms take a different approach where partner on-boarding is completed via training and development. Once new partners are through the door, they go through basic training. At the same time, the training coordinator schedules meetings between the incoming partner and each of the director-level people. (Associates go through the general employee process, but partners go through the more comprehensive on-boarding process.) For some firms, a similar process is used for a lawyer transferring out. Some of this has been driven by recent audits, which are forcing companies to track the checkout process more thoroughly.

In other firms, there is a lack of transparency around outgoing partners. For example, there are instances where IT hasn't known that the person was gone and the login remained active for a number of days. Everyone is still working in a silo, and this is a workflow where all of the various functions need to work together. There have also been instances where IT sets up an employee with an email account before they’ve even come on board.

Leading Practices

- Create a global checklist and a workflow that has a point of responsibility for both incoming and outgoing. While the individual tasks may be different, the processes are actually very similar. The same processes should also be considered for internal use.
- Establish a designated work environment to do the review and transition of all information upon joining, and identify what needs to be loaded onto the network systems, so conflicts can be identified and addressed.
- Acquire client authorization to the law firm to release the information. They don't need to give approval to have the information, as it’s implicit in the engagement letter.
- When new lawyers join a firm, they should only be allowed to bring information that relates to those clients who have agreed to move their active matters to the new firm with that lawyer. If a decision is made to bring in non-client information, there should be written confirmation that no business relationship exists between the new firm and the parties represented in or by that information. Processes outlining how that information will be managed, regardless of its form, must be documented and implemented. All non-clients should be entered into the new firm's conflict system and disclosed as former clients from a prior firm.
Lawyers coming into the new firm must be assisted in the process of assimilating their information into the approved repositories of the new firm. This necessarily covers both physical and electronic information. Any requested exceptions in information handling outside of firm policy should be approved by loss prevention counsel. Personal matters should be stored within a separate workspace on the DMS or to a specified network share. This space may also be used for the lawyer's client development and networking activities. Emphasize, however, that these areas are not to be used for the storage of client-related material.

For departing personnel, policy should detail required steps for handling information in possession of the departing individual, as well as information on the firm's network and external devices, such as laptops, hard drives, and home computers.

**Outgoing Transfers**

When it comes to transfers, firms need to look beyond just outgoing matters. With an outgoing lateral, IG needs to expand to include what happens to systems that are updated, how systems talk to each other (for example, between tickets created by HR and sent to technology), and the processes for other functional areas (i.e., H drive issues addressed, equipment gathered, etc.).

Most firms have a master checklist for when a lawyer leaves and the office manager knows that a lawyer is leaving. Oftentimes, however, when an employee or regular staff person leaves, the firm doesn’t have the same checklist in place. This means that RIM doesn't know until that person has already gone. What's more, some firms don't pay to send materials out of the door. Instead, they have a non-billable code where lawyers can put their time so that they can build a case as to why a client should pay.

**Leading Practices**

- Client transfers are client transfers and you shouldn't necessarily have a different process for a lateral lawyer. It's all about matter mobility.
- Nothing transfers without written client authorization (including email).
- Encrypt all FTP information.
- Don’t make copies of your records. IG people should be the ones who define the policy.
- As a general rule of thumb, if you wouldn't normally keep it as a physical copy, you should not be keeping electronic copies.

**Mergers**

In the case of a law firm merger, some firms sequester the information and information of the other firm. They have a process for handling the dictates, as well as soliciting confirmation of representation preference by each client. Information for clients that do not choose to be represented by the merged firm should be moved off the property.

In the case of mergers where one firm has well-defined processes to follow and the other does not, it is worthwhile to gather department leaders of each business unit to discuss the best approach. At times, this might appear to the firm with the well-defined processes that they have to start from scratch in getting stakeholder buy-in. In most cases, the final, approved approach will support the best interest of the newly merged firm.

**Leading Practices**

- Firms need to push hard to get some definitions around guiding principles: What are we going to keep? How far back are we going to go?
- During a merger, defined SLAs need to be put into place with the new merged entity.
- What the lawyer says is in the file gets released.
DOCUMENT PRESERVATION AND MANDATED DESTRUCTION

Legal Holds
There are typically three types of holds:

- **Third party:** Not against the firm.
- **Action Against the Firm:** IG is notified by the GC office whenever an issue is filed (i.e., claim or circumstance). This is required by the firm's insurance provider as notification of a potential insurance risk.
- **Internal Hold (based on termination or being sued by a former employee):** Most internal holds are handled confidentially and off the network, making them more challenging to handle.

Firms are looking for ways to manage holds and help lawyers collect required information, while at the same time ensuring that normal retention policies and practices do not destroy key information.

Leading Practices
- Firms should assign a gate keeper to be responsible for the legal holds (e.g., RIM, GC, etc.). This role is responsible for governing the process and making sure all other departments have completed the assigned tasks.
- A responsible lawyer should also participate in this process. There has to be a notice and an acknowledgement that a hold exists. A legal hold policy and process should be defined and awareness raised within the firm about what its impact on each department or practice group will be.
- Lawyers must manage their own information the same way they handle that of their clients (or as they counsel their clients to manage their own information). A means to identify all information storage locations and repositories must be implemented.
- Firms – in conjunction with their risk, compliance, or loss prevention teams – need to establish a process to lift holds when they are no longer required, with final documentation being provided to the IG group. There should be a periodic review of all holds based on an automated notification system, if possible. IG should implement regularly scheduled reviews of all existing holds with each managing lawyer to determine if there has been any change in the status of currently identified holds.
- Ideally, IG will drive the administrative functions of the hold, overseeing all aspects of its lifecycle.

Destruction Orders
Similar processes should be followed for destruction orders. In addition, a confirmation letter should be sent to the client outlining electronic retention and handling policies that the firm applies to its information. Backup tape retention duration and approved instances of access are two areas that are usually addressed in these communications.

There is an upward trend for destruction orders, as lawyers are realizing that they can give it to RIM to administer. It’s therefore important to spend a little more time up front defining the order. Lawyers will usually know how information needs to be categorized. Then firms need to take all records gathered, put them in a folder, and manually delete at the appropriate time.

Some firms communicate with IT to delete the electronic files out of the DMS (although not for Outlook). For paper files, they’ll contract with a storage facility to store the files and destroy them when appropriate – ultimately receiving a certification notice when it’s been done.

Leading Practices
- Implement a single IG process for gathering information (including transfers, legal holds, and destructions) with an additional component for destructions.


**ADMINISTRATIVE DEPARTMENT INFORMATION**

A firm's administrative information should also be governed by IG policy. This is not an area that has received great focus historically. Many firms have unmanaged repositories of administrative information. While the process will of necessity be different than the management of client information, firm administrative information should be governed by policy. It is up to each firm to determine if this warrants a closely managed approach or a simple document detailing the location of all such repositories firm-wide.

**Leading Practices**

- Information repositories are either official or transitory. All information should be reviewed from the official repository. Transitory databases are subsets of official ones and should be reviewed on a defined schedule for either deletion or inclusion into the official repository when the business need for keeping them has concluded.
- Transitory repositories may be stored on external media devices. No such device should be relied upon for long-term information retention.
- Be mindful of local information storage that may occur on devices, such as fax servers, photocopiers, and particularly on devices that are leased. Either have vendors guarantee in writing that information will be removed before the equipment is replaced, or require that the storage mediums within such units are physically destroyed prior to retirement.

**THIRD-PARTY RELATIONSHIPS**

**Contract Management**

As part of their vital records program, some firms store contracts in locked, fire-proof safes for which the RIM team or affiliated practice group is responsible. Some go further to require by policy that all contracts have to be recorded in an RMS or DMS. Contracts may be stored in DMS within a matter folder as a subfolder of their own or within an RMS similarly. Procurement may also sign off on contracts before they are filed.

**Leading Practices**

- Firms should limit or prevent contractors, vendors, and other non-firm personnel from DMS access. Firm or client information communicated via email to such parties should be done under firm-approved procedure that has been communicated clearly to them in advance.
- All contracts should be recorded in the RMS and tracked in a centralized governance system. Every contract should be approved by procurement before sending it for review to the appropriate lawyer.
3.1 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.
3.2 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.

### 3.3 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?

### 3.4 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.

### 3.5 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.

### 3.6 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?
3.7 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.

**3.8 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).

**3.9 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.
4.1 OVERVIEW AND INTRODUCTION

INFORMATION GOVERNANCE MOVING FORWARD

Planning and executing an Information Governance (IG) program are enormous steps for any law firm, but they are only the beginning. Once the core elements have been identified and are in place, the question becomes how do we best move forward to make IG an ongoing process and incorporate IG principles as a cultural function?

Although there isn’t a one-size-fits-all approach, successful IG programs have common denominators. The purpose of this Work Group was to identify, brainstorm, and discuss the common elements that can be applied universally to law firms – and develop practical visual maps that outline key roles and best practices that must be present to realize a thriving and effective IG program.

Because each firm is different (in culture, size, etc.), successfully advancing and promoting an IG Program is complex and not always intuitive and straight-forward. We focused on five common components and considerations to aid in this effort:

- Organizational Structure and Collaboration
- The Role of the IG Professional
- Marketing of the IG Program
- Communications
- The Value and Importance of Metrics

This report is organized around these five components, and is accompanied by 13 visual maps that illustrate these considerations, how an IG program impacts the firm, and best practices for incremental progress. These maps represent the initial brainstorming efforts of the group and are intended to serve as a starting point for strategic
planning efforts. It is important to note that these components are not intended to be a linear, chronological process that is “one and done.” Rather, they are a collection of activities and initiatives that need to happen simultaneously, in a coordinated approach that is consistent with firm culture, size, and existing program status.

4.2 IG ORGANIZATIONAL STRUCTURE AND COLLABORATION

The success of an IG program depends on two primary factors: structure and collaboration. It is important to recognize that everyone in the firm will be applying IG principles to how information is created, used, and retained. We are proposing that there be an IG organization (along with an established governing body) and staff in law firms. Most firms do not have a dedicated “IG Department.” An IG Department may well consist of a group of existing individuals who play a role in various subsets of IG functions. Once established (whether formally or informally), the IG department or team must play a central role and be empowered to lead the charge in developing a program.

Organizational alignment of the IG Department is key, and given the diversity across firms, must be positioned where it can be most productive within the organization. As identified by Work Groups 1 and 2, collaboration is a must for IG success; therefore the IG Department must be able to facilitate collaboration across the entire firm. The traditional siloed approach (i.e., practice group-centric with each administrative department working independently of one another) that is common within law firms will not be effective when the goal is developing a structured system and process to manage an ever-growing volume of information.

ROLES OF OTHER GROUPS

Work Group 2 focused on the various groups within the firm that play a role in IG initiatives. To achieve success in advancing an IG program, the firm must bring the right people to the table to facilitate a common understanding of the roles they play, the challenges they face, intersecting projects and initiatives, and what it takes to work together. The goal should be to create unity and enhance communication among and across the various departments or practice groups to drive IG forward.
Managing this effort can be challenging, and many firms are bringing new, non-legal talent into the firm – such as MBAs – with the business acumen to bridge the gap between the various groups by filtering out white noise and focusing on collaboration, training, and efficiency. The idea is to infuse IG into the fabric of the organization with minimal disruption – although growing pains are to be expected. If executed properly, the IG effort will enable lawyers to work the way they want and need to in order to efficiently serve clients, while still achieving the goals required for a successful IG Program.

Ideally, IG is the glue that connects information silos across the firm. It offers the strategy, knowledge, and tactical experience to facilitate action and develop holistic solutions to today’s information challenges. Figure 2 illustrates in additional detail the specific functions performed by the various support groups within the firm, the intersection with information management, and the overall connecting points with IG efforts. Special attention should be given to the challenges and benefits and opportunities for strategic partnerships between groups. It is important that each firm understand its own strengths and weaknesses to clearly establish unique challenges and benefits that may affect the successful implementation of IG efforts.

Figure 4.2: A map of the various roles across the organization that are critical to IG Program development.
4.3 THE IG PROFESSIONAL IN LAW FIRMS
THE EMERGING ROLE OF THE IG PROFESSIONAL

IG is a rapidly growing discipline in all organizations. Law firms are no different in this regard. As the industry works to better define IG, there is also much discussion surrounding the necessary qualities and traits of those individuals charged with developing and supporting it. Much like the traditional records manager evolved “accidentally,” current owners and leaders in IG have inherited, willingly or unwillingly, the role of providing IG guidance.

Law firms are recognizing the value of IG and leveraging various resources from within (such as records managers, IT leaders, eDiscovery experts, etc.) to meet the need. Firms may find that IG “talent” exists within their organization, and empowering, educating and mentoring those individuals may fill the need for IG leadership. In other instances, it may be in the firm’s best interest to create a dedicated position and seek the right individual from outside the firm to fill it.

RECORDS DEPARTMENT DEVELOPMENT

IG involves effectively and efficiently managing information and documents, which are two functions and areas of expertise traditionally held by a law firm’s records department. As such, the records manager plays a critical role in the development of an IG Program.

The institutional knowledge of a firm’s processes, procedures, structure, and culture is vital to driving a successful program. However, implementing IG requires change for everyone involved, including Records and Information Management (RIM) personnel. There may be significant alterations to what is considered a traditional job description for records managers. With change comes great opportunity, and firms need to support it by providing the tools, resources, and professional development that facilitates and encourages the evolving role of RIM.

Figure 4.3: A map of the new role of the RIM department and ways to encourage professional development.
As in recent years, the role of RIM will be highly visible and on the front lines of the change management process. Only through continuous training, ongoing educational opportunities, and a sound understanding of new technology can a firm develop its records manager and supporting staff to fulfill the expanded role – and empower him or her to make decisions, offer informed recommendations, provide strategic input, and take action regarding the IG program. The transition from “records professional” to “IG professional,” will not always be an easy task, but by evaluating current skill-sets versus the ability to transform and evolve, you can separate the wheat from the chaff.

Figure 3 specifically references strategies to effectively “sell” the concept of IG to records staff who may be deeply engrained in legacy processes and philosophies. It’s important to emphasize the personal and professional benefits to the individual in addition to the firm and provide encouragement and reinforcement for behaviors and skills that promote IG and related efforts.

**WITHIN RECORDS**

As important as it is for the records department to “up their game” when supporting and interacting with other groups, it is equally important for them to evolve their skills in working within the department. The skill set of the records professional has been traditionally paper-based, involved linear thinking, and not required an abundance of analytical skills. Records teams must recognize the importance of working collaboratively with one another in addition to supporting their “customers.” Records department personnel should receive training that goes beyond records-specific policies and procedures or their supporting software systems. They should be cross-trained to understand various tasks within the department and department interdependencies as they relate to IG, and have a clear understanding of the firm’s business and strategy.

![Figure 4.4: A map of key considerations when developing a messaging strategy to those supporting IG efforts. Existing job descriptions, for example, should be reviewed for relevancy to the evolving skills and expertise required and in many instances new job descriptions will be necessary. In order to attract and retain IG professionals, positions should match the strategic plan and provide a path for mobility.](image-url)
AVAILABLE TOOLS

Implementing and driving an IG program is a large undertaking that can be a daunting task—especially when one looks at the organizational changes that will take place. For records managers, the pressure of dealing with the evolving nature of that position, while helping drive the larger change-management effort across the organization, can be intense and overwhelming. The answer is to train continuously and leverage the various tools that are available to make this transition easier and more manageable. Focused educational efforts should be offered, in addition to making self-help opportunities available.

Myriad professional organizations boast resources, trainings, and certifications that can help prepare records professionals for this opportunity. There are also vendors, consultants, peer networks, and even social media sites that provide tools and support to help develop the skills required to lead the IG effort (see Figure 5).

It is likely the evolution of IG will help records managers look beyond their current role and facilitate a culture of continuous learning for themselves and within the firm. Most importantly, the growing IG community should provide guidance on where to look for information resources and training and encourage professional development. There is a plethora of information available, and many of these resources are free of charge. Given the sheer volume of information and resources available, it is important to seek out credible sources/organizations.

Figure 4.5: A map of the various professional development tools available to records managers and others.
**IG LEADERSHIP PROFILE**

An IG Program is only as good as the firm's commitment to enforce the policy and supporting processes. Many law firms have few, if any, consequences for non-compliance, especially if the culprit is a top billing lawyer. But it's important to remember that an IG program is a partnership between all facets of the organization, and one partner's disregard for the policy will impact the profitability and risk exposure of the entire firm. As such, strong leadership from a governing, authoritative body enforcing IG policy is critical to the success of the program.

An IG leader must possess the ability to enforce a change management effort, be aware of all other initiatives across the organization, command respect, and have the skills to communicate with all levels of the firm. Although few people will display all of the traits and characteristics identified as ideal, there is a general profile of what constitutes a good IG leader (see Figure 6).

![Figure 4.6: A general profile for an ideal IG leader.](image)

**4.4 MARKETING**

Marketing, or “selling”, the IG Program to all levels of the organization is necessary to promote adoption. Doing this, however, requires a strategic approach, an understanding of business operations, and the ability to communicate the benefits – “What's in it for me?” – to each group within the firm. A clear understanding of the individual benefits will generate enthusiasm for, and active participation, IG efforts.

There are three main audiences that should be considered when devising the strategy:

- Supporting Groups (e.g., IT, HR, Litigation Support, Knowledge Management, etc.)
- Management (Lawyer and C-Level Administrative)
- End Users
SELLING TO OTHER SUPPORTING GROUPS

True adoption of the IG Program requires buy-in from all groups within the firm – from finance, marketing, and IT to human resources, knowledge management, litigation support, and new business intake. This is a challenging task that requires a delicate balance of clearly defined benefits for the various stakeholders with the greater interests of the firm at large.

To do this, IG must have both a clear understanding of the policies and procedures and solid, professional relationships and alliances with all groups – lawyers and non-lawyers – within the firm. The success of the program depends on the ability to communicate the mutually beneficial nature of IG. The “What’s in it for me?” is different for every department; therefore it is important to have a good understanding of motivators and areas of mutual benefit (see Figure 7).

Figure 4.7: A map of the groups within the firm that are critical to a successful program and key considerations for each.
SELLING TO MANAGEMENT

Without buy-in and sign-off from management, the IG Program will not materialize, let alone thrive. More so than any other group within the firm, the effort of selling IG to management and senior executives is an exercise in demonstrating the expected return on the investment (see Figure 8). Arguably, the endorsement from management should be a precursor to conducting outreach to other groups.

As with any new initiative, there is a cost to getting started, so gaining approval (and a champion) for the effort means clearly stating the business case and articulating the increasingly vital role IG plays in the firm — from client, branding, risk, and cost savings perspectives. Most importantly, the entire effort needs to be supported with metrics. The viability of the IG Program depends on the ability to generate information that justifies the cost, effort, and use of resources that could otherwise be allocated to revenue-generating activities. Selling to end users and other groups must be done carefully. Marketing an IG Program to management requires a unique strategy, and appropriate planning is key. It is important to understand firm priorities, culture, and business plans. Roadblocks are inevitable, but it is helpful to identify as many of them as possible in advance of communication efforts or outreach.

Figure 4.8: A map illustrating the various elements that should be considered before selling the IG Program to management.
SELLING TO END USERS

When selling to end users, it’s important to stress how IG programs will generate value for everyone—from lawyers, secretaries, and directors to managers and legal support professionals. It is also important to remember that implementing an IG Program can create confusion, as well as the perception of adding extra work for end users. Change is intimidating by nature, so messaging is important. Success depends on communicating the ways that IG will make their jobs easier and create value. Users will be looking to IG for ways to increase their efficiency, create value for clients, solve problems, and improve productivity (see Figure 9).

Figure 4.9: A map illustrating the various elements that should be considered when selling to end users.
4.5 COMMUNICATIONS

Communications within a law firm can be challenging for a variety of reasons, not the least of which are firm politics and culture. As a result, those charged with sending the message may be either too busy or reluctant to do so for other reasons. In addition, the organizational structure of some firms makes clear, top-down communications challenging at best. Bridging communication gaps is crucial to the success of the program. However, the effort must be strategic, organized, and comprehensive to effectively reach all people at all levels within the firm. An effective communications strategy will vary from firm to firm, so it is important to not only develop a careful strategy as to what will be communicated, but also who is best equipped to deliver the communication.

SETTING EXPECTATIONS

There is always a fair amount of fear and uncertainty when initiating an IG Program, so it is critical to set the expectations early and ensure the plan is communicated effectively to both internal and external stakeholders.

For your internal stakeholders, it should be made clear that this is a partnership with reciprocal properties (i.e., IG will do this, and in return you are expected to do this, and as a result we will mutually benefit). An ideal program will leverage opportunities to make the life of the end user easier. It is also important to communicate what can and will be measured, how it will be monitored, how it will be enforced, and the repercussions for non-compliance. These same expectations must be established with external stakeholders, as well, including existing clients, new firms, acquisitions, and incoming and departing lawyers. Various factors play a role, such as personnel resources, budget, and service-level expectations.

There will be resistance to the effort, and many of those reservations will stem from such concerns as changes to day-to-day practices, budget, and upfront expenses. However, the present value of the effort is worth more than the time and money that will be spent on the same effort in the future. The proliferation of information in law firms continues to grow. That said, it is impractical and impossible to attempt to “boil the ocean” by addressing all IG issues at once. An incremental approach is recommended, and, once decided, plans and expectations should be communicated appropriately. The longer a firm waits to act, the greater the negative impact will be down the road (see Figure 10).

Figure 4.10: A map illustrating what should be considered when communicating the expectations of the IG Program.
MESSAGING OF IG PROGRAM

Poorly communicating about your IG Program can yield worse results than not communicating the plan at all. For this reason, investing time to develop short, concise, and targeted messages that are tailored for individual segments of the firm is essential. Communications that are effective for one group may not resonate with another. Also, keep in mind the “What’s in it for me?” mentality of the various groups, and be sure to demonstrate the net gain of their investment – in time, resources, and budget – by presenting a strong business case for the IG effort.

Although the message will take on a slightly different tone depending on what practice or administrative group is being addressed, it is important to consistently emphasize the expected universal benefits. These include reducing expenses, increasing efficiencies, meeting compliance, sharing knowledge, and mitigating risk. It is critical to back up these benefits with metrics that demonstrate progress and incremental improvements. The next section covers metrics in more detail, but keep in mind that, regardless of audience, the who, what, when, where, why, and how of IG must be clearly articulated and consistently emphasized.

A law firm’s first priority is serving its clients; therefore, it is important to keep the focus on delivering value to the client. In the end, the IG effort is as much about practicing law as it is fulfilling an ethical and fiduciary duty to protect clients’ information. A properly designed IG program can reap benefits in many areas (see Figure 11).

Figure 4.11: A map illustrating the critical elements of messaging the IG Program.
4.6 METRICS

Metrics are the backbone of a successful IG initiative. Whether you are capturing cost savings or performance information, the ability to gather meaningful information and generate reports that demonstrate the program’s progress and successes is, perhaps, the most important element of the overall program. Without metrics, the initiative will never grow legs or retain the support required – from senior leadership or end users – to sustain it, leaving it ultimately sidelined by other more immediate initiatives. As mentioned previously, development and maintenance of an IG program are not “one and done” tasks. Careful analysis of metrics allows for informed, calculated decision making to support necessary changes to the program and the continued reiteration of the value IG brings.

Capturing the information, however, is a huge undertaking and requires a deliberate and strategic approach – not to mention buy-in and cooperation from every level of the firm.

HOW ARE WE DOING IT NOW?

In order to implement an effective IG Program (future state), it is necessary conduct an “as is” assessment to determine exactly how you are managing your efforts now (current state) – a challenging task that must involve input and participation from the entire firm.

The difficulty in mapping your current state is the sheer number of moving parts that must be identified and then quantified as a baseline. This effort includes everything from technology, system usage, and help desk tickets to processes, policies, and storage. Once you have identified strategic goals and objectives, determined what you need to measure, and accurately captured how you are doing it today, you will have a framework for demonstrating the success of the IG effort. It is important to note that no two firms are in the same stage of development, nor do they have the same priorities. As such, each firm needs to perform an individual analysis and evaluation to chart their own course. Often, a strategy of first identifying and addressing “low hanging fruit” to gain momentum and prove incremental results will garner support and buy-in for additional IG efforts (see Figure 12).

Figure 4.12: A map illustrating the components to consider when assessing your current state.
VALUE OF METRICS

The value of metrics can't be overstated when establishing an IG Program. By benchmarking at the onset of the program, firms provide a baseline against which future metrics will be compared. It is essential that the application of an IG program can show both reduced costs and risk to the organization. With this information, one can justify how vital an IG program is to the firm and demonstrate that value to other users and stakeholders within the organization.

Figure 4.13: A map illustrating the various components that must be considered to maximize the value of metrics.
Various examples of valuable metrics may include:

- Systematic records of number of emails filed
- Number of file share folders created
- DMS monitoring to determine questionable user behavior
- Volume of extranets created and/or decommissioned
- Closed matter reports reconciled with timekeeper reports to give insights as to proactive matter closing activity
- Number of physical records and growth over previous periods
- Yr/Yr physical and electronic storage cost trends
- Compliance with retention/destruction schedules
- Service level deliverables such as the amount of time that lapses between the request for information to its delivery
- Number of records processed (i.e. created, indexed, disposed of) over specified periods of time
- # weeks/months/years to integrate lateral hire files into the program
- Size of electronic repositories to be added to the IG program and growth trends over previous periods
- # information security breaches/inadvertent disclosures

We have previously stated that IG is the glue that connects information silos. Metrics are the energy to propel your IG program going forward. They provide the useful insight to make program adjustments – from policy, procedure, and technology perspectives –and enable informed decision-making. Once measurable improvements are realized, metrics simplify the communications effort by determining what to promote – and to whom (see Figure 13).

As with other components of an IG Program, the value of metrics will vary from firm to firm. It is important to identify what, specifically, is of value to your firm. This will help guide in determining what should be measured.
Conclusion

There is no doubt that Information Governance (IG) is a moving target. As technology changes, policies evolve, and the line between what does and does not need to be governed continues to move, firms must be committed to not only implementing sound IG policies, but also auditing and updating them on a regular basis. It is the belief of this Steering Committee that the proposed IG framework set out in this report represents a comprehensive IG foundation upon which firms can build over time.

That said, we recognize that, due to the scope of IG and its transformational nature, no single document on the subject can ever be all-encompassing. As such, we close with a request to the broader legal community: Please use this framework as a catalyst for strategic discussions at your firm on how to build an IG program that fits your needs. In addition, we welcome comments on this body of work, as we will continue to refine the framework through the Work Groups and an annual Symposium.
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.