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[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.

WORK GROUP 3

A Proposed Law Firm Information Security Assessment Framework

WORK GROUP PARTICIPANTS

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

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

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

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

Brian Lynch, Director – Risk Practice, IntApp

Eric Mosca, CRM, Director of Operations, In Outsource

Paul Singleton, Director of Risk Management, Bingham McCutchen LLP

Susan Trombley, MLIS, Director, Consulting, Iron Mountain

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.

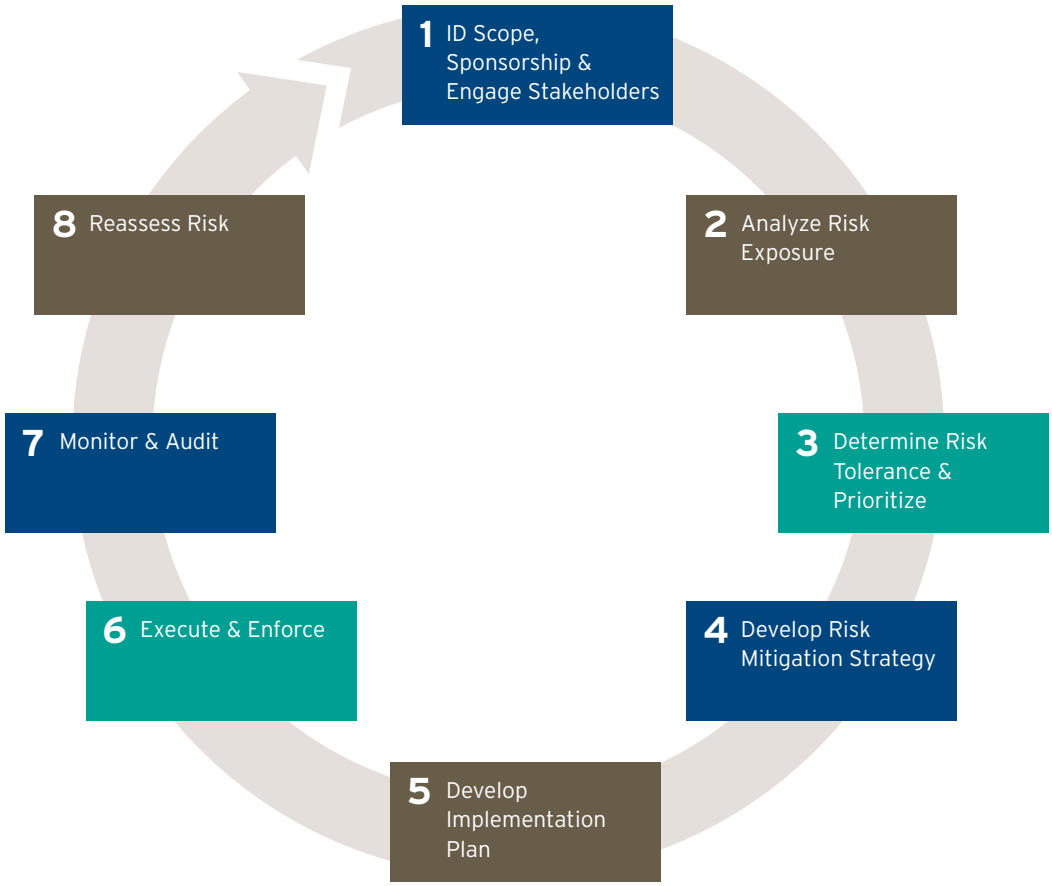

Figure 3.1: The Information Security Assessment Framework.

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.

WORK GROUP 4

How to Move Forward with an Information Governance Program in a Law Firm

WORK GROUP PARTICIPANTS

Chair: Leigh Isaacs, Director – Records & Information Management, Orrick, Herrington & Sutcliffe LLP

Odell Bryant, Director of Records and Conflicts Administration, Cravath, Swaine & Moore LLP

James Flynn, Director of Records & Docket, Winston & Strawn LLP

Grant W. James, CRM, Firm Records Manager, Troutman Sanders LLP

Faron Lyons, Account Manager, OpenText

Janice Raphael, Director, Legal Enterprise Accounts, Iron Mountain

Doug Smith, Records Manager, Wiley Rein LLP

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