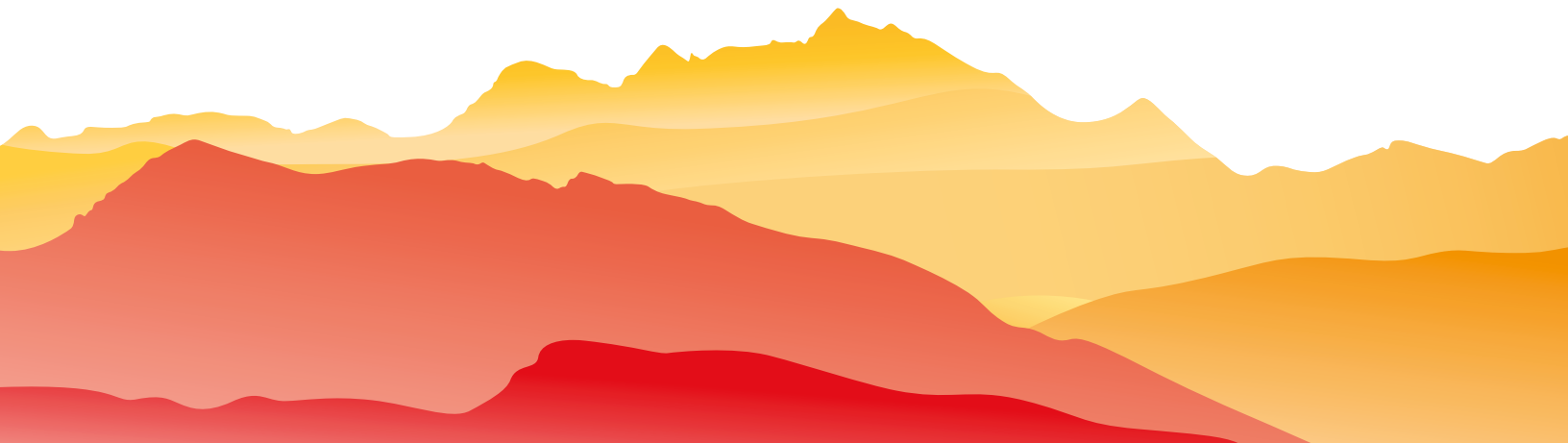
IRON MOUNTAIN®

2023 Law Firm Information Governance Symposium

You have an IG policy, now what?

A practical guide to putting your policy into practice



Contents

Authors

Brianne Aul
Senior Manager of Information Governance Strategy and Operations
Morgan Lewis Bockius LLP

Chuck Barth
Director of Information Governance
SheppardMullin

Bryn Bowen
Practice Group Leader, Risk
Intapp, Inc

Galina Datskovsky, Ph.D., CRM, FAI
Member of the board of directors
OpenAxes

Michele Gossmeyer
Global Director, Information Governance, Risk and Compliance
Dentons

Christine Hunter
Counsel, General Counsel's Office
Blake, Cassels & Graydon LLP

Sharon Keck
Sr. Paralegal & Escheat Product Analyst
Card Compliant LLC

Jim Merrifield
Director of Information Governance and Business Intake
Robinson & Cole LLP

Rudy Moliere
Director of Information Governance
Morgan Lewis Bockius LLP

Jill Sterbakov, Esq.
Information Governance Compliance Manager
Morgan Lewis Bockius LLP

Scott Taylor
Director, Information Governance & Intake Compliance
Smith Gambrell Russell

Introduction

Creating and implementing an effective Information Governance (IG) policy is a critical first step an organisation must take to secure data, comply with regulations, and meet ethical standards when managing information. Beyond those requirements, law firms can maximise the benefits of a robust IG program, including the efficiencies and cost reductions that result from better information management. There's more, however, to an IG program than the ideas embodied in the policies. The goals of these policies must be implemented and evaluated for ongoing effectiveness and compliance. This paper addresses how to turn IG policies into action plans.

What is an IG policy?

An IG policy is a high-level plan that embraces the general goals and acceptable procedures of an organisation. An IG policy provides a strategic roadmap to following the principles of information governance (ARMA principles; LFIGS 2.0). It describes each firm's IG function and provides directives on how these functions are to be fulfilled. This can be one comprehensive policy or smaller more targeted policies that cover or work in conjunction with related firm operations, e.g., privacy, risk management, information security, etc. It addresses both client matters and administrative functions of the firm.

How policy differs from procedures

While policies are a roadmap to your firm's IG program, they function best as a high-level explanation versus the detailed plans of the procedures put in place to operationalise the policies. Procedures are the implementation of the policy: they are agile and open to rapid alterations. They are also specific to the who/what/how/when/where that each process involves.

As an example of a policy versus procedure, we can look at matter transfer requests. A policy on what happens when a matter is to be transferred out of the firm might state what consents or authorisations are required (e.g., written consent from client and the Office of General Counsel (OGC)), who initiates the process, how outstanding fees are handled, who reviews records prior to release, who approves the release, who decides if a transfer agreement is necessary, what types of materials should be transferred. The matter transfer procedure will be much more granular. For example, each internal stakeholder in the process identifies the contacts and develops a flowchart for how the request progresses. That process addresses the following questions:

- Does the responsible attorney forward the request to the OGC, and does the OGC or IG contact work with that attorney to obtain written consent from the client?
- Who contacts billing to determine outstanding fees?
- Who is responsible for overseeing the gathering of the records to be released and what is the process in place to do that?
- What is the process for review of the records (can it be handled by IG or the OGC team, or must the responsible attorney or their team conduct the review)?
- Who negotiates the transfer agreement?
- Is there an escalation process for hiccups in the process?
- How are releases tracked?
- How long is the retention of the information about the transfers?
- Is a copy of the transferred materials retained and, if so, for how long?

This does not mean a policy should be light on details. A retention and disposition policy may have its record retention schedule as an addendum to the policy, rather than a separate process. A policy, however, should be broad enough that it does not require frequent modifications.

The importance of effective implementation

Having a policy that is not followed can be more problematic than having no policy at all. Clients, regulators, and business associates regularly ask if firms have policies in place, and often request to review them. Clients increasingly conduct audits of the firms that handle their information to ensure the policies they've been apprised of, and their own directives, are met. Failing to comply with the policies that govern your firm can be considered misrepresentation and pose a great risk to your firm.

Considerations for a tactical plan to follow your IG policies

This paper presumes your IG policies are in place and provides steps to operationalise, socialise, and monitor them. It addresses the following factors:

- Identifying and acquiring the people necessary to undertake the process
- Communicating/socialising and educating the firm on the policies
- Technology used in the firm and the technology to assist with compliance
- Enforcement/compliance, including gathering and assessing metrics and tracking
- Frequency of review and updates

If you do not yet have policies in place, the following resource may be a beneficial place to start: LFIGS 2.0: An Established Law Firm Information Governance Framework (2019). The support you received from your firm's senior management to craft these policies is even more important to building the procedures based on them. Having the leadership of the firm, including those directing practice groups and administrative functions, champion your program drives its success.

Identifying and acquiring the people necessary

Implementation of IG policies requires identifying and deploying the right people. A staffing plan depends on the firm's size and organisational structure. It should consider who "owns" the IG functions and how to assign the resulting responsibilities.

Staffing for firms of all sizes

Firms exist in all sizes and can range from a sole practitioner to thousands of lawyers and staff. No matter the size, it's necessary to make sure all data and governance policies are followed. The good news is that IG support can be scaled to match the needs of each entity.

In a smaller firm (or a larger firm still striving to obtain resources for an IG program), support team members wear many hats. There generally isn't enough work or budget to justify a full-time, dedicated staff member for each unique function. Often, the resource(s) in IT may cover some technical, information security, and electronic governance needs. Legal support staff can help cover physical file and document management.

Advice for smaller firms is to move toward digital solutions and storage options as this helps eliminate the need for file rooms and support. If physical files are required, your administrative support (legal assistants, services, or office managers) can manage these items.

Small firms may also want to consider investing in a basic document management system and records management system to help manage files electronically. These systems eliminate the need for cumbersome manual processes that are more prone to human error.

As a firm adds lawyers, the business should review its staffing roles and workflow. Are there any roles that are overwhelmed with singular or diversified duties? It's best to perform an analysis of the roles and job duties to identify areas for improvement or restructuring. It's also important to decide which support functions are critical and prioritise new hiring appropriately. While there are times when compliance roles tend to be less of a priority, it's important to dedicate roles to ensure your firm is following policy and procedure. As you grow, your firm must adapt to governance, security, and compliance procedures. As with any technology rollout, the implementation and evolution of IG policies and procedures can benefit from a staged approach.

Many firms are transitioning traditional records management staff to broader IG roles that focus on a wider remit of electronic data handling. Traditional records management teams have a great base of knowledge and skills to build and expand a firm's data-management focus. And sometimes a bit of strategic direction from industry IG consultants can help strengthen the program and build confidence in the team (a bit more on this later in the paper).

Where does the IG authority hail from?

Not all firms choose to have a centralised IG authority such as a chief information governance officer (CIGO). Many appoint an individual to take on responsibility for implementing and directing the firm's IG program. This individual needs to be a strategic leader who can provide firm-wide direction to attorneys and staff on all aspects of the organisation's IG efforts. If the firm's IG leader was not identified during the policy-drafting process, assign this role by considering which individuals were most involved in the policy development. This is an area where your firm's leadership champions can be helpful; if you are creating a new director-level position that may be filled either internally or externally, their buy-in will drive approval.

Of course, not all firms have the same staffing needs. Each firm should define its roles and responsibilities to oversee its IG program. IG responsibilities could fall within groups such as:

- General counsel/risk management committee
- Practice group leaders
- Matter billing/responsible attorney
- Records and information governance leaders
- Administrative directors

Who owns each part of an IG policy?

Before reviewing any proposed model for an IG department, it's key to understand the difference between the generally accepted roles of IT, Information Security, and OGC. In many smaller organisations, these terms are sometimes used interchangeably or are all managed within one group. When a larger organisation has chosen to form a distinct functional area for each of the three, it is helpful to define the roles and responsibilities to ensure proper management of data. All teams must work and collaborate to facilitate a successful program.

OGC

The General Counsel's office is the primary resource for evaluating risk and providing the appropriate compliance rules to mitigate risk at the level the firm defines as appropriate. Your OGC is your resource for creating procedures and policies such as retention schedules, litigation holds, destruction orders, and client file transfers.

IT

Typically, an IT department oversees the installation and maintenance of computer systems within a firm. Its primary function is to ensure that the systems run smoothly. The IT department must evaluate and install the proper hardware and software necessary to keep the governance tools functioning properly. A useful analogy is a bucket and water: IT is responsible for the bucket and ensuring that the bucket is the right size, there are no holes in it, it is safe, and it is placed in the right location. Other areas are responsible for the water that goes in and out of the bucket, including the quality of the water and that it goes to the right place.

Information Security (InfoSec)

The InfoSec department is responsible for implementing and maintaining organisation-wide information security policies, standards, and guidelines. It provides security awareness education and ensures that everyone knows their role in maintaining security. The InfoSec department provides the mechanisms that support the security program outlined by the policy and is responsible for helping prevent data breaches and monitoring and reacting to attacks. InfoSec sets the policies for how data is secured on the network with a focus on protecting the organisation from external threats. The governance policy builds on this framework and focuses on the internal security of and access to data.

In summary, IT provides the framework/infrastructure for information management, InfoSec uses tools and skills to protect the infrastructure from internal and external threats, and General Counsel provides the guidance and mandates on ethical and regulatory standards. All three make up parts of a successful IG program. An IG program may fall under the auspices of any of these groups or could be its own "C" group that incorporates direction from each.

Using firm structures to identify liaisons

Strategic partnerships between groups are a must. In addition to the people who are officially assigned to an IG program, identifying liaisons or change agents in other administrative and practice groups will supplement the staffing plan. These liaisons can be those that have excelled in their compliance, those that have reformed from needing assistance to high IG achievers, and those that demonstrate they understand and are invested in the firm's IG program. Finding these liaisons to assist with various groups across the firm, e.g., different regions, practice groups, etc., helps ensure that the IG program is both socialised and takes account of specific issues from these individual groups. And establishing cross-functional working groups, with a regular meeting cadence, to both inform and make decisions, can be very effective.

Structure/responsibilities

Some key IG-related roles within a firm include some or all of the following, noting that the official department they sit in may vary:

Records staff help lawyers and staff carry out their responsibilities under the policy to manage active matter files in various ways, including:

- Conduct periodic reviews to identify materials for which retention requirements have been met.
- Secure retention review approvals and disposal of records in accordance with records destruction procedures, including but not limited to the certification of destruction once completed.
- Ensure that retention and disposition take account of issues such as client directives found in outside counsel guidelines, ethical walls, mandated preservation, or destruction.
- Maintain detailed and accurate records of retention implementation for all matters.
- Provide records and information management orientation to incoming lawyers and staff and ongoing support as needed.
- Report compliance issues to leadership as appropriate.

In addition to these traditional records roles, an IG unit may oversee the firm's privacy, matter mobility, and/or knowledge management programs. If it does not, it will need to develop working relationships with each of these groups to ensure individual needs are taken into account.

Practice group leaders/administrative department heads ensure that every person who reports to them is in compliance with the policy. Each of these units may designate one or more group members to liaise with the IG staff.

Matter responsible attorney or designee is responsible for ensuring that client-matter files are maintained as required by the policy.

Matter billing attorney is responsible for the matter and client relationship and should be consulted with questions regarding maintenance of client-matter files as required by the policy.

Potential outsourcing

As with any staffing reorganisation, there is always the possibility of outsourcing the entire team or taking a hybrid approach. It typically works best for the strategic leadership functions of the team such as the CIGO, director, managers, etc. to be in-house employees, as they tend to know the inner workings of the firm and are more invested in its success.

However, outsourcing tactical functions of the team is an option. For example, many firms have decided to outsource core records management functions such as file creation, circulation, and scanning of files. This allows the leadership team to focus on tasks such as matter mobility, retention, and disposition and data classification.

An example of outsourcing: Firm X's IG organisation consists of in-house leadership responsible for the policies, technology, strategy, and operationalisation of the IG program. However, this same firm also partners with an outsourced organisation to perform tasks such as digitisation, physical records management tasks, and disposition processes. Personnel management tasks reside with that outsourcing entity, but the team works under the supervision and instruction of in-house IG leadership.

Gain firm buy-in for staffing

As is the case with the launch of your IG program, gaining buy-in for staffing is key. Due to high-profile security breaches and increased data privacy laws and regulations, many firms have been successful in hiring staff to support defensible deletion and classification of data. What used to be a backburner task has recently moved to the top of the pile. Firms realised very quickly that they needed to dedicate either a single resource or team to ensure data is classified and deleted in a timely manner. Procrastination in this area is no longer an option. And the recent evolution of artificial intelligence (AI) is bringing into question the balance of destruction vs. using data to build AI knowledge sources.

Another option is to hire from within and further build the skills of legal assistants. Because legal assistants are on the front lines, they are uniquely positioned to assist with tasks that support enforcement of the overall IG policy. They can help with tasks such as data classification, file management, and matter security. They may also be valuable resources to help with lawyer buy-in.

The evolving role of chief data officer

As data continues to grow, we're seeing the rise of more roles at the C-suite level in regulated industries and law firms. A chief data officer (CDO) is becoming more common within larger companies that have very large data sets that must be managed to benefit the business. Capital One appointed the first CDO in 2002. Only a few organisations followed suit in the decade that followed, and progress in this role has only recently started to gain greater traction.

"The chief data officer is the senior person, with a business focus, who understands the strategy and direction of the business, but their focus is on how to underpin that with data," says Caroline Carruthers, Director at consulting firm Carruthers and Jackson, former Chief Data Officer of Network Rail, and co-author of The Chief Data Officer's Playbook and Data-Driven Business Transformation: How to Disrupt, Innovate, and Stay Ahead of the Competition.

The CDO is a senior executive who bears responsibility for the firm's enterprise-wide data and information strategy, governance, control, policy development, and effective exploitation. The CDO's role combines accountability and responsibility for information protection and privacy, information governance, data quality, and data lifecycle management, along with the exploitation of data assets to create business value. While IG may be a natural fit under the CDO's office, the CDO would be responsible for many other activities related to the utilisation of data, including:

- Operations: Enabling data usability, availability, and efficiency
- Innovation: Driving enterprise digital transformation innovation, cost reduction, and revenue generation
- Analytics: Supporting analytics and reporting on products, customers, operations, and markets

The distinction and interplay between Data Governance and Information Governance can be complex.

Communication and socialisation of IG policies

A law firm's IG policies may be robust and comprehensive, but that matters little if they are not communicated well. Awareness and training are crucial to effectiveness and compliance.

Potential forums for policy communication

According to Prosci Methodology, one must communicate a key message five to seven times for it to be effective—typically employees do not hear or internalise what the business is trying to share when the communication only happens one time. This is certainly applicable to IG policies, which are likely to be just one set of documents a partner or employee is expected to acknowledge and comply with. Fortunately, there are multiple creative ways an IG department can 'market' its policies across even a very large organisation.

Below are a few effective examples:

Orientation

Information Governance policies, at minimum, should be provided to all new partners and employees upon their arrival at a firm. This is especially important in situations where a partner or larger lateral groups are joining and likely transferring several active clients and matters. Additionally, the IG team should be included in any scheduled orientation for a new hire. This creates opportunities for the new joiner to better understand the IG expectations (a more tailored messaging of the policies) and for the new joiner to put a face and a name to the department. This allows for follow-up questions that may arise from new joiners who want to understand how their data is stored and accessible, even if it's reiterating what was previously discussed.

Depending on the orientation timing and overarching attendance, the IG department can tailor its policy messaging based on the needs of the person. For example, in orientation sessions with one or two partners joining from the same firm, it may be valuable for the IG representative to understand the type of culture those partners are used to. Simple comments such as "I'm completely digital" or "Are you the person I contact about my paper files coming over?" provide some understanding as to where there may be potential areas of easy compliance, or where there will likely need to be more training and follow-up.

IG awareness sessions

Using opportunities for engagement and traditional "selling" methods can also help drive policy messaging and reception. Presentations or "roadshows"—especially ones that have incentives such as free meals, swag, or raffles/drawings—can attract people and ensure that they are hearing the salient points of the IG policies in a more digestible way. With many firms working in a hybrid structure, collaborative technology can also make virtual town hall sessions engaging, offering people an opportunity to provide their feedback/questions in a way that helps ensure continued engagement. While the main talking points about the policy should remain the same, especially across offices, practice groups, and departments, the how, the why, and the 'what's in it for me?' messaging can and should be customised to the audience and the current environment of the firm to ensure better understanding and adoption.

Consider whether the office is undergoing a move or renovation, whether the firm has recently adopted a more hybrid working structure, or whether new technology has been implemented. Example, "the document management system (DMS) is the official repository for the matter record" can be a uniform policy message, but explaining how the firm is addressing the increasing adoption of Microsoft Teams through this same policy statement will likely carry a much more powerful impact. For a broader discussion on the challenges of and best practices around implementing Teams, please see our 2020 paper, The Impact of MS Teams on Law Firm IG.

Presentations can take the form of the traditional one- or two-hour slide deck approach, or shorter more targeted bursts, such as a table in the firm lobby with swag to grab attention or a few minutes at the beginning of a practice group meeting.

While presentations are a good way to communicate policy messaging, this shouldn't be the only way IG awareness happens. Platforms and opportunities for the message recipients to ask questions, provide feedback, or pose scenarios are ideal for ensuring what may not be clearly outlined in the policy. Circling back to the prior example of the policy statement, "the DMS is the official repository for matter records," if users have an opportunity to ask questions about how to use certain features of the DMS, or if they have opportunities to share concerns about using the DMS, there are not only opportunities to drive better policy compliance and understanding, but also to ensure that potential technical issues are addressed, learning hurdles are removed, assistance is provided, and/or that individuals are working more efficiently.

Elevator pitches

Elevator pitches have long been used to deliver important messages in short and sweet bullet points; they present a perfect opportunity for IG practitioners to distill IG policies into simple messaging, tailored to the persona. They can also present a significant benefit for a larger firm with a larger, multi-structured IG organisation; they provide a uniform set of talking points and can ultimately become a semi-mantra for more junior-level IG practitioners who may be asked ad-hoc questions or to provide guidance on the ground.

Impactful messaging: Potential policy communication methods

The forum by which policy communication is delivered is certainly important, but so too are the methods the IG practitioner uses to deliver the message. Simply regurgitating what is in the policy documents will not achieve the desired levels of understanding and compliance; creative messaging, "real-life" examples and statistics, or gamification, however, can create more user engagement and better messaging retention.

Creative messaging

During the late 1990s, the Allegheny Health Department in Pennsylvania leveraged well-known literary classics—specifically, creating adapted paragraphs illustrating the woes of unsanitary conditions—to remind people of the importance of washing their hands in public restrooms. Through the usage of humor and well-known and beloved characters, the important but otherwise obvious and somewhat uninteresting instruction—"wash your hands"—became more memorable to the recipients. Creative types of messaging for IG policies can have a similar effect. Somewhat "dry" topics to an end user, such as proper filing repositories, document retention, or lateral intake, can seem less dry with attractive branding, humor, or even themes that resonate with people. One firm, for example, created a horror movie–inspired clip to demonstrate why "extra copies" of documents would not be archived as part of the matter file.

Real-life examples and statistics

While the somewhat cliched statement, "You don't want to be on the front page of The New York Times" can lose impact if it's overused, sharing public examples of when and where organisations who failed to comply with (or potentially did not have) IG policies created reputational and financial damage can emphasise why following a particular IG policy is so important. These examples should be carefully considered for relevance before using them, however; using a larger financial institution can drive a point home, but a law firm of similar size and demographics may be much more impactful. The goal is to create a "This could have been me/us" reaction to change or solidify behavior; ensuring the example is one that resonates with the reader is critical to achieving this. And of course, be careful when using examples that may involve clients, as there may be sensitivities as to how you use their name, even if taken from public references.

Gamification

Gamification of IG policies can be done in multiple formats. It can be as simple as a quiz, or something more elaborate to illustrate why a particular policy is important. Some potential ways to gamify IG policies are:

- Create a searching "fire drill" (with fake documents) to demonstrate the importance of filing in established repositories and being able to search for a document in a short period of time.
- Provide a listing of pseudo client/matters with corresponding pseudo-retention information to have the user calculate the destruction eligibility date.
- Establish policy "badging" to recognise policy compliance, such as when an attorney responds to a disposition notification by the IG team, or when a secretary ensures written client instruction is provided for a file transfer to the necessary parties, and that the proper protocols are followed.

- Partner with other groups such as InfoSec to create the IG equivalent of a phishing test to demonstrate how the IG policies can be applied daily.

It's often stated that attorneys are competitive by nature, and as such, gamification can certainly create healthy competition among practice groups, offices, or even individuals.

Policy training

Just as policy acknowledgment and policy awareness are critical parts of adoption and compliance, so too are education and training. Virtual training delivery (and in-person, when sensible) are certainly part of most training program designs, but there are additional considerations as well, especially when considering training on IG policies:

- CLE accreditation: While not always feasible, having a policy-related class that would constitute CLE credit for lawyers is certainly an attractive way to gain user attendance and participation. Incorporating CLE codes in latter spots of training has historically been used in other programs to ensure attendance remains in place and focused. Work with your OGC or lawyers development teams for options here.

- Persona-based training: while some IG policy messaging is uniform across the firm, other portions are not relevant to certain groups, titles, or regions. Keep in mind that the "what do I have to do?" or "what's in it for me?" questions are the ones people most likely want answered. Consider having training that is focused on certain groups of individuals, with aligned messaging and instruction. Also look for opportunities to "horn in" on their own training initiatives or team meetings.

- Requirements for interaction: Incorporation of knowledge checks or "acknowledgment buttons" throughout can be an easy and practical way to ensure users are paying attention. If other policies, such as information security, require verification, see if IG can be tagged onto that.

Much like policies, policy training should be reviewed annually to ensure up-to-date information and that any knowledge checks are relevant to common IG challenges.

Compliance and enforcement

Ensuring compliance with the firm's IG policy is not for the faint of heart. This is where tracking the "areas of opportunity" for non-compliance becomes a key part of the initial groundwork that needs to be done while planning a schema for sustainable and actionable IG.

General compliance challenges

The first challenge is to identify the greatest areas of risk. Prime among those are unsecured data repositories susceptible to breach, improper application of and non-compliance with legal hold conditions, complying with agreed-upon client directives through Outside Counsel Guidelines (OCGs), and any logistical challenges of complying with client or regulatory requirements. Ensuring compliance involves:

- Developing a prioritisation strategy that captures the most frequent and highest risk areas of opportunity based on risk, representations, and achievability/ resources

- Identifying top firm pain points

- Assessing terms in agreements/representations with clients; finding the commonality among them and determining how to address client requirements that may conflict with firm requirements, policies, or practices

- Tracking and incorporating governing regulations/ ethical rules into processes

Metrics and tracking

The ability to measure and properly track the overall compliance of your firm's practitioners and staff with its IG policy is a highly desired state and provides several key practical benefits. Having a good measure of how well your firm is complying can be easily leveraged for client and regulatory agency audits. In addition, the increased due diligence being performed by insurers in issuing cyber insurance to law firms is also a key consideration for having an audit trail supporting IG compliance. Tracking elements include:

- Dashboards. Developing dashboards is a way to glean information about user behavior, particularly in assessing filing behavior. Empty folders, user activity across the DMS, email mailbox size and organisation, usage of network and local drives can all be surfaced in a well-designed dashboard using any of a multitude of providers in this space.
- Defining approved repositories and creating a data map. Once assessed, user behavior in the approved repositories (e.g., DMS, structured file shares, defined Teams sites), use of those repositories on macro and individual user level, and misuse of the folder structure—one catch-all folder as dumping ground—can be surfaced and actioned with awareness and training.
- Addressing non-preferred repositories. Next, non-preferred/approved repositories can be monitored and tracked using file analysis software (e.g. Varonis, Active Navigation, ShinyDocs, etc.) Are these repositories being abused in a way that leaves client data exposed that should be subject to an access rights regime? There also are basic tools such as tree-size reports that can give your team the ability to see spaces on local drives that are not already locked down.
- Managing personal or specially classified information (e.g., PHI/PII). Personal and other particularly sensitive information in both managed and unmanaged repositories pose a particular concern in this age of General Data Protection Regulation (GDPR), and other such regimes. Their treatment is dealt with in more detail in our paper, Privacy, Security, and Regulatory Concerns: Rapidly Changing Technology Footprint in Law Firms.
- Ensuring mandated preservation (e.g., legal hold) or destruction orders are followed
- Taking account of Walls or other information segregation programs already in play, or establishing them if not
- Assisting users with compliance:
  - Prioritising bringing them into compliance, such as worst offender, office, practice group, etc.)
  - Understand user pain points: discomfort with tech; too busy to migrate previous data; no delegate to assist with filing; email (link folders to DMS)
  - Change management for difficult personalities: use success stories from targeted groups before approaching tough outliers
- Identifying potential pitfalls, such as third-party vendor compliance or information-sharing technologies that employees might be using on their own (e.g., WhatsApp, ChatGPT, and consumer-based sharing sites such as Dropbox, if not blocked as part of your IT security controls, chat functionality not under your control/retention)

Measure against client OCGs

- Effective firm IG compliance must incorporate the directives that come from clients, in the form of OCGs, engagement letters, or other sources, such as audit request reports. A firm needs a process that tracks these directives and ensures they are followed. If the client directive is extraordinary or too onerous for the firm's current processes, identify how a negotiation with that client can take place to find a better path.

Attestation

- Several methods can be employed to assess and encourage users' compliance with client-mandated IG-related operations. Good business intake or OCG management software offers the option to prompt any user opening a matter, putting in time, or creating a document having to acknowledge that they have read and understand the terms of the applicable OCG. Some firms have used random knowledge checks on OCG terms to be sure people understand and read them.

Technology to help with compliance

Enforcement and/or monitoring are important aspects of a program and cannot be successfully achieved without the use of technology. However, technology is not a foolproof solution nor is it to be used as the sole monitoring and enforcement mechanism.

Basic standard IG technologies, such as a DMS and records management system (RMS), have been in use for years and have become standard in law firms. The use of collaboration tools, such as Microsoft SharePoint and Teams, has become more common in recent years. These are not necessarily meant specifically for IG policy enforcement. They can help with compliance, but only if they're set up properly. Setting up these systems by client matter will make collaboration, access controls, as well as retention and disposition easier. This applies to both on-premises and cloud systems.

Unfortunately, proper setup procedures are often not followed, and the systems are only as good as their setup in both aiding and monitoring compliance. For example, a Microsoft Teams setup that is specifically meant to have collaboration by matter can be an effective way to enforce matter security and ethical walls. It's critical then to implement appropriate retention and disposition policy per matter, which can be achieved if the initial setup of collaboration software is done in accordance with the policy (e.g., considers the retention period of the data, limits access to people assigned to the matter).

It's crucial to discuss all governance policies with the IT teams responsible for the setup. In fact, all collaboration tools should be set up with the policy in mind for best compliance. There are, as mentioned already, security and access controls built into most of the tools. It's therefore important to have a clear checklist of IG policy items that you'll want incorporated into the technology tool. The checklist has to be short, easily accessible, and written in terms that are understandable by each team that needs to implement them. For example, if OCGs require certain access controls and the policy discusses it, the step can simply say that the security team needs to set up access controls for the Teams site in accordance with the ethical wall outline. In other words, make sure the checklists are easily digestible and stored in an easily accessible location, such as your firm Intranet site.

Email filing is still a process that many firms find difficult to enforce. In addition, WhatsApp and other texting technologies have become popular (despite prohibition of use of these in some firm policies), and filing only occurs if the lawyer summarises the conversation in a separate memo to the file. Compliance there may still be a challenge, and organisations need to consider ways of setting up procedures for archiving messages.

Many of the IG policies are driven by OCGs, and those can certainly be encoded in the DMS and RMS. Likewise, it's also essential to encode those in the security tools used outside of those systems.

For security purposes, there are both micro and macro issues that must be implemented. On the macro side, all access to a firm's systems and data must be carefully protected whether in the cloud or on-premises. This is doable and enforceable with many automated tools. Here, IG needs to discuss requirements for various data with the security team. Typically, the team is excellent at protecting perimeters but not great at protecting data assets. This should be discussed as access to certain data areas must be restricted based on matter access controls. Automatic technical processes for protecting data security should be active. Further, the security of data should be synchronised to be automatically reflected when personnel leave or join the firm, and when they are reassigned to various matters. IT security teams have technology to do that, and it's important to request the audit reports from those systems and review them monthly to ensure compliance is maintained; focus on changes.

Further, it's important to discuss with the security team how they restrict email from flowing to unintended parties. There have been products such as data leak prevention (DLP) tools that are prevalent in the financial sector to enforce or monitor policy violations. There are newer tools that tag data with self-destruction tags if it is sent outside the firm, thus limiting data loss. Because most of these tools are implemented by the security team, it is best to be involved in their planning and to determine whether more extensive monitoring is needed or possible.

Part of the IG policy almost always includes legal holds. The days of manual legal holds, where a custodian is responsible for the execution and preservation are (hopefully) long gone. If the firm wants to implement the policy, legal hold software is required. Such software finds the appropriate information and either preserves it in place or makes a copy of the information and stores it for further examination and production. There are many examples of these products, such as Epic, Intapp Walls, Exterro, Ipro, and OpenAxes to name a few. This paper is not an endorsement of a specific product.

The legal hold steps can be fully automated, so compliance can be guaranteed with the right automation and procedures.

Technology used in the firm

It's important that the checklist we referenced above is applied to all applicable technologies used within the firm. We already mentioned collaboration tools such as Teams, and of course any DMS, RMS, and DLP systems in use must be set up this way. If other cloud-based software is used, ensure that the cloud provider allows flexible policies as well as appropriate retention, disposition, and removal of information and guarantees that disposition procedures comply with firm guidelines.

In complying with OCG requirements and in keeping the firm safe and secure, all third-party vendors should undergo an assessment. It's possible to implement vendor assessment tools such as Prevalent and Privva to help make sure that vendors are in compliance, keep track of their answers, and issue any remediation requests. Automating the process is a more effective way of ensuring compliance than collecting manual answers.

It's also important for the firm to conduct internal compliance assessments to ensure the requirements of the IG policies are being met. This can be effectively automated in the vendor assessment software used to assess external vendors.

Frequency of policy reviews and updates

Ensuring that your policies are regularly reviewed and up-to-date is a key part of your IG program. Out-of-date policies create confusion for your user community and can also increase the risk of people not following proper protocols and even misrepresenting client requirements. Having well-written policies, with the appropriate level of detail, helps ensure that they do not need to be rewritten often. And as much as you may think that people in your firm hate policies, you'll often find that lack of policies can be even more frustrating. Many people are thankful for clarity and guidance when they receive policies.

Frequency

Generally speaking, an annual review cycle is a good frequency for your policy management program. This allows your team to plan structured time for reviews without requiring too much time for the task. It's also a good way for your IG team to stay current with what is being communicated to and expected of your user community. If you have an extensive set of policies, it may be helpful to divide the set into quarters. You can then set an annual review cycle for one-quarter of your policies to be reviewed each quarter. This helps make the review tasks less daunting and keeps policy familiarity within your IG team fresh throughout the entire year.

There will be circumstances that call for mid-cycle or more frequent reviews. Examples include changes in legislation, such as GDPR, significant system changes that impact how your data is stored or processed, or a pattern of changing client requirements. Client requirements should be monitored holistically, ensuring that you are not reactively changing your policies for one specific client or client requirement without considering how the change impacts the full population (including other clients) to whom the policy applies.

Additionally, your policies, if written at the right level, will not require updating for every new technology or change. For example, when Microsoft Teams first came out, many IG teams wrestled with the volume of policy change required based on this significantly new platform. But upon further review, many firms with well-written policies realised that although the technology platform was a sizable change, the underlying governance for that platform still applied. Things such as retention for messaging, how data is stored, and access controls for teams and channels could be driven in ways similar to existing platforms such as Skype, DMS, and file shares.

Another important point to consider in your review frequency decision is that updates to your policy can trigger re-attestation requirements. Your program should include clear indication of what triggers a requirement for re-attestation. Anything that has an impact on requirements for how your users operate should be communicated to all those to whom the policy applies. Some examples here would be password length/complexity requirements, file-saving protocols, and retention requirements.

Process

It's beneficial to establish a process for how your policies will be reviewed. This includes who is involved, what triggers or drives changes to your policies (see above Frequency), and how those changes are tracked, approved, and communicated to all those to whom they apply.

Reviewing policies is not the most exciting work for everyone. Therefore, creating a process that is manageable and achievable goes a long way in helping ensure its success. If you have multiple people on your team, you may consider dividing the detailed reviews among your team members. Assigning policies to those who work most closely with the content can help ensure reviews are as relevant and applicable as possible.

Another approach is to have each team member present the policy highlights and suggested changes to the other members of your team. This helps ensure that everyone on the team is familiar with all of the policy content while balancing the workload across the group. It also allows for good discussion among the team and may even spark healthy debate in some instances, driving your team to think deeper about the various topics. You can also encourage your team to consider recent support calls, common questions, or interesting scenarios they've encountered to determine if these can drive valuable edits to the policy to continue to strengthen them and make them as relevant as possible.

You may want to consider forming a policy review committee. Regardless of how formal or extensive your team is, the review process should include **senior leadership**. This helps ensure that there is executive support for your policies, and should challenges arise related to executing or implementing policies, leadership can support the IG team in compliance efforts. You may also want to consider including stakeholders from various functions on your review committee. People such as secretaries, paralegals, departmental leads, and others who are most impacted can offer valuable insight on realistic workflow/execution, and can go a long way in supporting more seamless and successful implementation. These committee members can also help with the marketing aspect of policy adoption, as the message of policy adherence often resonates best when it comes from those "in the trenches."

Your **policy template/format** should include a revision-tracking page. This is a key component of audit and client review functions, and your policy review cycle should include a consistent method for updating the tracking page. This typically includes who reviewed the policy, the date it was reviewed, and a summary of changes (or notation that no changes were required/made).

Your policies are a key part of your IG program. Once they're in place, having a structured focus on how to implement, staff, manage, communicate, train, track, and maintain them helps set your program up for success. And your program will be ready for the rapidly changing world of technology, information, and data governance ahead.

IRON MOUNTAIN®

1300 476 668 | ironmountain.com/au
0800 732 255 | ironmountain.com/nz

About Iron Mountain

Iron Mountain Incorporated (NYSE: IRM), founded in 1951, is the global leader for storage and information management services. Trusted by more than 220,000 organisations around the world, and with a real estate network of more than 85 million square feet across more than 1,400 facilities in over 50 countries, Iron Mountain stores and protects billions of information assets, including critical business information, highly sensitive data, and cultural and historical artifacts. Providing solutions that include secure storage, information management, digital transformation, secure destruction, as well as data centres, art storage and logistics, and cloud services, Iron Mountain helps organisations to lower cost and risk, comply with regulations, recover from disaster, and enable a more digital way of working. Visit www.ironmountain.com for more information.