It Takes a Village: Managing Information Governance

Work Group 2 Report
Law Firm Information Governance Symposium

IRON MOUNTAIN®

Contents

WORK GROUP 2

Executive Summary

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 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

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.

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.

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.

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 laws 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

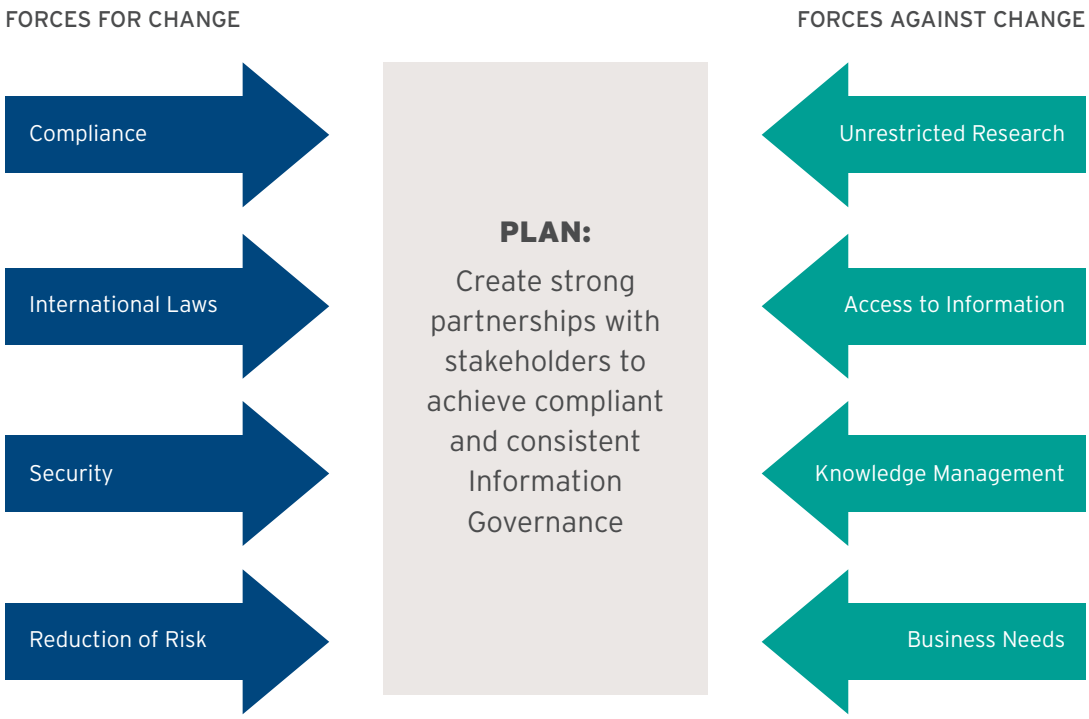

Figure 2.2: A force field analysis of elements that push a firm toward change and those that hold a firm from change. Note that it is possible to apply weight to such an analysis. For example on a scale of one to five, Compliance may be a five, whereas Unrestricted Research might be a three. Adding the 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.

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.

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.

KEY PROCESSES[1] 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.

[1] 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 to 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.

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

ironmountain.com

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

US-LAW-EXT-WP-082412-002.2