



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*

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

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

Symposium Leader

Carolyn Casey
Sr. Manager, Legal Vertical, Iron Mountain

Contents

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

Executive Summary

This report contains four separate Work Group reports from the Law Firm Information Governance Symposium, held May 22-24, 2012. An executive summary of each Work Group report follows.

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

WORK GROUP 1

Defining an Information Governance Framework

WORK GROUP PARTICIPANTS

Co-chair: Bryn Bowen, Director Records and Information Management, Greenberg Traurig

Co-chair: Rudy Moliere, Director of Information Governance and Records Management, White & Case LLP

Derick Arthur, Director of Records & Facilities, Proskauer Rose

Carolyn Casey, Sr. Manager, Legal Vertical, Iron Mountain

Beth Chiaiese, National Director of Loss Prevention, Foley & Lardner

Terry Coan, Senior Director, HBR Consulting LLC

Frank LaSorsa, Director of Records and Compliance, Kelley Drye

Brian McCauley, Director of Information Governance & Records, McDermott Will & Emery

Ann Ostrander, Senior Director, Loss Prevention, Kirkland & Ellis LLP

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

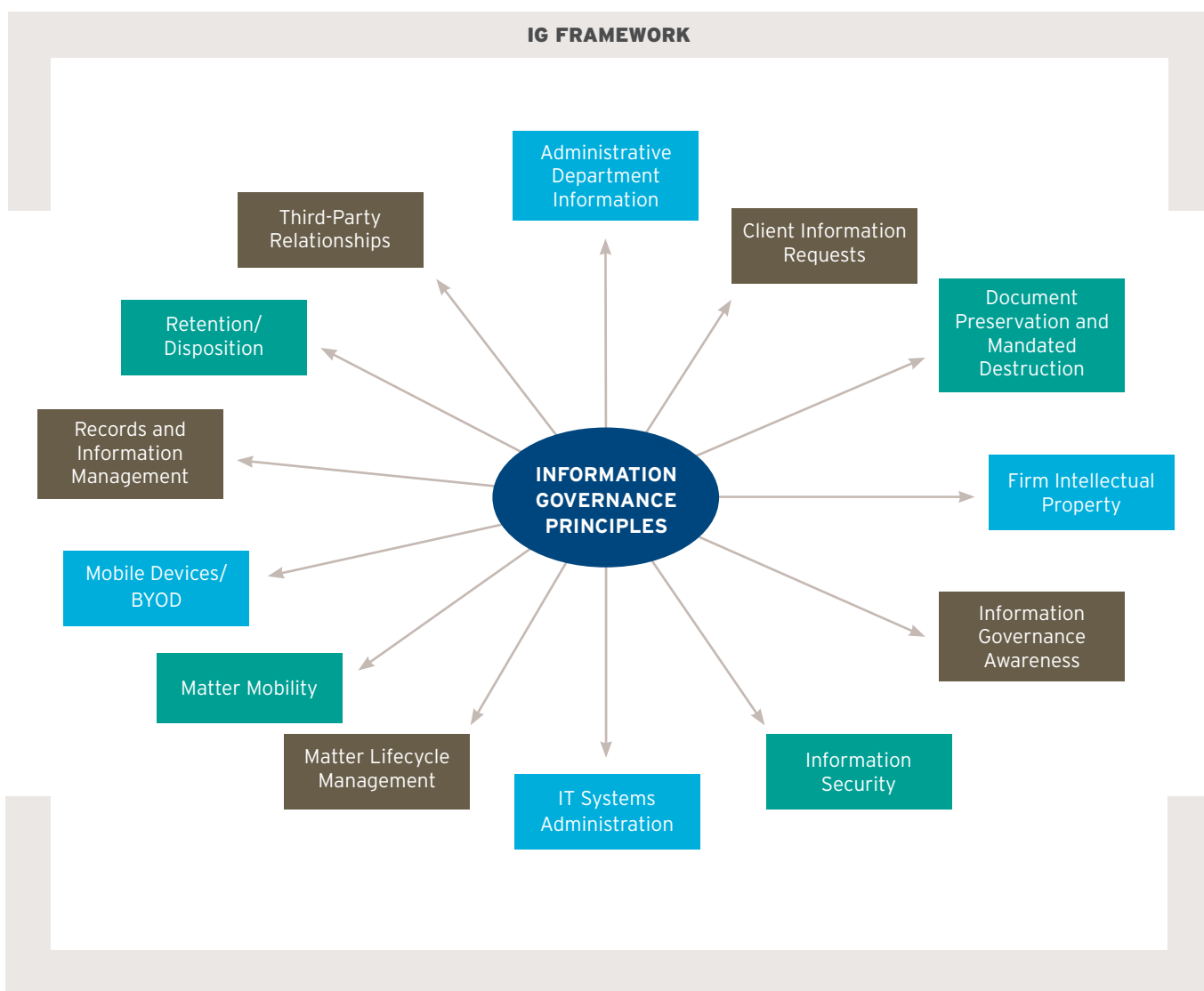
Firms will need to establish a set of core principles that will permeate their IG program and processes, including:

- 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

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

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:



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.

FORCE FIELD ANALYSIS EXAMPLE

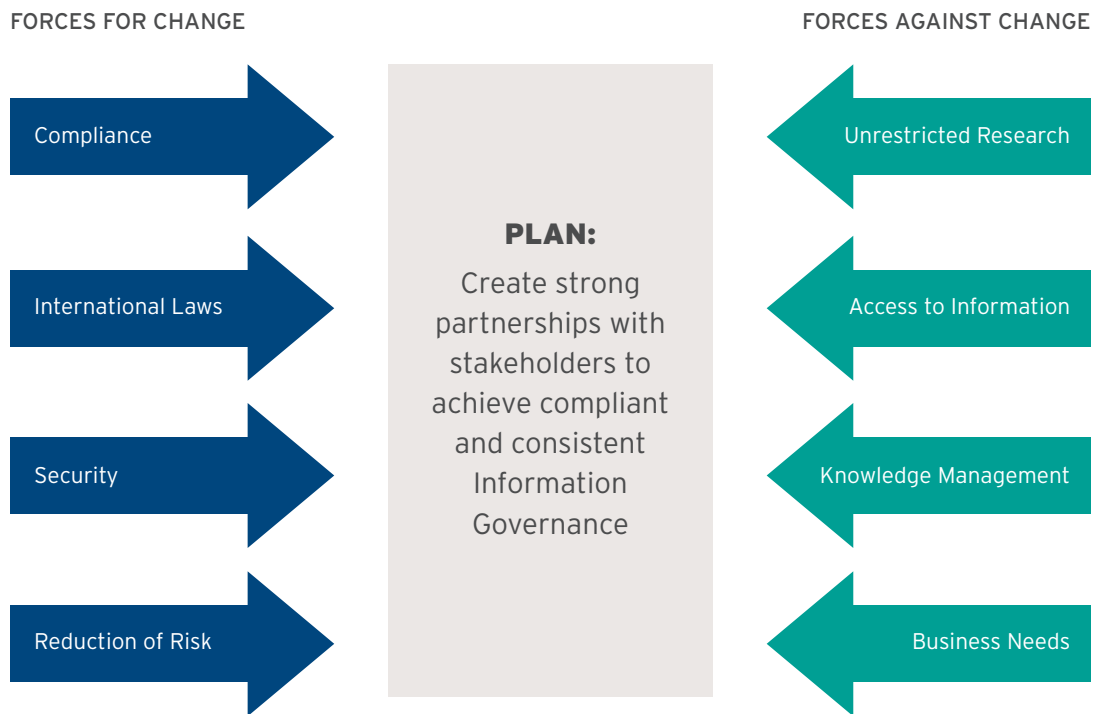


Figure 2.2: A force field analysis of elements that push a firm toward change and those that hold a firm from change. Note that it is possible to apply weight to such an analysis. For example on a scale of one to five, Compliance may be a five, whereas Unrestricted Research might be a three. Adding the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

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.

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.