IRON MOUNTAIN®

Building Law Firm Information Governance

Prime Your Key Processes

Introduction

The adoption of effective information governance (IG) has become critical in law firms. Clients remain highly interested in how firms govern their information in light of increased regulatory requirements for personally identifiable information (PII) and personal health information (PHI). Information security has become more complex with lawyers' increased use of mobile devices to access information and the growth of cyber-threats. The Law Firm Information Governance Symposium (Symposium) was established in 2012 as a think tank to give the legal industry a roadmap for addressing the impact of these and other trends on how law firms manage information. Our first publication, the 2012 *A Proposed Law Firm Information Governance Framework* (Proposed Framework) offered firms an initial IG framework that included proposed guiding principles, key processes definitions, best practices and methods for starting an IG program.

The Symposium Steering Committee, Work Group Participants and Iron Mountain are pleased to provide the legal community with two new publications from the 2013 Symposium. In this report, *Building Law Firm Information Governance, Prime Your Key Processes*, we go deeper into the "*how to*" of building information governance in law firms. In a tandem report, the *2013 Emerging Trends in Law Firm Information Governance* report, we offer insights into three emerging trends impacting law firm information governance: Big data, predictive coding and the 24/7 law firm. It is our hope that firms will use these reports to infuse IG into their unique processes and culture, and gain the client service improvement, risk mitigation and cost containment benefits we believe result from effective information governance.

SYMPOSIUM STEERING COMMITTEE

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

Bryn Bowen, CRM
Principal
Greenheart Consulting Partners LLC

Leigh Isaacs, CIP
Director of Records and Information Governance
Orrick, Herrington & Sutcliffe LLP

Rudy Moliere
Director of Records and Information
Morgan, Lewis & Bockius LLP

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

Carolyn Casey, Esq.
Senior Manager, Legal Vertical
Iron Mountain

WORK GROUP PARTICIPANTS

WORK GROUP 1 – IG Advisory Board, IT Systems Administration and IG Awareness Processes

Co-Chair: Bryn Bowen, CRM
Principal,
Greenheart Consulting Partners LLC

Co-Chair: Rudy Moliere
Director of Records and Information,
Morgan, Lewis & Bockius LLP

Beth Chiaiese, CRM, MLIS
Director of Professional Responsibility & Compliance,
Foley & Lardner LLP

Galina Datskovsky, CRM, PhD
Principal, Independent Business and Information Governance Consultant

Frank LaSorsa, CRM
Director of Records and Information,
Kelley Drye & Warren LLP

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

Brian Donato
Chief Information Officer,
Vorys, Sater Seymour and Pease LLP

Matt Kivlin
Director of Product Management, Legal,
Iron Mountain

WORK GROUP 2 – Matter Life Cycle Management, Records and Information Management, Retention Disposition, Matter Mobility and Information Mobility Processes

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

Derick Arthur
Director of Records & Facilities,
Proskauer Rose LLP

Scott Christensen
Director of Technology – US,
Edwards Wildman Palmer LLP

Esther Diamond
Records Manager,
Locke Lord LLP

Patricia A. Fitzpatrick
Director of Practice Management,
CPA Katten Muchin Rosenman LLP

Deb Rifenbark, CRM
Chief Records Officer,
Stinson Morrison Hecker LLP

David B. Steward, CRM
Husch Blackwell LLP

WORK GROUP 3 – Security, Client Information Requests and Document Preservation and Mandated Destruction Processes

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

Beth Faircloth
Director of Risk Management,
Seyfarth Shaw LLP

Norma Knudson
Director of Office Administration & Compliance Support,
Faegre Baker Daniels LLP

Brian Lynch
Director – Risk Practice,
IntApp

Eric Mosca, CRM
Director of Operations,
InOutsource

WORK GROUP 4 – Administrative Department Information, Firm Intellectual Property, Third-Party Relationships and Monitoring Key Processes

Co-Chair: Leigh Isaacs, CIP
Director of Records and Information Governance,
Orrick, Herrington, & Sutcliffe LLP

Co-Chair: Dana C. Moore
Information Governance Compliance Manager,
Foley & Lardner LLP

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

Carolyn Casey, Esq.
Senior Manager, Legal Vertical,
Iron Mountain

Terrence J. Coan, CRM
Senior Director,
HBR Consulting LLP

Samantha Lofton
Director of Records Information, Risk Management and Practice Support,
Ice Miller LLP

Faron Lyons
Open Text Inc.

Brian B. McCauley, CRM
Director of Information Governance,
McDermott Will & Emery LLP

Steven Shock
Chief Technology Officer,
Irell & Manella LLP

Contents

Building IG: The Information Governance Advisory Board

This chapter expands upon the definition of an Information Governance Advisory Board from the Proposed Framework and offers practical advice on the initial steps to form this board in the law firm.

INFORMATION GOVERNANCE ADVISORY BOARD

An IG Advisory board is a decision making body composed of key stakeholders of information who understand the governance needs of the firm. Its members are tasked with guiding and building governance policies and processes to help support the way lawyers work today.

KEY ROLES AND RESPONSIBILITIES OF THE ADVISORY BOARD

The IG Advisory board function may vary from firm to firm, but the primary role is to make strategic decisions regarding information governance in the firm, create short, medium and long-term plans for IG and monitor associated projects. The following is a list of the critical roles and responsibilities this board should perform in your firm:

- Create and/or oversee creation of IG policies and guidelines
- Sponsor and monitor IG related projects and advocate for resources/budget
- Create a strategic information governance roadmap, including one-, three- and five-year plans
  - Review and monitor the roadmap throughout the year and make adjustment as needed
- Review and monitor IG policies and processes for adaptability, acceptability and compliance by considering the following questions:
  - Should any processes change?
  - Is more training needed? If so, who and what level?
  - Is there a structural issue with any policy?
- Adjust IG policies and processes, as appropriate
  - Respond to audit findings
  - Advise on feedback loop to ensure implementation of changes
  - Advise on communication strategy

ADVISORY BOARD CHAMPIONS

We recommend identifying one or more champions or entry points into management to help justify and drive the creation of an IG Advisory Board. Depending on the firm's culture, potential champions include:

- Business Administrative Partner or Chief Operating Officer
- Members of the Management Committee

- Managing Partners
- General or Firm Counsel
- Practice Leaders
- Records & Information Management Leaders
- Conflicts and New Business Intake
- Security Leaders
- Chief Knowledge Officer
- Chief Marketing Officer
- Chief Information Officer
- Other C-level Executives (e.g. Docketing, Litigation Support)
- Regulatory Lawyers (for triggers, such as risk and privacy)

The key to gaining support or buy-in from these champions is to address their triggers or pain points. Most potential champions will respond to one or more of the following issues:

- Client demands to meet certain IG principles
- Risk (data leakage and confidentiality) and potential legal liability
- Compliance
- Need for richer business information
- Privacy
- Costs related to:
  - Increased efficiency of managing information
  - Defense and discovery
  - Electronic information storage and maintenance
- Competitive advantage
- Issues that have reached critical mass, such as outgrowing physical document storage space, on and offsite, and the effect on office size and configuration.

ADVISORY BOARD MEMBERS

Once a champion(s) is determined, add to the Advisory Board membership using the following list of potential influencers, committee members and stakeholders:

- HR and Finance Executives/Managers
- Practice Leaders
- Records/Information Managers
- IT Directors and Managers
- Representatives from departments that are significant consumers and producers of information
- Other leaders within the organization who can influence the direction and adoption of strong IG practices, such as office administrators who have an interest in/understanding of IG

PRIORITIZING THE ADVISORY BOARD AGENDA

For a successful start-up of your board, you will want to prioritize what initiatives the board will tackle first. Here are some suggested approaches for setting the board's early agenda:

- Understand and map out problems, such as:
  - Inconsistent file transfers related to on- and off-boarding
  - Ethical wall breaches
  - Information security leakage
  - Client demands (outside counsel guidelines)
  - Regulatory requirements (e.g., HIPAA, HITECH, Dodd Frank)
- Define the painful issues facing the firm, which include managing email and electronic documents, explosive growth of storage, cloud outsourcing and others
- Identify low-hanging fruit that can show quick results if addressed, such as storage, matter mobility, attorney, employee and client onboarding from an IT perspective
- Highlight areas of greatest risk, such as the exposure of client records, data leakage or difficulty managing information on various devices
- Keep pace with emerging trends, technologies and changing environments
  - Identify the risks and benefits of each
  - Example to consider:
    - Managing electronic information, such as email, text messages and other forms of messaging
    - Data loss/leakage
    - Best practices for managing information on various devices
    - Client-mandated use of external tools and storage devices

GO FOR EARLY WINS

After creating an IG Advisory Board, it is crucial to maintain momentum by engineering quick – but substantive – early wins. As a start, identify the issues and then assign them to one of the areas below, giving priority to those that fall into the high risk/high reward category.

HIGH RISK/LOW REWARD	**HIGH RISK/HIGH REWARD**
LOW RISK/LOW REWARD	**LOW RISK/HIGH REWARD**

THE INFORMATION GOVERNANCE LEADER

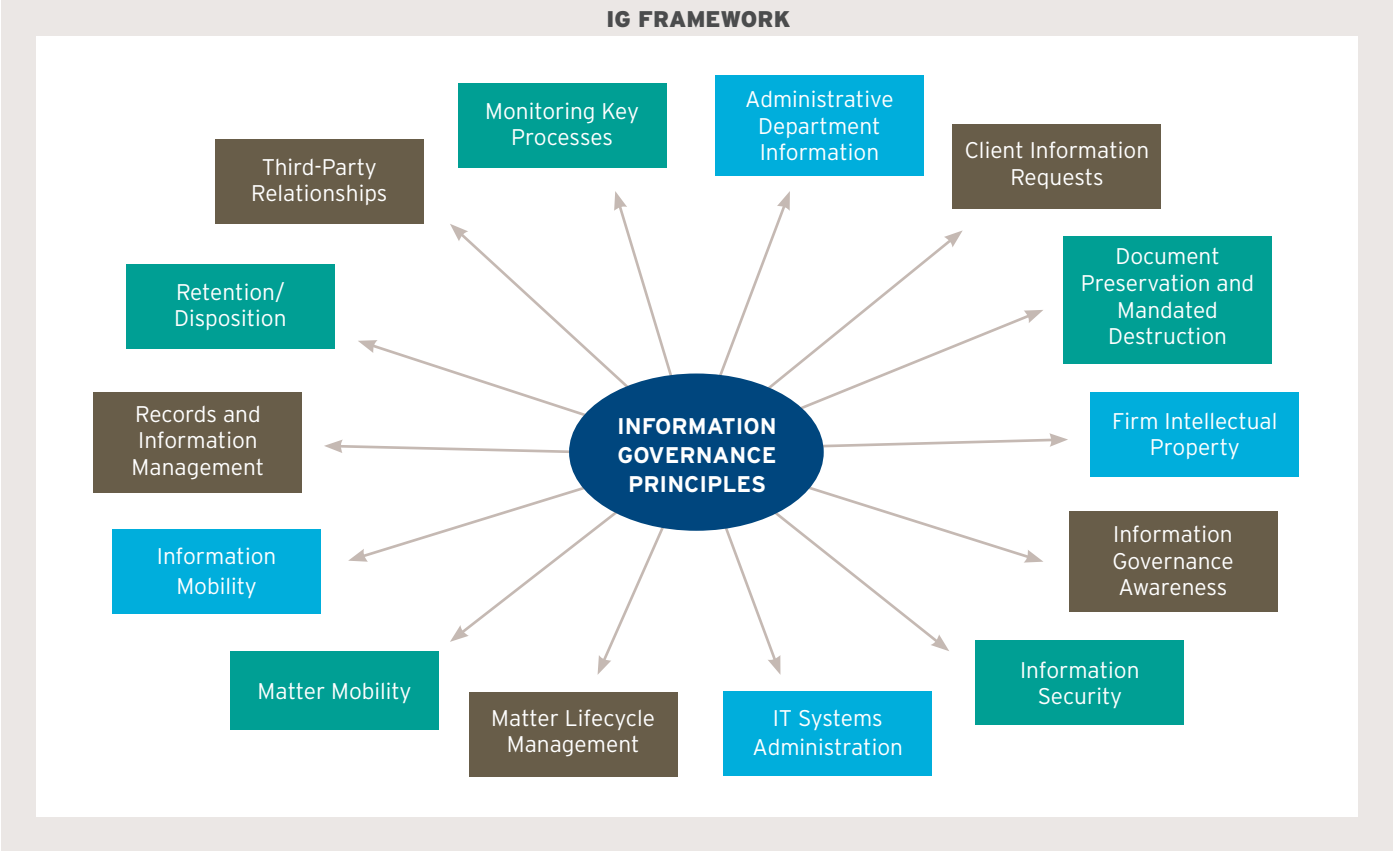
Finally, we should mention that, while not all firms will choose to have a Chief Information Governance Officer (CIGO), many do nominate an individual to take on the responsibility for planning, implementing and directing the firm's IG programs — whether full-time or as part of additional responsibilities. What's needed is a strategic leader who can provide firm-wide direction to attorneys and staff on all aspects of the organization's IG efforts, including, but not limited to, the RIM program, the firm's ethical and legal compliance information requirements, the preservation or destruction of information, the confidentiality, privacy and security of information and the mobility of information.

A template with more details on the job description for this role can be found in the Appendix 1.0 to this document.

How to Build Information Governance into Key Processes

This chapter provides practical advice on how to build IG into the key law firm processes identified in the 2012 Proposed Framework. In this chapter, you will find detailed definitions, potential obstacles firms may encounter and how to overcome them with best practices, and practical anecdotal advice for building IG into your processes.

The 2012 Work Groups created the graphic below of the Proposed Framework to convey the idea that the core principles developed by the firm's IG Advisory Board should guide 13 key processes identified by the Work Groups. In 2013, the Work Groups updated this graphical framework based on feedback gained throughout 2012 from discussions at conferences, webcasts and in local panel events. The updates are: (1) a 14th process was added: Monitoring Key Processes. A definition and full discussion of this additional process is in this report below; (2) the process previously called Mobile Devices/BYOD is changed to: Information Mobility, a broader, more appropriate description of the process of giving guidance and developing policies on security and access issues related to mobile devices, personal devices, remote access, etc.



1. IT SYSTEMS ADMINISTRATION PROCESS

IT systems administration is the process of providing guidance on systems selection and implementation, database administration, commissioning, decommissioning and developing systems and information migration.

COMMON PITFALLS THAT COMPLICATE IT SYSTEMS ADMINISTRATION

Here are some common issues facing IT that IG can positively impact:

- Budgets for storage or infrastructure are flat
- New media sources and attachment sizes make it difficult to ingest increasing volumes of data
- Litigation preparedness requires firms to store growing volumes of information
- Transfers, document holds, data security and privacy lack clear IG policies
- Transitory data may not be subject to destruction and retention policies
- Old systems should be decommissioned in accordance with IG principles, reducing risks related to data that should have been destroyed or maintained in a readable format
- Unstructured data is difficult to manage

BEST PRACTICE RECOMMENDATIONS

- Build a detailed and dynamic data map of all information-creating systems and their maintenance routines. Integrate IG principles as part of systems procurement and maintenance processes:
  - Be mindful of local information storage that may occur on devices, such as fax servers, photocopiers and particularly on devices that are leased.
  - Define protocols for the establishment and decommissioning of Team Sites related to client projects. This is again a part of the same issue.
  - Store transitory repositories on external media devices to facilitate efficient disposition.
- For current and proposed systems, interview system stakeholders and owners in order to assist with the procurement and maintenance of technology in accordance with IG principles. (Please refer to Appendix 2.0 for list of questions to guide IG systems purchases.)
- Publish IG guidelines and conduct awareness campaigns.
- Clarify system ownership and roles.
- Maintain consistent communication with IT through IG/IT committees, and roles.

BEST PRACTICES IN ACTION

1. One firm recently performed a study to identify the volume and percentage of data stored in three of its primary data repositories (see Table 1 on the following page). The study found that data stored in an unstructured repository could not be effectively managed across its lifecycle — and yet 96 percent of the firm's data was in that location.

To remedy the situation, the firm is deploying a matter centricity solution, which makes the document management system (DMS) a more attractive/usable repository for attorneys and staff. Once the system is deployed, IT and Records Management will work with users to migrate data from the unstructured network file shares and email to the DMS, where it can be profiled to a specific client matter. And when the migration is complete, the firm will be able to manage the entire information lifecycle — from creation to destruction. When a client matter is closed in the billing system, a close date is assigned and a defined retention period is applied to all of the electronic data associated/profiled to that specific client matter.

Table 1. Volume and percentage of data stored in primary repositories

REPOSITORY	DATA VOLUME (PERCENT OF TOTAL)	STRUCTURED/UNSTRUCTURED
EMAIL (EXCHANGE)	79%	Unstructured
FILE SHARES (PERCENT OF TOTAL)	17%	Unstructured
DOCUMENT MANAGEMENT SYSTEM (DMS)	4%	Structured

Structured = associated w/specific client matter
Unstructured = not associated w/ specific client matter

2. A time-honored tradition among Microsoft® Exchange Server system administrators at one firm was to keep a backup copy of the email database to ensure that, if anything went wrong during an upgrade or conversion, they could retrieve data. Unfortunately, these backup copies, which were often created on tape, typically ended up in a desk drawer and were forgotten. When discovered during a move, they were found to contain old email data that was no longer available on the active system and well beyond its retention period. Needless to say, the old tapes were securely destroyed and the firm implemented a policy and process for handling email backups that ensures they are kept only for the prescribed retention period.

Please see the New System Request Checklist Template in Appendix 2.0 for a list of questions that IT should ask when someone in the firm wants to bring in a new system.

2. INFORMATION GOVERNANCE AWARENESS PROCESS

Information governance awareness is the process of providing guidance, proactive education and training to the enterprise, especially to frontline support personnel and local office administrators.

COMMON OBSTACLES THAT COMPLICATE INFORMATION GOVERNANCE AWARENESS

- There is an unsanctioned transfer of information.
- Personnel are incompletely or inadequately trained on compliance obligations and firm information management systems.
- There is no approved BYOD policy and no IG influence or oversight.
- There is a lack of the auditing processes that would identify opportunities for retraining.
- Training on IG is not required of all firm members.
- Users are inundated with information.
- Users are unaware that many conveniences, such as emailing documents home, savings documents to the cloud or drafting work product on mobile devices, pose significant IG risks.
- IG is often viewed as a hindrance to "getting work done."

BEST PRACTICE RECOMMENDATIONS

- Communicate and train through annual e-learning, as well as the use of videos and quizzes.
- Tailor training to the audience (e.g., attorneys versus administrators.)
- Publish "Top 10" guidelines on IG policy via cheat sheets, employee newsletter articles, posters, etc.
- Send emails with spotlights on specific guidelines, ideally from senior leadership.
- Categorize information by topic, such as policies related to data on a personal device.
- Develop and conduct formal training that offers continuing legal education (CLE) credit.
- Configure systems with IG alerts.
- Team with the marketing department to establish and communicate key IG messaging
- Conduct lawyer outreach and program promotion activities.
- Demonstrate tangible ROI from good governance
- Take advantage of timely news items to promote IG awareness.

For more information on this area, see IG Job Description Template Appendix 1.0 to this document.

BEST PRACTICES IN ACTION

1. To combat employees' tendencies to keep everything, one firm established an organization-wide email retention policy. All emails in an inbox or sent items folder are automatically deleted when the sent or received date equals 180 days.

2. Another firm uses a "three zone" approach to email. Zone 1 is for transitory information that is subject to limited retention of 30, 90 or 180 days, which represents ~60 percent of the total. Zone 2 is for in-progress work. Thirty percent of the total, these emails are moved into folders, predictive coding is performed and they are checked into the firm's DMS. Retention on Zone 2 items runs two to three years. Finally, Zone 3 is for records, which comprise just five to 10 percent of the *total amount of emails*. Records retention policies apply to these items as they are stored in the records management system.

3. A firm has required a certain number of training hours for its staff members. And IG professionals are helping push the IG awareness agenda by inserting IG principles into common training courses. Additionally, IG is helping staff meet their training requirements while learning about basic IG principles by developing approved classes that count toward the staff members' training requirements.

3. MATTER LIFECYCLE MANAGEMENT

Matter lifecycle management is the process of capturing new client or matter information that is organized by areas of law and/or practice groups, including client engagement documentation, waivers and ethical wall requirements. Governance mandates the management of information during the active phase, as well as the process of systematically deactivating matters in firm systems at the conclusion of formal representation (matter closing).

COMMON PITFALLS THAT COMPLICATE MATTER LIFECYCLE MANAGEMENT

- Attorneys work on matters that do not have engagement letters and have not cleared the intake process.
- Because information lives in multiple repositories inside and outside the firm, it is difficult to manage the matter lifecycle.
- Matters are not closed in a timely fashion and may affect the clearing of new matters.
- Attorneys sign off on outside counsel guidelines that may impact retention/destruction without vetting them with IG.

BEST PRACTICE RECOMMENDATIONS

- Establish a process for identifying and clearing conflicts that reflect the Firm's risk tolerance and culture.
- Document, audit and enforce policies and processes for opening and closing matters. Setting the "tone from the top" is essential to the successful Matter Lifecycle Management program.
- Develop a policy consistent with the generally accepted record keeping principles developed by ARMA International
- Integrate matter life cycle awareness into information management training programs
- Regularly update and communicate matter management policies
- Invest in technological tools that enhance matter lifecycle management, such as new business intake workflow, conflict management, document management, and records management.

BEST PRACTICES IN ACTION

1. RIM policies also need to consider data security and access. Some clients want assurance that only those attorneys that are working on their matters have access to their records. In these types of scenarios, firms should consider implementing an automated "confidentiality management system" to restrict access to the information in all repositories.
2. A firm reduced the time required to add new business from days to hours by implementing an automated workflow system for new business intake. The NBI process now includes a workflow tool which not only accelerates the current matter acceptance but also captures answers to risk- focused questions, conflict decisions, engagement details, attorney authorizations etc, so that they can be leveraged for future use in decision making as part of the matter knowledge base.

4. RECORDS AND INFORMATION MANAGEMENT

Records and Information Management includes the management of information in all forms, regardless of media or repository. This process consists of creating, and periodically revising, firm policies and processes for managing the firm's information assets – including folder structures, taxonomy, and identification of discrete data.

COMMON PITFALLS THAT COMPLICATE RIM

- Users operate where it is most convenient or where business needs dictate, regardless of IG policies. Attorneys require access to client information 24/7, from any location-on-site, at the client, while traveling and in the courtroom. It is increasingly difficult to control the movement of information given the various business drivers.
- Multiple file sets are created for convenience and then never destroyed.
- IG is not always aware of the repositories being used by attorneys and staff.
- Repositories can be unstructured and not compliant with IG policies and processes.
- Mergers can make it difficult to standardize on a single set of IG best practices.
- If there is no IG, Information Technology and Records Management may be focused on different goals. This disparity often creates friction and competing priorities within the organization.

BEST PRACTICE RECOMMENDATIONS

- Develop a policy for the destruction of information that is not formally stored or managed in firm-sanctioned repositories. For example, you may wish to set an expiration date on all information saved on users' home drives and develop a nightly process that deletes anything that is older than a defined number of days. This will force users to move the data to a sanctioned repository if it needs to remain accessible in the future.
- Ensure repositories are easy to use for all levels of users and have documentation identifying what purpose they serve and who they support. A data map is ideal for documenting all related information for records and information management. Combine repositories where possible to establish standards, information and knowledge sharing.

– Establish a review process for all new applications that includes IG as a way to ensure proper IG practices are applied.

– Disallow users saving to shared drives, hard drives, etc., without correct profiling that includes client matter, a standard folder title, etc.

BEST PRACTICES IN ACTION

1. A firm nominated its Records Manager as the single point of contact for all requests to delete information and leverages its existing IT support ticket process to expedite the process. This approach works well because it is established an understood process for the entire firm.

2. IG practices can vary widely from firm to firm – a fact that is very clear in merger and acquisition scenarios. One firm found that a practice group it inherited, while savvy in its use of technology, lacked any appreciation for common RIM and IT best practices regarding email usage, backup and retention. At the time of a merger, RIM policies, practices and technologies should be evaluated and the best ones carried forward. The work to bring each firm's practices in line can be challenging – and there is often an education component that should not be overlooked or minimized.

3. A way of growth for many law firms now revolve around lateral mobility. Often, single practitioners or smaller firms are involved. Knowledge on how to effectively manage information is not inherited. By utilizing the skill sets and knowledge of records managers and technologists, an environment of standalone repositories, duplicative archived e-mail directories/repositories, a non client/matter centric environment can quickly become a standardized, collaborative one where the laterals quickly become integrated and productive.

5. RETENTION DISPOSITION

Retention disposition is the process of applying lifecycle management practices to client and firm information. Enacting disposition as defined under the retention schedule provides a defensible position to the disposition of current and legacy information.

COMMON PITFALLS THAT COMPLICATE RETENTION DISPOSITION

– Organizations are overwhelmed with "old stuff." They are unable to establish a project plan about what to keep and what to destroy. Firm engagement letters may address client record disposition without thought of supporting the actual practice, which may cause potential risks to clients.

– Before final disposition can occur, some state regulations require the final review be completed by an attorney.

– Getting attorneys to focus on client retention reviews is very difficult – and getting them to actually pull the trigger on destruction can be even more difficult.

– Destruction can be perceived as more costly than the operational dollars being spent on storage (both physical and electronic.)

– Litigation often becomes complex, with existing cases morphing into new cases, which prevents old information from being destroyed per the retention schedule.

– Some structured databases and systems may pose destruction challenges. These systems should be identified and carved out per the schedule as exceptions to the normal destruction process. For example, it is not easy or practical to delete data for specific date ranges from a firms' financial system. Amounts billed and monies collected need to balance to support firm financial statements and clients' outstanding accounts.

BEST PRACTICE RECOMMENDATIONS

- Provide a flexible policy that allows the framework to successfully implement a disposition program without hindering business.
- Define disposition practices in the engagement letter, while keeping local jurisdictional requirements in mind.
- Be aware of legal holds when applying retention to records — destruction must not occur until the legal hold has been lifted.
- Consistently apply retention policies so the organization does not expose clients or the firm to unnecessary risks. Consistently apply the same retention to the same type of records, regardless of the media type or repository. Break legacy information into small projects to make it easier to apply retention.
- Include backups in the firm's retention schedule. Be sure to factor in the backup tape rotation schedule when calculating exactly how long the data could be retrieved. Make sure that retention is applied in small satellite offices where you may not had a designated IT or Record staff person.
- Confirm that a deletion does just that — removes all traces of a record (different systems destroy records in different ways and, in some situations, information could still be recovered.)
- Hold users responsible for following the retention policy, which should include disposition of non-record material, transitory material and convenience copies management. This responsibility extends to media and home/personal computers.
- Make IG part of the process of adding new applications. As new applications are included, the information must be added to the retention schedule. This includes applications inside the firm, as well as those stored with outside vendors and in SAA- hosted environments. Third-party agreements should include a discussion about final disposition of information held by the third party
- Ensure that matters, such as patent, trademark and trusts are given the extended lifecycle that they require. For example, a trust agreement needs to remain active and available until the individual has died and his estate has been settled in the courts.

BEST PRACTICES IN ACTION

1. A firm instituted a formal process to track records stored offsite with third-party vendors and apply retention policies to this information. This process was developed in response to a situation where the firm's Records Manager became aware of the fact that hard drives with many years' worth of client discovery data was being held by a vendor without any regard for the firm's content or retention requirements. If the vendor had not contacted the firm, it is quite possible the firm would never have known about the poorly managed information.

6. MATTER MOBILITY

Matter mobility is the process of moving matters and their associated information into and out of the law firm, as triggered by client directives and lateral mobility.

COMMON PITFALLS THAT COMPLICATE MATTER MOBILITY

- New attorneys often bring material into the firm that is not client related, which raises cost NS risk exposure and has ethical consequences.
- Client transfers happen without client authorization. When a client is transferring, information from all the repositories are not necessarily transferred, leaving the firm at risk.
- Historically, paper files were identified as the "official" file, and individuals attached a more formal description as reference to its content. Electronically, individuals have adopted a personal style in their naming conventions (acronyms, shortcuts), which are not transparent to others when attempting to associate the information to a client/matter. It is difficult to bring in information from a non-matter centric environment into a matter centric one or vice versa. There is always potential for lost information having an unknown relationship.

BEST PRACTICE RECOMMENDATIONS

- Allow incoming attorneys to bring information for matters that have cleared conflicts. For mergers or large groups joining the firm, it is paramount that conflict be an integral part of the combining of the matters.
- Advise incoming attorneys of your onboarding policy and provide a checklist to ensure they adhere to firm standards.
- Disallow departing attorneys from taking any client information. Matters should transfer out of the firm only if there is authorization from the client. Attorneys should only be able to take personal information when they depart. (i.e. personal email, contacts, calendar).
- Develop a process for exiting attorneys that includes moving all client information to a structured repository and confirming that the attorney has deleted all copies that exist outside the repositories.
- Implement a standard review transfer process and checklist that covers what may or may not be released. It should also include a checklist of all repositories.
- Transfer information in a secure fashion, such as through encryption or secure file transfer.

BEST PRACTICES IN ACTION

2. A firm designed workspaces with three top folders: official matter records, nonofficial matter records and matter administration. The Microsoft Outlook® folders for all firm employees are automatically linked to the "official matter records" bucket by default. This minimizes the volume of materials that need to be reviewed and results in better management of information when the matter or attorney leaves the firm.

3. At one firm, RM is responsible for the coordination of transferring information from all repositories, working with IT and Practice Support to ensure that all information, regardless of repository or format, is transferred out. In addition, RM is responsible for making sure the information is deleted from firm systems 180 days after the transfer is complete.

7. INFORMATION MOBILITY

Information mobility is the process of providing guidance and compliance with firm policies/procedures, with respect to acceptable storage, use and security of client information, on both firm-issued and personally owned devices.

Note: The 2013 Work Group renamed the process, "Mobile Devices/BYOD" as named in the Proposed Framework, to "Information Mobility".

COMMON PITFALLS THAT COMPLICATE INFORMATION MOBILITY

- Attorneys do not always comply with metadata scrubbing policies.
- Data can be lost when a device is lost, stolen or replaced.
- Attorneys email or use an unsecure file sharing site to transfer information home, so they can work outside the office.
- Firms do not have a process for identifying and reporting end user data breaches or hacking from the outside.
- Encryption is not standard across manufacturers.
- It is difficult to wipe home or personal computers.

BEST PRACTICE RECOMMENDATIONS

- Allow information to be accessed, but only permit it to leave the firm in a specific, and defined manner. Technically or by policy, disallow data to be copied to home or personal computers.
- Implement systems that disallow the transfer of certain types of data and unauthorized cut and paste.
- Develop a policy that disallowing data transferring with unencrypted devices.

- Ensure the firm's overall security policy has special consideration for privacy, HIPAA and HITECH- related regulations. Consider local jurisdictional data privacy laws, especially if you have a global presence.
- Hold users responsible for reporting data breaches and lost, stolen or otherwise compromised devices.
- Ensure IG, IT and privacy are all part of any third-party contract negotiation that will allow data to be store, transferred or view outside of the firm.

BEST PRACTICES IN ACTION

1. A firm instituted controls that allow its attorneys to view data, but prohibit use of a "save as" on local disks/devices. This prevents people from making personal copies of information. The firm achieves this through the use of dumb terminals on attorney desktops that have no local storage and provide remote access to data in a controlled environment.

2. One firm deals with the growing incidences of lost or stolen devices, which can happen as often as once every three days, by employing a mobile device management (MDM) strategy that automatically "wipes" of all data from the device when an incident is reported. This allows the firm to mitigate any risk of a security breach when sensitive information on the device is disclosed. In addition, all laptops are encrypted.

3. Many firms are beginning to explore the feasibility of using a secure, externally hosted environment for collaboration. This allows firm attorneys to upload documents and share them with other members of their own organization, as well as their clients and third parties. The advantage of this approach is that it allows the data to remain secure while it is in-transit and while it is at rest. The document no longer needs to be emailed back and forth in order to collaborate. Traditionally, file sharing across email can be protected while the data is in-transit, but it often becomes exposed once the email is received and the attachment resides in the firm email system. If a mobile device is configured to allow access to firm email, then the attachment can also be opened and viewed once the message is received. This becomes a point of concern because mobile devices are casually shared with family and friends for non-work related purposes. Using s secure portal limits the potential for this type of exposure because the user must visit a separate hosted environment via a separate login and password before gaining access to the information.

8. INFORMATION SECURITY

Information security is the process of controlling access to information, such as establishing ethical walls and confidential access controls. It includes the protection of personally identifiable information (PII) or personal health information (PHI), as well as the control of internal and remote access to systems. Information security impacts all facets of the law firm, and as such, it must be applied to the firm's technology, internal resources (such as attorneys and administrative assistants), and overall firm culture. Due to the increased spotlight on information security, it has become a crucial factor in determining the continued growth, or even existence, of a client relationship.

From an information governance perspective, there are a number of points in the matter lifecycle where information security procedures may need to be reviewed or even revised. These stages can be considered discrete parts of the overall client/matter relationship. In similar fashion, the arrival of a new attorney or an administrative staff member presents comparable opportunities to reaffirm the firm's overall security measures and culture.

COMMON PITFALLS THAT COMPLICATE INFORMATION SECURITY

The hazards surrounding an unstructured information security program can be likened to those that may occur during the course of a poorly planned relationship, in that failure to understand expectations can ultimately lead to conflicting interests and significant breakdowns in communication.

Consider the following concerns should a solid information security program not be established:

The Courtship

- Lateral hires are not prompted to disclose existing security measures or guidelines for clients they bring to the firm.
- Standard procedures regarding information security are not developed by the firm to maintain consistency amongst all parties.
- Communications regarding security protocols are not conducted at all, or are conducted weeks or months into the engagement or employment - after work has already been performed.
- Attorneys and clients cling to familiar ways of working/interacting, which makes it difficult to effect a cultural change that conforms to updated policies and processes.

Rising Tensions

- The firm incorrectly assumes attorneys will inherently understand how established software programs should be used to classify and protect more sensitive data.
- Client and attorney demands are in conflict with information security, thus the firm is left to weigh exceptions to the policy in order to make accommodations.
- Data that could pose a risk to other active clients and matters is accepted by the firm.
- Workarounds are developed in order to circumvent the firm's approved data structure and repositories.
- Attorneys are unsure of how to respond to client inquiries regarding security measures.

The Break-up

- Departing attorneys are not motivated to address security requirements as they relate to data being transferred to their new firms.
- The departing attorney's new firm may have a more stringent information security program that does not permit the same data that the firm did, thus leaving the firm with data they do not want or should not have.
- Client data being kept in non-approved repositories is transferred or lost without the firm's knowledge.
- The firm does not consistently enforce formal departure processes, if said processes even exist.

BEST PRACTICE RECOMMENDATIONS

Create a defined Information Security policy. This policy should:

- Effectively address all known security concerns.
- Be based upon defined ROI and the firm's established risk tolerance.
- Identify firm-approved repositories (which are capable of supporting security requirements).
- Define other "acceptable" uses of technology with regard to managing information.
- Create a firm-specific "culture of adoption."
- Leverage examples of relevant security breaches or malpractice claims, in order to guide policy and compliance efforts.
- Be regularly reviewed and revised to encompass new risk management issues.
- Be supported and promoted by senior officials of the firm.
- Identify consequences for failing to comply with policy requirements.

Educate users on information security measures. The education program should:

- Be consistent and habitual.
- Communicate firm-approved repositories for information.
- Promote solutions or alternatives to otherwise risky information management practices (e.g., saving data to local hard drives, using non-encrypted devices, etc.)
- Reiterate firm policies.
- Require a staff "sign off" in which employees acknowledge their understanding of the policies.

Once the policy has been established, and training conducted, enforce compliance. This could include:

- Establishing a compliance function in a current employee's job responsibilities or hiring a dedicated compliance employee for such efforts.
- Monitoring the administrative and access rights of users and groups.
- Monitoring access logs.
- Generating monthly reports for review by Information Governance or Risk Management resources within the firm.
- Escalating issues of non-compliance to the appropriate individual or team. In certain situations where non-compliance directly impacts an agreement with a given client, the attorney responsible for that client relationship might also need to be involved.
- Developing and communicating the consequences of non-compliance. As appropriate, include "real-life" examples of when firms or employees have been sanctioned for failure to adhere to security requirements.

Consider adopting and tailoring the Information Security Assessment Framework outlined in Chapter 3 of the Proposed Framework for your firm. See two new templates for that process included in this report.

BEST PRACTICES IN ACTION

1. By providing the information security policy to a lateral hire at the onset, one firm was able to ensure data is being secured through the firm's approved systems. This also provides the lateral hire an opportunity to explain to the corresponding clients what impact, if any, this will have in terms of their matter handling. Additionally, the policy might also motivate the lateral hire to proffer any understood arrangements with certain clients regarding data privacy, so the new firm can ensure it is addressing the requirements accordingly.

2. With appropriate security training given, all parties of a firm are aware of the correct procedure to request documents to which they may not otherwise be given access. Rather than obtaining the document via measures that might put the security controls in jeopardy, attorneys can ensure that their requests are vetted through the appropriate teams and the necessary access is given through system channels.

3. One firm provides its own information security guidelines to clients, governing the transfer of information between parties. The guidelines are modified as new regulations and requirements arise. With an established information security policy and training program in place, the firm is better able to demonstrate to the client that it values the privacy of the information to which it is entrusted.

9. CLIENT INFORMATION REQUESTS

Client information requests is the process of efficiently, consistently, and appropriately responding to client requests regarding IG policies and procedures, requests for proposal (RFPs), questionnaires, surveys, proposed outside counsel guidelines, client audits and file delivery requests. Such requests can come at a variety of points in the lifecycle of a client, or potential client, engagement. Client information requests may include multiple topics across the firm's IG

program, and information might be required from several departments within the firm. Responses to such requests might require further follow-up with the firm by the client, or may prompt the client to provide their own set of requirements for the firm to follow.

COMMON PITFALLS THAT COMPLICATE CLIENT INFORMATION REQUESTS

- The attorney or firm may agree to comply with client requests, but fail to notify the appropriate parties responsible for managing the data in question.
- The firm designs its current environment to comply with client requirements, but fails to monitor/maintain it as new technology or new requirements emerge.
- Some firm environments are so unstructured that it prohibits them from providing efficient, compliant and complete responses to client requests.
- Certain security requirements from the client create a significant cost or inefficiency for the firm's current environment.
- Attorneys and administrative staff not working directly with the client in question may not fully appreciate why the requirements are in place, thereby increasing the risk of non-compliance by the firm.

BEST PRACTICE RECOMMENDATIONS

- Besides involving Firm Management or General Counsel, designate an administrative team with representatives from IT, Records Management, and Business Intake, and/or assign a "risk quarterback" who will be responsible for responding to client information requests.
- Mitigate the inherent conflicts between business development and risk efforts — don't allow partners to personally respond on the firm's behalf without additional approval.
- Develop and implement a foundational strategy and policy from which to negotiate — eliminating the vulnerabilities associated with ongoing, one-off responses.
- Communicate the final submitted responses to all impacted parties.
- Institute and conduct periodic internal audits to ensure readiness for third-party audits.
- Ensure all firm personnel are aware of the reasoning behind the procedures and the consequences for the firm if the procedures are not followed.

BEST PRACTICES IN ACTION

1. One firm instituted a policy where RFPs are circulated to the "risk quarterback" and his/her designated team as referenced above for review prior to responding. This not only ensures an accurate response, but it allows everyone involved to raise concerns, recommend reference information and plan appropriately for the effort. With this approach, all parties in the firm are familiar with the security requirements necessary to comply with a third-party audit.

10. DOCUMENT PRESERVATION AND MANDATED DESTRUCTION

Document preservation is the process of preserving potentially responsive information, ensuring the suspension of a scheduled disposition and complying with a custodial legal hold during the discovery phase of litigation, investigations and audits. Mandated destruction covers the destruction of information as mandated by the court or by agreement among parties.

COMMON PITFALLS THAT COMPLICATE DOCUMENT PRESERVATION AND MANDATED DESTRUCTION

- Data that isn't managed in a firm-supported repository may not be properly addressed when a preservation or destruction disposition occurs.
- Firms err on the side of document preservation over destruction, resulting in exponential storage growth and related costs.

– Firms may not have a process developed to follow up regarding established litigation holds to determine if they have expired – thus, leading to over-retention of records.

BEST PRACTICE RECOMMENDATIONS

– Create a checklist of all areas where client data may reside.

– Develop an electronic sign-off process (e.g., destruction order software).

– Run destruction requests through an assigned/dedicated person/team to maintain defensible practices.

– Ensure internal awareness of destruction decisions.

BEST PRACTICES IN ACTION

1. By utilizing an electronic sign-off on destruction orders, a firm was able to confirm that pertinent data had been destroyed in all systems and demonstrate its compliance as required to external parties. By distributing a complete listing of all current holds (with status updates) to appropriate staff member, and scheduling reviews of retention holds, the same firm is able to ensure that all parties continue to adhere to hold requirements and materials no longer on hold aren't retained for longer than required.

11. ADMINISTRATIVE DEPARTMENT INFORMATION

Administrative department information is the process of managing the firm's internal, strategic and operational business information, including the preservation of the vital records needed to ensure business continuity, compliance with legal and/or regulatory requirements and efficient responses to litigation and investigation requests. Consistent application of retention values must be utilized using firm-approved repositories. Administrative and business records include those that are the results of a deliberative process to engage new business, as well as information created and received by firm business operations.

Administrative information should be managed and classified using a two-level hierarchy (similar to client/matter), in which the top level represents the administrative business functional areas (clients) and the second level represents the core business activities performed by the functional area (matters).

While each law firm may be unique in its organizational structure, functional areas that may be impacted include:

– Firm management, such as the Chairman, Managing Partners and Practice Group Leaders

– Chief Operating Officer (COO) and other executive officers

– General Counsel, Risk Management, Loss Prevention

– Finance and Accounting

– Information Technology

– Facilities Management

– Library and Research

– Records and Information

– Human Resources

– Legal Recruiting/Development

– Business Development

– Marketing and Press Communications

– Client Intake, New Business Intake, Matter Administration and Lateral On-boarding

COMMON PITFALLS THAT COMPLICATE ADMINISTRATIVE DEPARTMENT INFORMATION

- Contract management is decentralized, and disparate functions manage their own contract procurement and renewal processes.
- It can be difficult to ascertain which department owns specific business activities and the responsibility for maintaining the associated records.
- Failure to apply consistent data privacy and security language within contracts across all departments within the firm results in additional risk.
- Storing information in unmanaged repositories creates challenges to implement and maintain information management practices.
- Docket management contains information that should be evaluated as to how and what becomes a "record of information" that could be disclosed.

BEST PRACTICE RECOMMENDATIONS

- Manage firm business records using a defined approach, assigning a unique series of numbers to each administrative function for use in managing their activities, similar to client matter management.
- Ensure that official administrative files provide evidence of the firm's compliance with international, federal and state laws and regulations.
- Define firm-approved repositories, where records should be stored.
- Identify the firm's line-of-business applications and map them to the relevant categories in the retention schedule.
- Create departmental ownership of the contracts and liability associated with IG.
- Establish best practices for managing and/or disposing of information contained in transitory repositories.
- Reference malpractice insurance GC guidelines from an insurance consortium (risk management.)

BEST PRACTICES IN ACTION

Several firms have been able to strengthen their processes around the management of administrative department information through a combination of senior management support and ongoing training/education.
Some examples include:

1. A managing partner created a directive to back up and classify all information into the appropriate database with applied retention. This endorsement by key stakeholders (from the administrative business unit and Information Technology) helped to implement and enforce the program.

2. The general counsel in one firm established and supported teams that promote better understanding of processes among associates, paralegals and secretaries.

3. During an audit, a records management team discovered that the firm's employees lacked an understanding of the process or purpose of IG. The firm addressed the situation by proactively involving administrative department leaders and teams. This helped ensure that effective collaboration took place and supported acceptance of the policies.

4. Better employee communication regarding the negative impacts of noncompliance helped one firm end a "boycott" of the use of the DM and RM process. Today, its staff no longer uses file shares as a dumpin ground for unclassified files.

12. FIRM INTELLECTUAL PROPERTY

Firm intellectual property (IP) is protected by adhering to the process of capturing and preserving the firm's knowledge, operational, creative and historical artifacts holding commercial, business or strategic value. Examples of firm IP include marketing and branding materials, knowledge management (KM) resources, contact information, firm initiative planning information, business development strategies, strategic plans, case management protocols, lateral lawyer growth records, financial information and firm policies and procedures.

Firm IP has historically been unmanaged or managed randomly — with little to no centralization or consistency. This presents challenges when retaining documents and data that represent the firm's knowhow. Frequently, this IP stems from work performed on behalf of clients and documents contain information unique to a specific client or engagement. Regardless of the challenges, proper governance and management of firm IP is critical to making the firm more efficient and providing a competitive edge.

COMMON PITFALLS THAT COMPLICATE FIRM INTELLECTUAL PROPERTY

- Use of KM and DM creates a proliferation and duplication of information in separate systems, which forces the firm to sanitize information.
- Multiple copies in many locations lead to retention challenges.
- Firm IP found in marketing material, web sites and photographs may have permanent retention and storage considerations within shared drives and DM systems.
- Historical information revealing how a firm has evolved creates challenges, such as tracking partnership agreements and change in firm leadership or partnership structure.
- Firm IP needs to be maintained, secured and sanitized to protect trade secrets.
- Firms do not have a classification or designated repositories for IP, resulting in difficulty or inability to locate, retrieve, protect or leverage information.
- Third-party consulting work product, including workflow diagrams, process and procedures, is not managed within the IG framework.
- Branding strategies and processes developed as a competitive and/or marketing differentiator are not treated or maintained as IP.
- Historical case destruction can provide some challenges for KM and utilization of work product and other IP for reference in future matters.

BEST PRACTICE RECOMMENDATIONS

- Define what is/is not considered IP, such as whether it's limited to formal patented trademarks or copyright protection or more broadly applied to encompass firm knowhow.
- Identify and locate the firm's IP and ensure that it is adequately secured.
- Sanitize/redact firm IP stemming from client information for precedence work product.
- Establish a process for treating precedential documents within the KM system.

BEST PRACTICES IN ACTION

1. A law firm provided specific criteria for managing historical information in its records retention and disposition policy and program. It also assigned the responsibility of overseeing the program to a partner and senior administrative staff member.

2. Recognizing that much of its history is retained in the personal or administrative files for legacy partners, one firm developed a procedure to carefully review materials left behind by retired or deceased partners and extract valuable information.

3. Creating an awareness program, defining roles and responsibilities (i.e. reviewing for comment, declaring as precedent, etc.) and automating key processes and reporting allowed another firm to gain greater control of its IP, and minimize alterations that could result in risk.

13. THIRD-PARTY CONTRACTING

Third-party contracting is the process of ensuring consistent contracting language and defining service-level agreements (SLAs), where applicable, in accordance with firm policies regarding information access and protection. Many firms contract with outside organizations to perform a range of key functions. As such, standardized and consistent policies, processes and procedures must be established and clearly communicated to define rules, duties and responsibilities for how third-party partners must comply with IG. Given that the risks posed by today's third-party relationships are dramatically different than the risks posed by legal vendors of the past, failure to do so can result in liability and risk exposure and potentially create catastrophic consequences for law firms and clients.

COMMON PITFALLS THAT COMPLICATE THIRD-PARTY CONTRACTING

- Contracts don't have language that addresses the provisions of a data breach by third parties.
- Contracts lack indemnification and limits of liabilities with third-party contractors.
- Contracts don't clearly address ownership (i.e. that which belongs to the firm vs. other parties).
- Contracts don't clearly address lifecycle management of information, including ultimate disposition.
- Contracts don't clearly address issues related to access, privacy or how information is stored.

BEST PRACTICE RECOMMENDATIONS

- Create a standardized and auditable process wherein contracts with third-party vendors are reviewed and approved to ensure adherence to the firm's IG processes or any firm-approved templates or boilerplates.
- Ensure that the third-party contract approval process includes the best practices identified in this report.
- Hold third-party vendors and employees to the same standards as firm personnel as it relates to information security and compliance.
- Document the information management, storage security and compliance requirements for third-party providers.
- Create a preferred vendor list that has been vetted by the firm, where contract terms have already been negotiated and vendors are placed on an "ok to use" list.
- Integrate data protection, privacy, security and compliance requirements (e.g. ARRA, HITECH, Safe Harbor, PII and HIPAA) into the contracting agreement.
- Regularly audit third-party compliance with firm policies, regulatory requirements and protocols related to the firm's ethical obligations.
- Restrict third-party vendors' access to only the information needed to perform the contracted services.
- Establish a set of provisions that addresses non-disclosure, indemnification, limited liability and warranty for third-party contractors.
- Review all existing and future third-party contracts for compliance with specific provisions set forth by the firm relating to indemnification, limits of liability and warranty.

BEST PRACTICES IN ACTION

1. A firm that routinely outsources eDiscovery for specific matters amended its contract language to ensure that third parties agree to follow the firm's overall information security provisions and SLAs in alignment with its IG requirements.

2. A firm created policy and process that involved the review of all vendor contracts to confirm that they allow auditing rights, contain a robust complaint response, reporting and monitoring system and include adequate representations and warranties relating to the duties of the vendor carrying out its responsibilities. This includes such things as proper training of staff, compliance with federal and state consumer laws and audit rights and self-testing. Ultimately, this helped third-party data breaches from resulting in public harm to a specific matter — or to the firm's reputation.

3. To ensure consistent and thorough due diligence, a firm created a questionnaire to be used when evaluating and engaging with third-party vendors.

4. To further mitigate risk and cost of premiums, a law firm worked closely with its malpractice insurance carrier to ensure compliance with its insurers' guidelines for standard policy clauses, escalation protocols, etc.

5. A firm that outsources printing, document productions and other services that require client records be sent offsite has policies in place to be made aware of any outsourcing used by its contracted vendors for overflow or support. As such, the firm can work with direct contracted third parties to ensure third-party controls extend to contractors.

14. MONITORING KEY PROCESSES

Firms should monitor and evaluate key information governance processes on a regular basis to ensure that the organization meets the goals of the program. Our 2012 Framework proposed three primary goals for IG: (1) improved client service through rapid information access, (2) risk mitigation to ensure professional, regulatory and legal obligations are met, and (3) cost containment in areas such as real estate, information storage, insurance and other potential liabilities. Monitoring key processes entails establishing operational metrics and benchmarks, which are routinely monitored and analyzed, to evaluate the overall effectiveness of the IG program. For this information to remain relevant and useful operational metrics and benchmarks should be refined as appropriate to support an evolving IG program.

COMMON PITFALLS THAT COMPLICATE MONITORING KEY PROCESSES

- It can be challenging to define individuals and departments responsible for the creation and implementation of monitoring and auditing of processes.
- It may difficult to gain consensus on what aspects of the key processes should be measured, monitored and adjusted.
- Key processes rarely, if ever, apply to only one department or group within the firm. Depending upon firm culture, it is often challenging to apply consistent monitoring of processes across all departments.
- Effective monitoring of key processes requires personnel and technology resources. With increasing frequency, firms are challenged to do more with less and monitoring may not appear to be a critical function that justifies financial investment.

BEST PRACTICE RECOMMENDATIONS

- Build the monitoring process into the IG program that is ultimately approved and supported by firm leadership.
- Develop a well-defined, measurable IG program that includes an IG Advisory Board. It is important to create an IG framework that establishes strategic goals and works specifically for the firm and is commensurate with a firm's IG maturity level.

– Identify unique metrics to evaluate key processes, including whether the process can be automated. Examples may include:
  - Number of items (including emails) filed into a DM repository
  - Number of IG-related training sessions and attendance
  - Number of physical records and growth over a defined time period
  - Number of information security breaches
  - DMS monitoring of user activity
– To ensure compliance and ability to conduct an effective audit, determine departmental owners of information (both for administrative and client files).

BEST PRACTICES IN ACTION

1. Gaining support for an email management policy by conveying the benefits (efficiency, cost savings and risk mitigation) of doing so to key stakeholders. This was accomplished by measuring systems and server space required to store large volumes of unnecessary email. In addition, the firm demonstrated system performance improvements, increased reliability of search, and number of departed employee mailboxes that could be deleted since relevant emails were captured elsewhere.

2. Setting thresholds for common DMS tasks (e.g. export, email, print, etc.) and monitoring user activity provided a firm with an opportunity to proactively address suspicious activity, and thus, mitigate risk of firm or client information leaving the firm in a manner inconsistent with established processes and procedures.

3. Recognizing that there were cost savings to be gained in monitoring offsite storage activities, a firm was able to decrease spending in this area by reducing the number of rush deliveries and contracting special pricing with the vendor for scheduled deliveries.

4. Monitoring and measuring various new business intake activities helped a firm in a variety of ways. Minimizing the time required to open a new client/matter resulted in greater compliance with firm policies and procedures. And following up on whether actual work on an engagement commenced after being opened allowed the firm to collect business intelligence that was used for strategic planning.

5. Achieving compliance in closing matters is a challenge for many firms. Failure to do so has the potential to result in both increased cost and risk. One firm established a procedure and monitoring process to communicate with timekeepers for matters that can be closed and automate the closing of a matter based upon last accounts receivable. Doing so provided them with a mechanism to trigger retention and disposition, and eliminated potential conflicts with engaging new business.

APPENDIX 1.0

Building an IG Advisory Board – *IG Job Description Template*

This template was written for a Chief Information Governance Officer (CIGO) and thus assumes the role is strategic, placed at a high level and has firm-wide responsibility for all IG programs. Firms using this template should adapt the language to the role they are filling (e.g., scale the requirements accordingly if filling a C-level, director or manager role.)

SUMMARY OF THE ROLE

The Chief Information Governance Officer [INSERT TITLE] ("CIGO") plans, implements and directs the firm's Information Governance ("IG") programs. The CIGO is a strategic leader who provides firm-wide direction to attorneys and staff on all aspects of the firm's IG efforts, including, but not limited to, the Records and Information Management ("RIM") program; ethical and legal compliance requirements related to information; the preservation or destruction of information; the confidentiality, privacy and security of information; and the mobility of information. This position directly oversees the following functional areas [INSERT FUNCTIONAL AREAS]. The CIGO reports to: [INSERT TITLE OF SUPERIORS].

The CIGO: [SELECT THE HIGH-LEVEL ROLE DESCRIPTIONS APPROPRIATE FOR THE FIRM]

- Collaborates actively with key stakeholders, including the [LIST STAKEHOLDERS] to develop and implement the firm's IG and RIM programs.
- Develops and oversees implementation of a strategic program applying industry-leading practices and methodologies to support the achievement of short-, medium- and long-term IG goals.
- Oversees development and implementation of policies and guidelines for the management of all information at the firm.
- Collaborates with system owners on the governance of data within their systems.
- Develops, oversees (or in some cases, implements) and enforces strategies and procedures to ensure the confidentiality, privacy and security of client and firm information.
- Acts as or collaborates with the Privacy Official for the firm in the management of processes related to the investigation of potential data breaches.
- Ensures that the IG and RIM programs govern information assets in all formats, including hard-copy and electronic.
- Ensures that the IG and RIM programs comply with applicable ethical and legal requirements in relevant jurisdictions.
- Develops and implements a communications and outreach strategy to achieve awareness and integration of the program throughout the firm.
- Communicates program requirements and goals to firm personnel through education, coaching and change management strategies that increase user adoption and compliance.
- Monitors program effectiveness utilizing benchmarks to evaluate and improve program performance.

DUTIES AND RESPONSIBILITIES

- Strategic Planning: [Insert description of the strategic planning responsibilities of the CIGO.] [SAMPLE LANGUAGE: Develops and maintains both short- and long-term strategic plans for the governance of the firm's information, including both client and firm business information, in all forms and formats.]
- Information Governance Advisory Board (IGAB) Chair [OR Insert name of firm IG committee]: [SAMPLE LANGUAGE: Selects and appoints members, defines the scope of IGAB work, leads meeting discussions, brings appropriate issues to the IGAB and prepares committee documentation (agenda, minutes, etc.)]
- Policies: [Insert language that describes CIGO responsibility for the development of IG policies.] [SAMPLE LANGUAGE: Develops policies that govern both client and firm business information, including how the firm creates, uses, secures, maintains, stores, releases, acquires, preserves, retains and disposes of information.]
- Procedures and Programs: [Insert language that describes the specific programs the CIGO oversees.] [SAMPLE LANGUAGE: Directs and oversees the design and implementation of processes and programs that support the firm's IG efforts, including the RIM program, litigation holds related to the firm or to clients where the firm has responsive records, information mobility related to incoming or departing lawyers and clients, confidentiality and privacy, and records retention and disposition.]
- Compliance: [Insert language that describes the CIGO's responsibilities regarding legal compliance.] [SAMPLE LANGUAGE: Ensures that the Firm's IG policies, processes and programs comply with applicable rules and laws regarding the management of both client and firm business information.]
- Privacy Official (in the absence of a CISO): [Insert language that describes the CIGO's responsibilities to act as the firm's Privacy Official.] [SAMPLE LANGUAGE: Receives reports from firm personnel regarding potential data breaches, including the loss or disclosure of confidential client information, personal information or any information the unauthorized release of which is subject to law or regulation. Investigates such reports, and recommends follow up action to the firm. Oversees any required actions to report such breaches and to resolve them according to applicable law or regulation.]
- Communication: [Insert language that describes the communication responsibilities of the CIGO.] [SAMPLE LANGUAGE: Communicates information about the IG program at all levels of the firm, including lawyers, legal support staff and firm administration. Provides regular update and information about the IG program to firm management.]
- Collaboration: [Insert language that describes how the CIGO collaborates to achieve IG goals and objectives.] [SAMPLE LANGUAGE: Works with firm management and other administrative leaders to collect information necessary to build components of the IG program, and also consults with various firm leaders and departments on IG issues. Serves on related firm committees to provide IG perspective or ensure IG awareness.]
- Direction and Management: [Insert language regarding the functional areas the CIGO has direct responsibility to manage.] [SAMPLE LANGUAGE: Has firm-wide responsibility to direct and manage the following functional areas: [List functional areas]. Develops staff plans, and hires and develops functional leaders. Oversees work of functional leaders, including IG-related procedure and program development and implementation.]
- Systems: [Insert language that describes the CIGO's responsibilities for various Firm systems.] [SAMPLE LANGUAGE: Along with IT Director, jointly oversees primary content management systems including the firm's document management system, records management system and other key content repositories. Works with administrative department leaders to ensure that all other functional information systems conform to defined IG standards. Defines lifecycle requirements for the retention and disposition of information in all firm systems. Participates in requirements definition, vendor review and system selection efforts to ensure new systems conform to IG standards. Stays current regarding law firm technology, including new trends, products and best practices.]Third Party Access

to Information: [Insert language that describes CIGO's responsibilities to establish standards for third-party access to information.] [SAMPLE LANGUAGE: Defines standards for the access of client or Firm business information by third parties, including processes to define scope of access and to review and/or approve contract language regarding information access.]

- Continuous Improvement and Audit: [Insert language that describes CIGO's responsibilities to continuously improve IG policies, processes and programs, including regular audit and follow up.] [SAMPLE LANGUAGE: Engages in the continuous improvement of IG policies, processes and programs by actively seeking input from stakeholders and other personnel, and by implementing processes to audit programs for compliance].
- Budget and Financial Management: [Insert language that describes CIGO's budgetary responsibilities.] [SAMPLE LANGUAGE: Develops and maintains budgets for various IG functions, including personnel, travel, education, supplies, systems, subscriptions and other required expenses. Develops proposed budgets for various IG initiatives as part of strategic planning efforts. Negotiates applicable vendor contracts. Reviews and approves invoices.]
- Industry Awareness: [Insert language that describes the Firm's expectations for the CIGO's awareness of industry trends and best practices.] [SAMPLE LANGUAGE: Stays current with leading industry practices and new developments in the area of IG and RIM. Participates in continuing education, research, networking and professional and industry organizations.]
- Travel: [Insert travel requirements for CIGO.] [SAMPLE LANGUAGE: Requires extensive travel.]

EDUCATION AND PROFESSIONAL CERTIFICATIONS

- Educational Requirements: [Insert language regarding minimum educational requirements.] [SAMPLE LANGUAGE: The CIGO must have a minimum of a bachelor's degree. An advanced degree, a law degree or a degree in an information management related field is desirable.]
- Professional Certifications: [Insert language that describes various professional certifications that are desired for the CIGO.] [SAMPLE LANGUAGE: Professional certifications in various technical areas related to IG are recommended, although not required. These include: [CRM, CIGP, IGP etc.]]

EXPERIENCE REQUIREMENTS

- Minimum of [Insert required years of experience] [SAMPLE LANGUAGE: five years of experience in strategic leadership in a professional services organization. A record of progressively responsible business positions.]
- Previous experience [Insert language describing previous experience the Firm wants for the CIGO] [SAMPLE LANGUAGE: in a law firm, professional services or consulting firm, leading various areas related to the management of information, such as RIM, security, privacy or legal compliance is required.]

KNOWLEDGE, SKILLS AND ABILITIES [SELECT THE HIGH-LEVEL ROLE DESCRIPTIONS APPROPRIATE FOR THE FIRM]

- Strategic Thinking and Planning: Develops a long-range vision for the IG program and translates vision into achievable short and long-term strategies and initiatives.
- Leadership: Influences the firm and firm personnel to adopt and comply with the IG program.
- Management: Identifies and selects talented leaders and staff to drive IG programs and initiatives. Develops the IG team to achieve operational and professional success. Demonstrates strong organizational and operational skills.

- Communication: Possesses advanced written and oral communication skills. Scales communications to all levels within the firm. Translates complex issues into simple concepts. Advocates the IG vision, strategies and initiatives to firm management.
- Problem Solving: Analyzes problems, collects data, establishes facts and diagnoses solutions. Exercises judgment and discernment. Escalates problems appropriately.
- Interpersonal: Develops strong relationships at all levels of the firm. Manages and mediates conflict as necessary. Works in teams, collaborates and consults.
- Change Management: Develops programs that facilitate adoption of the IG program. Balances competing firm priorities.
- Technical: Prefers strong subject matter knowledge in areas of direct and related responsibility, including RIM, privacy, security, technology, systems, legal compliance, project management, research and other ancillary areas.
- Budget and Financial Management: Creates budgets and financial plans to support IG initiatives.

APPENDIX 2.0

IT Systems Administration – *New System Request Checklist Template*

The following is a list of questions that IG should ask when someone in the firm wants to bring in a new system. The goal is to ensure that good IG practices are defined around the project:

- What is the business need for procuring this system and how will it be used?
- Who is the business owner of this system?
- Will this system be a repository for records?
  - Is there a need to lock down records or screens?
  - What capabilities does it offer for classifying/identifying records?
  - What capabilities does the system provide to apply a retention schedule and disposition plan?
- Does it have the ability to disposition the record?
- Does it contain something that is unique and is authoritative on the record?
- Is it a copy of data?
- Is it the official system of record or part of the assembly line/process that produces the record?
- What type of information is this system managing?
  - Client?
  - Firm administration?
  - Other?
- Does it transport medium or creator-specific information?
- What are the expected points of integration and pass through?
- What are the related requirements around:
  - Uptime?
  - Data redundancy?
- Will data be used in place or replicated for use?
- What are the business requirements regarding backup?
  - What do we need to back up and how should it be backed up?
  - What is the purpose of the backup – how will it be used? (It should be DR only at all times.)
  - How long do we need to retain a backup?
  - If the system and data are cloud-based, how does the provider back things up? What is the provider's policy for backups and disposition, as well as data production and migration? (See the ARMA cloud guideline.)

APPENDIX 3.0

Process Implementation Template

Below are the elements originally identified in the the work group 3 section of the 2012 proposed framework to be considered in developing your firm's implementation strategy. Examples and leading questions have been added to help frame those elements in your firm's environment. The leading questions are not to be used as a checklist. In fact they should lead to more questions that will need to be answered as you develop your strategy. The template is designed as a scalable roadmap to assist administrative staff in creating a risk mitigation strategy based upon the firm's stated needs or in anticipation of modifications required to accommodate changes to laws and regulations. This is the preliminary planning stage before the execution of the plan and the enforcement of compliance.

DETAILED COST ANALYSIS

<As part of the implementation plan of any new system or process, the project team must conduct a more granular review of the associated costs to determine appropriate budget, efficiency and return on investment. While this list is not applicable to all proposed processes or systems outlined in this framework, nor is it all-encompassing, some key items to consider are: technology (licensing, maintenance, infrastructure), resources (consultants, vendors, additional personnel), and training (trainers, session fees, course materials.)>

EXAMPLE:

If the firm were implementing a new ethical wall process, it might invest in new (or updated) software to help streamline the process. With that, there might be vendor support with the implementation, as well as training sessions that need to be conducted with the applicable staff members responsible for managing the software within the firm environment.

Leading Questions:

a Technology

- Will implementation require firm to purchase new software licenses?
- Will the technology that addresses the proposed integrate into the firm's infrastructure?
- Will the technology require outside consultants and/or maintenance agreements?

b Resources

- Can in-house resources be leveraged to perform this, or are outside resources necessary?
- Who will be responsible for implementation and ongoing oversight?
- Can the necessary internal project management/IT costs be appropriately estimated?

c Training

- What is the scope of the training?
- What needs to be trained? Who needs to be trained (e.g. trainer, user, etc.)?
- What is format of training (in-person/webinar, train the trainer, etc)?
- What is the continual training plan?
- What is the plan for training new hires?

WORKFLOW

‹In this area, the project sponsor or his/her designee will be crucial to outlining the desired process and what steps need to be taken to perform that process. Some areas that should be covered are departmental areas that will be impacted by the process or technology, tasks that need to be performed/monitored in accordance with new process or technology and by whom, any potential areas for probable deviation and alternative processes or approval, plus key changes to the future workflow.›

EXAMPLE:

A new ethical wall process will impact those teams that manage electronic and physical data for the firm, especially if the default access for information within the firm's document and records management systems is public. When constructing the ethical wall workflow, any impact on these systems, or action steps required by these teams, should be documented.

Leading Questions:

a Outside Events

- What are outside triggers that kick off these workflows?
- Audit request?
- Retention period?
- Departing client/attorney?

b Tasks

- What are the standard steps that need to be taken to complete the request?
- What are the decision points?

c Roles

- Who has authority to make the decision?
- Can this role handle the volume?
- Are there cultural/geographical/regulatory variances?
- Escalation alternatives? Does this happen often enough to be built into workflow?
- Who approves exceptions?

AUTOMATION/TECHNOLOGY CONCERNS

‹Once the workflow has been documented, it's an opportune time to review what areas could become automated, and if so, what technology might assist in the automation of those processes. For example, if a particular audit needs to be performed on a system, is it possible to set up a nightly run to generate that information? Again, while technology might not have been the goal of the initial implementation, one might find in reviewing the workflow that there are available technologies to assist with the process itself. Conducting a "road show" of products might also generate some additional ways to improve the proposed implementation, so that it's a more robust or secure system.›

EXAMPLE:

While technology may not have been included in the firm's original plan for an ethical wall process, upon creating the workflow, the firm might determine a need for new technology that will help facilitate or automate, wall creation and expansion into other firm systems. Alternatively, the Firm might determine that other software the firm is looking to implement must comply with the ethical wall software already in place. If technology and/or automated processes are determined, it's important to ensure they are documented in the detailed cost analysis.

Leading Questions:

a Process Review for Technology Candidacy

- Are there a significant amount of employees in many groups involved?
- Is the process repeatable and predictable?
- Are there unique and variable processes that are hard to automate?
- Is the process well-defined, labor-intensive and high-volume?

b Service Levels and Metrics

- Will automation reduce risk and provide compliance audit trails?
- Have baseline metrics been established?
- What metrics could be gathered using automation?
- Do we want to use automation to set service level agreements?

c Technology Review

- Does an in-house workflow tool exist?
- Do vendors exist that can automate the workflow?
- Can the system be automated but also allow for human decision making (keeping control over process)?
- Will events be triggered or scheduled?
- Is the technology scalable?
- Does the technology meet any required industry standards?
- What are integration points and will the technology work with those systems?
- What is deployment effort and do we have the resources to deploy?

ROI

‹For the initial implementation, and for periodic re-assessments, ROI will likely be key to determining the success of the program. Depending upon the implementation, there are a variety of desired returns, and all are not necessarily financial. Some key factors to take into account for ROI, besides, of course, the initial investments are: expected cost savings, expected risk prevention and potential revenue generation.›

EXAMPLE:

For the implementation of a new ethical wall process, there will likely be a reduction in risk exposure to the firm, as well as a cost benefit in terms of insurance. Additionally, ethical wall processes can be leveraged in RFPs to differentiate firms from their competitors in terms of security. These should be calculated into the realized ROI.

Leading Questions:

a Desired Results

- What are the expected benefits of moving forward with implementation?
- Cost savings?
- Risk mitigation?
- Revenue generation?

b Timeline

- When will the expected return be realized?
- Will the return be ongoing?

c Metrics

- How will ROI be calculated?
- What measurements can be used to monitor ROI?
- Who will be responsible for monitoring the metrics?
- If the ROI is not what was initially expected, what will be the process to review?

TRAINING AND ADOPTION PLANS

‹As part of the adoption plan, the training plan should be geared towards acceptance and proper usage of the tool or process. It should take into account the fact that those to be trained could be stationed at different levels in the firm and/or use the system or process across multiple levels. At minimum, it should contain the intended users by access level, training venue and media and user follow-up and requirements. The adoption plan will likely commence with user awareness of the system or process and continue into the evaluation of system usage. As mentioned, training and education will be part of this overall plan, but also consider marketing, support, and scheduling.›

EXAMPLE:

Once the ethical wall process has been established, training for the appropriate individuals and teams should be developed and conducted, and processes should be documented. A user awareness plan regarding the benefits of the ethical wall process, including ethical requirements, should be explained to the appropriate parties. Refer to the communications template for further process considerations.

Leading Questions:

a Training Groups

- What type of training groups will be required?
- "Train the trainer" (super-user)?
- Administrative groups?
- Legal secretaries/paralegals?
- Attorneys?

b Training Materials/Environment

- How will the material be presented?
- eLearnings?
- Training manuals?
- Classrooms?
- Will there be a need for additional trainers, including external training groups?
- Will there be an opportunity for "refresher" training?
- Will training be mandatory or optional?
- How will attendance be recorded?

c Adoption

- What is the realistic projected adoption goal?
- What metrics will be used to measure results?
- What is the ETA as to when this goal is expected to be achieved?
- What marketing tools will be used to communicate the implementation?
- email blasts?
- Blog messages?
- Videos?
- Disciplinary Action
- Will there be any consequences for users failing to adopt the implementation?
- When will they be implemented?

CONTROL PROCEDURES

‹Ensure that the project sponsor or designee has identified the individual responsible for policing usage of the system. This individual should be able to provide a report within a given timeframe (which may vary in accordance with the lifecycle of the system) regarding overall system usage, system errors or deviations from the system itself. Any disciplinary action for improper usage of the system should be discussed and implemented as necessary.›

EXAMPLE:

The individual responsible for implementing the ethical walls, or the appropriate IT team managing the ethical wall software, can generate reports based upon number of walls implemented and wall violations (if applicable.)

Leading Questions:

a System Usage

- Which team/party will be responsible for monitoring system usage?
- How often will system usage be monitored?
- What is the outlined expectation of usage for each user group? Are there groups that will not be using this system, and what will be their process/system?

b System Errors

- How will system errors be reported?
- Who will be responsible for follow-up education/training if an error is determined to be user-related?
- What, if any, disciplinary action will occur for an employee if he/she continues to use the system incorrectly?

METRICS

‹Looking at the reports from the control procedures and referring back to the established ROI, it should be determined whether the firm is on target to meet those expectations.›

Leading Question:

Are the metrics originally identified sufficient enough to determine ROI and user adoption, or are additional metrics required?

AUDITING AND MONITORING

‹The implemented process should be audited and monitored to identify whether additional training is necessary.›

EXAMPLE:

The ethical wall process should be monitored to ensure the appropriate walls are being implemented as it relates to the matter restriction. For example, is there a clear understanding of when a matter warrants an inclusionary wall as opposed to an exclusionary wall? If not, staff will likely require further education on the process.

APPENDIX 4.0
Risk Mitigation Strategy Template

Below, are the elements originally identified in the work group 3 section of the 2012 proposed framework to be considered in developing your firm's risk mitigation strategy. Examples and leading questions have been added to help frame those elements in your firm's environment. The leading questions are not to be used as a checklist. In fact they should lead to more questions that will need to be answered as you develop your strategy. The template is designed as a scalable road map to assist administrative staff in creating a risk mitigation strategy based upon the firm's stated needs or in anticipation of changes needed to accommodate changes to laws and regulations. This is the preliminary planning stage before the development of the Implementation Plan.

ACCESS OR CONTROL CONCERN

‹Detail the type of access being granted or restricted or the user behavior being enforced. General categories include new technology, new regulation, new client requirement and new leading practice. Note the scope of the access or control being limited and the desired outcome.›

EXAMPLES:

New Technology – Enterprise search technology will allow all firm employees to search across the document management system, HR data, contact relationship management system and network drives for documents and metadata. Enterprise search functionality also threatens to expose content previously kept confidential through obscurity or inadequate security controls.

New Regulation – HIPAA/HITECH places additional burdens on the firm to protect personal health information (PHI) where the firm is functioning as the business associate of a covered entity. The Firm must institute mechanisms to encrypt communications containing PHI and develop procedures to monitor for and report breaches of PHI.

Leading Questions:

a What is the internal business driver for the firm to make this change or adopt the new technology?

b How does this change enable the Firm to better service clients, work more efficiently, meet ethical obligations or save money?

c Is there a financial impact if we do not address this access or control concern?

d How do our competitors and clients handle this concern? What are the best practices being discussed by other?

e Who is asking us to address this access or control concern (e.g. clients, general counsel, new regulations or courts)?

f Does this impact our work with a specific client or potentially affect the entire firm?

g Will implementing a control limit efficiency of attorneys or support staff?

h What is the cultural impact of implementing this technology or control?

i What is the timeline for implementing this access or control?

j To whom will this apply? Attorneys? All staff?

k Who's authorized to make the decision to implement this change?

l Who will take ownership of this access or control for implementation and for future monitoring?

POLICY DEVELOPMENT NEEDS

‹Indicate need to create or update policy documentation; include high-level policy points and necessary procedural documentation. Provide estimate of time required for drafting and review of new documentation›

EXAMPLE:

Internal Firm Policy Change — Updates are needed to the computer usage policy and IT and help line support procedures, resulting from the decision to no longer allow users the ability to download .exe files to firm hardware.

Approximately eight to 10 hours are needed for policy updates, utilizing an outside consultant. And, four to six hours are planned for internal policy review and approval. Notification would need to be provided to all users and the help line and IT staff will need to be trained on how to handle or escalate requests to download .exe files.

Leading Questions:

a What new/updated policies have to be drafted?

b What new/updated procedures have to be drafted?

c Will new policy conflict with any current policy?

d Is anyone already working on any aspect of this already?

e How long will policy/procedure drafting take? Who will be reviewing drafts?

f Who's responsible for enforcing? What is the escalating process?

g Who's responsible for communication of new policies and procedures to the Firm?

h Is there a need to consult with outside resources?

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.›

Leading Questions:

a What is the scope of the training?

b Who needs to be trained e.g trainer, user, etc.) ? What equipment, device or procedure will be involved in the training process?

c What format (e.g. in-person/webinar, train the trainer, on-demand video, all of the above, etc.) will be utilized for training?

d Will future training be required? What is the ongoing training plan to provide refreshers and address new hires?

e How do we encourage participation?

INFRASTRUCTURE UPDATES NEEDED

‹Detail the necessary changes to the firm infrastructure necessary to implement the control or technology. This may include physical hardware, software, deployment methodologies, tracking and reporting tools or new administrative positions.›

EXAMPLE:

Firm Access Control Change – The firm has made the decision to monitor and control access to both the Firm's document repositories and the time and billing system for individuals involved with ethical walls, including screens. The Firm will need to assess whether or not it has the technology needed to implement this decision or if it will they need to access software.

Leading Questions:

a Can the required change be made in the current infrastructure or is the purchase of new software necessary?

b Will the technology that addresses the proposed control integrate into the firm's infrastructure?

c Are physical control limitations a concern? (e.g. keycard access, lockable cabinets, fireproof suppression, etc.)?

d Does the Firm have the proper organizational structure to implement, monitor and review this control?

e How will infrastructure updates be received culturally?

RESOURCES

‹Document the resources that will be brought to bear for this risk mitigation approach. These may include research tools or subscriptions, outside auditors or persons dedicating time to this effort. Note the expected time commitment on a weekly and/or on an ongoing basis, as well as any costs associated with utilization of this resource and the impact to any existing job responsibilities.›

Leading Questions:

a Can this role be taken on by existing resource?

b Who is involved and how much of the person's time is required?

c Do we need to create or hire new positions?

d Do we have job descriptions aligned with success?

e Do we need human capital or could this be automated? If automated, do we have people with the right skill set to administer the automation or know what training will be necessary?

f Is there a needs analysis completed for technology/subscription resources and will it require an RFP to secure?

g Are there information resources we need?

h What are the credible sources for this information?

HIGH-LEVEL COST ANALYSIS

‹Provide a high-level analysis of all costs associated with implementation of the risk management control. Include capital expenditures, personnel costs, operating expenses software and hardware costs, etc.›

Leading Questions:

a What are the technology costs?

b What are the implementation costs and ROI (please refer to Implementation framework)?

c What are the resource costs?

d What are the training costs?

DELIVERY OF FINDINGS

‹Indicate the approval necessary to move forward with implementation of this risk management control. Provide links to approval documentation, support of professional malpractice insurer or outside opinion.›

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 website at www.ironmountain.com for more information.

US-LAW-EXT-BR-072313-001

800 899 IRON (4766) / ironmountain.com