IRON MOUNTAIN®

CLIENT INFORMATION GOVERNANCE REQUESTS: HOW THE LANDSCAPE HAS CHANGED

2021 LAW FIRM INFORMATION GOVERNANCE SYMPOSIUM

CONTENTS

AUTHORS:

BRIANNE AUL
Firmwide Senior Records and Information Governance Manager
Morgan Lewis & Bockius, LLP

MAUREEN BABCOCK
IT Business Operations Manager
Snell & Wilmer L.L.P.

CHUCK BARTH
Director of Information Governance
Sheppard Mullin

ANDREW CORRIDORE
Information Governance Compliance Manager
Akin Gump Strauss Hauer & Feld LLP

LEIGH ISAACS
Director, Information Governance
DLA Piper

NORMA KNUDSON
Director of Space Planning and Compliance Support
Faegre Baker Daniels

JESSICA MARLETTE
Information Governance Counsel
White & Case LLP

JAMES MERRIFIELD
Director of Information Governance & Business Intake
Robinson and Cole

JILL STERBAKOV
Manager, Information Governance Compliance
Morgan, Lewis & Bockius LLP

JOHAN WIDJAJA
Assistant Director, Records and Information Governance
Morgan Lewis

JOHN ZAHRADNICK
Business Development Lead
InOutsource

INTRODUCTION

The Law Firm Information Governance Symposium (LFIGS) wrote our seminal white paper on Outside Counsel Guidelines (OCGs) in 2014 and has since added to it with entries in 2016 and 2018. Client guidelines may come in the form of OCGs, engagement letters or client agreements and, collectively, are referred to as Client Information Governance Requirements (CIGRs). Our papers discuss the opportunities for law firms provided by CIGRs and how Information Governance (IG) professionals can help promote various initiatives by focusing on the topics that clients care about. In addition, we've included a myriad of practical and specific assistance, such as best approaches for setting up CIGR intake procedures, some typical client technology requirements, and ways to better partner with your General Counsel. Chances are, if you have a specific question related to CIGRs, we've covered it before or it's addressed in this paper.

The goal of this paper is to dive into some topics in more detail while also exploring some new topics that have become increasingly important. Where in past papers we briefly touched upon Firm priorities and initiatives that can be furthered with CIGRs as featured considerations, in this paper we delve further into how you can leverage client mandates in a big way. We also get into some best practices by giving anecdotal evidence on what's been working, what hasn't, and what we plan to try next.

The last three years have brought a lot of changes to the information landscape and with that comes meaningful changes to the mandates issued by our clients. To that end, we take a look at the Association of Corporate Counsel (ACC) guidelines and how best to develop a standard approach. We also explore the new normal of remote work and how clients are changing their requirements to account for this new way of working.

So let's kick this off with a look at how to leverage client requirements to drive our own Information Governance initiatives.

ENGAGEMENT LETTERS V. OCGS

Engagement letters have been a mainstay of law firms for many years. Traditionally, the engagement letter informed the Firm's approach to managing certain key administrative areas for each client. In addition, many U.S. states require a signed agreement between the Firm and its client; the engagement letter checked that compliance box. As early as 2010, clients began to implement their version of the engagement letter with OCGs. In 2014, LFIGS wrote its first paper about OCGs called "Outside Counsel Guidelines Management: An Information Governance Issue," and in 2016, published another entitled "Staying in Compliance with Client Conditions." Both provide useful background on OCGs.

Two of the most common documents passed between a law firm and a client are engagement letters and OCGs. Engagement letters are usually initiated by the billing and/or responsible partner who has a direct relationship with the client. They are typically drafted from a common outline, which lays out the legal relationship between the client and the law firm, such as rate structures, billing procedures, indemnification and dispute resolution, among others. All of these subjects were, and are, quite familiar to an attorney. As clients began to send OCGs to their lawyers, a responsible partner within the Firm again approved and then signed them on behalf of the Firm. This created problems for Firms, as partners well-versed in contract law were not as knowledgeable in the operations, policies and controls used in other areas of the Firm. OCGs were being approved that contained requirements that the Firm simply could not meet as specified by the client.

Client requirements within the OCG are predictably unpredictable and can vary widely between clients. What one client specifies in great detail in an OCG, another may not even mention. General clauses, such as those requiring the Firm to comply with "all applicable international, federal or state law" are easy to acknowledge, but harder to comply with unless the Firm or practice group provides additional direction. Attorneys who are experts in their chosen areas of law may not be conversant with the current requirements of state, federal and international privacy laws and how those laws affect how client information is handled. With no reference to requirements specified in both the engagement letter and the OCG, Firm personnel may be complying with engagement letter requirements that have been changed or superseded within the OCG. An attorney's lack of complete awareness of the requirements as specified in both documents is not an acceptable reason for noncompliance.

All law firms struggle with this lack of uniformity. Hours of staff and attorney time are required to review client OCGs and then gather and formulate responses. This has added significantly to the overhead of administrative groups who must not only communicate, and often explain, what the client wants, but then must also wrangle attorneys, support staff and, at times, vendors and service providers to get the needed answers. Firm administrators typically have to absorb this additional investment of time and effort using their existing resources.

Complexity increases when reviewing the documents considering:

- sections within the OCG may supersede or fundamentally change what was originally agreed to in the engagement letter
- both documents are often composed and sent to your Firm by client personnel (or third party consultants) working in different departments who often have little knowledge of or connection to each other, and
- OCG requirements for compliance in specific areas may be counter to the Firm's policies or to legal constraints.

Firms need an effective way to identify and manage the terms and conditions in both the engagement letter and the OCG. Without that, they will be unable to evaluate information to support compliance with the terms or conditions within each document, as well as understand when further clarification with the client is required. One or both of the documents may need to be modified to define clearly which document, or section of a document, will prevail if there is competing or conflicting language.

For your own IG personnel, you must establish an accessible, concise and current summary of requirements for easy reference. You may want to obtain an acknowledgement from the legal team that they have read, and will comply with, the posted requirements.

It is a fair assumption that some law firms will continue to review, process or regard engagement letters separately from OCGs. With the proliferation of privacy laws and technological advances in response to malware, along with up and coming AI capabilities, now is the time to re-evaluate and improve your Firm's management and compliance with the terms in engagement letters and OCGs. To do so, you will need to identify, and rely on, your Firm's administrative stakeholders whose job responsibilities most closely align to the requirements sections of the documents.

IMPACT OF CIGRS ON FIRM PRIORITIES AND INITIATIVES

Let's face it, getting the buy-in for that shiny new software or new initiative is often tougher than we'd like it to be. As IG professionals, we tend to press for initiatives that, to put it simply, manage data more effectively or reduce overall risk. When we bring these initiatives to executive management, often the first question is, "how much time and/or money will this cost the Firm?" This doesn't mean that executive management doesn't care about the reduction in risk, but how we frame our needs may make all the difference in getting approval. CIGRs might just help us do that.

Requirements are becoming more rigorous each year. Processes that started out with simple engagement letters between an attorney and their client have evolved into complex review processes with stakeholders from every side of the business - more on that later. Today, CIGRs cover everything from legal terms, billing guidelines, IT security and data privacy, diversity minimums, annual rate reviews, and the list goes on. We've established that we can no longer address these requirements in a vacuum, viewing them each individually in the context of the particular attorney-client relationship. Firms must take a holistic approach to identifying common requirements across client engagements in order to ensure compliance. When we take this crucial proactive step, we can synthesize all of our client requirements to determine where they overlap with our own initiatives, and we may also identify requirements that force us to reassess our initiatives.

Clients no longer want to hear that a requirement is on the roadmap; they want to see progress. Identifying common requirements is a key factor in prioritizing future projects and initiatives. When we can identify the stakeholders, we can assess the impact on the Firm, and when we can identify the clients, we can assess the bottom-line impact to the business. For instance, data privacy requirements have exploded over the past several years, and Firms that tie those requirements back to key clients have been able to justify the spend. Client requirements around rate increases may spark discussions and new processes to ensure attorneys proactively review rates to ensure the Firm takes advantage of opportunities to increase rates, which may also lead to better practices with other clients.. Whether it be information governance, administrative, or financial requirements, taking a holistic and centralized approach will help drive initiatives within the Firm.

CIGRs come to us in a variety of forms, some more formal than others. The two most common formats are the "Engagement Letter" and the "Outside Counsel Guidelines." Now that we have an understanding of the types of CIGRs and potential impact to the Firm as a whole, let's focus on the varying departments that may be impacted.

OCG PROVISIONS IMPACTING MULTIPLE ADMINISTRATIVE GROUPS

In previous papers on managing client directives, we addressed the process of identifying the groups in a Firm that are potentially implicated by these directives and how to establish a process that ensures these groups receive the guidelines. A Firm's administrative stakeholders in the CIGR process include: New Business Intake, Information Technology, Information Security, Accounting/Billing, Human Resources, Office of General Counsel, Privacy, Facilities, Marketing, Vendor Management, Diversity and Inclusion and, of course, Information Governance/Records Management.

CIGRs are disseminated to applicable stakeholders via either a decentralized or centralized approach.

In a decentralized approach, the recipient of the CIGR sends them directly to others in the Firm associated with the requirements. This approach places more responsibility on the attorney, or other original points of intake, to ensure the Firm's CIGR dissemination and tracking process is followed. As such, all possible entry points must be educated as to the necessary steps in order to ensure a complete and accurate response.

A centralized approach provides the point(s) of intake with a single contact who is responsible for CIGR distribution and follow up. That single contact may be a single custodian, who can maintain a central repository of CIGRs received by the Firm. Alternatively, it may be a task force/committee, a group of individuals representing different functional areas who collectively respond to CIGRs, or a small committee comprised of individual custodians who collectively work through CIGRs with department representatives. In each case, the collective is a single point of contact, typically through an email distribution list or automated workflow solution.

Either of these structures enable the recipient stakeholders to review the CIGRs and identify the provisions applicable to them. Much of the time, what applies to whom is obvious, e.g., allowable entries for bills go to Accounting, or encryption standards go to Information Security. However, often there are terms that can affect the operations of more than one stakeholder in the Firm. For example, a section on "confidentiality of information" may have specific impact for Information Technology, Legal/Risk, Privacy, IG and others. Or the billing section may address the retention of records post-matter closure that substantiate the statements.

If you're an IG professional in search of items in the CIGR relevant to your law firm's retention process and you find a section on "record retention," you might be tempted to limit your review to this piece. Typically, if such a section exists, it describes expectations for the return, maintenance and destruction of client materials, such as originals and work product performed on behalf of the client. It may mandate a communications process regarding records management at the end of the Matter.

Even if your scope of responsibility is limited to managing the records retention and disposition process, your CIGR review should not end there. Terms related to requirements for retention and disposition of information related to representation often exist in sections that belong to other departments in your Firm. Those aforementioned "confidentiality of information" terms may be in an entirely different section, in an attachment or addendum or even in a client audit. While a record retention section requires the Firm to maintain a copy of the client file for a period of time following a Matter closure, that "confidentiality" section might dictate the return or destruction of information it deems confidential immediately after it is no longer required to service the Matter.

Your CIGR process may have designated the responsibility for ensuring a client's specific confidentiality terms be met by other groups, such as Privacy, Information Technology, Information Security, or your General Counsel. CIGRs sometimes, but not always, provide a definition of what it considers to be the "confidential" material that requires additional steps beyond those described in its records retention section, and such a definition may help clarify which group owns the responsibility to accomplish those steps[1]. If not, it is advisable to seek clarification from the client.

Conversely, a "Record Retention" section could contain a directive that might fall more squarely within the bailiwick of your Firm's Billing, IT, Privacy or other department. For example, it may state technical requirements for the manner of returning client information, specific steps regarding storage of physical records (which may implicate Facilities), or retention terms regarding records it expects you to keep to substantiate bills.

Communication is crucial in these crossover scenarios. A plan for dealing with terms that affect multiple administrative groups or directives a team may not have initial access to (e.g., an IT security addendum or client audit) should be baked into the CIGR process. In both a decentralized or centralized approach where an individual is responsible for maintaining a database, a readily available list of contacts designated for CIGR management in each administrative group facilitates the sharing of information and apportions the responsibilities for these crossover terms. Where a CIGR task force or committee oversees the process, it is best to determine which terms may cross over into different groups and develop a plan to determine who will take the lead to respond.

Accomplishing all of these recommendations manually is time consuming and prone to error or omission. Technology and workflows can help better enable this process and minimize risk and cost associated with manual processes.

WORKFLOWS AND TOOLS

The old adage of process before technology still holds true – nothing has changed there. In order to capitalize on new technologies to significantly improve the efficiency of your CIGR processes and minimize associated risks, you need to first have a handle on your CIGR processes, the good and the bad. The following are workflow decision points you need to have in place before embarking down the road of a CIGR technology project:

- **Corral the troops**. We've discussed the impact of CIGRs on multiple groups. Gather the appropriate representatives from those groups early on.
- **Consider the scope.** Are you only using this process for engagement letters and outside counsel guidelines? What about business associate agreements? Given the types of questions and responses required under RFPs and security assessments and questionnaires, should you extend the process to include this type of content as well? Each of these processes represents a level of commitment to clients.
- **Vendor capabilities**. Just as clients impose mandates and assess their law firms, law firms similarly need to impose mandates and assess their vendors. Increasingly, CIGRs mandate that law firms have such procedures and controls in place. Template Master Service Agreements have become commonplace in many Firms and are designed to ensure vendors provision software or provide services in a manner consistent with the Firm's CIGRs. This "kitchen sink" approach provides a safety net, but may result in drawn out negotiations around terms that are not relevant to the vendor or service.
- **Centralize the process.** Is there an intake process for CIGRs? Do they come in haphazardly and/or sit in siloes?? We recommend a centralized approach, even operating under a manual process, to minimize risk and ensure consistent responses. Designate who should have primary responsibility – Compliance/Risk, Security, IG, General Counsel, Business Intake, etc.
- **Centralize the information**. Just as with all the other administrative and client-related information in your Firm, CIGRs should also follow proper information governance. They need to be in a central location and restricted/locked down to the appropriate individuals. This process is critical, not only for managing the guidelines, but also for performing an analysis of the current requirements "in effect" today.
- **Define systems impacted.** As you analyze the requirements and expectations set forth by CIGRs, you'll need to define the impact on existing systems. What systems store Client-Matter information and how do your key requirements impact them? If a requirement calls for records to be stored for longer than your standard retention period, can your records management system log that policy? Understanding the natural lifecycle of data in your current systems provides additional insight on what deviations the Firm can or cannot accommodate. Knowledge of your limitations not only helps you avoid risk, but allows you to prepare alternative resolutions to meet in the middle when your processes can't accommodate an initial request.

- **Analyze key terms and requirements.** What are the key terms or provisions that need to be reviewed? Can you categorize them? When performing this analysis, it is critical not only to discuss concerns relative to each department or practice within the Firm, but also to analyze how they tend to appear or how they are referenced in different CIGRs. For example, there may not be a specific records provision although there are provisions that relate to records referenced as return of materials, data, or information. Getting ahead of this analysis prior to the implementation of a new technology or process will better inform project discussions and potentially identify processes that need to be revisited. Though CIGRs can include everything under the sun, these are some of the most common terms:
  - Billing and rate changes
  - Confidentiality
  - Records Management and Information Governance including data segregation, data residency requirements and retention
  - Information security, audits, and breach notifications
  - Third party/vendor management
  - Diversity, equity, and inclusion standards
  - Conflicts and Waivers
  - Privacy and Personal Data Protection
  - Intellectual Property Rights
  - Liability-related provisions including indemnification and force majeure
  - Cyber Insurance
- **Determine a baseline for acceptable criteria.** Template responses for key requirements or criteria not only streamline processes by making decisions easier, they standardize answers to ensure responses to our clients are consistent while minimizing risk by ensuring staff do not consent to terms that cannot be implemented. In addition to standard templates, you should also decide on acceptable deviations. For example, if the default retention rule for a record is seven years, what is the longest period the Firm is willing to hold the information - 10, 20 years? Although your default language for breach notifications may be "reasonable," can you commit to a more defined timeframe, such as "48 hours?"

DEFINE THE RISK APPETITE.

It is nearly impossible to achieve 100% compliance, especially given the evolving regulatory landscape within the U.S. and beyond. What we can do is set a threshold of reasonable risk laid out by General Counsel in order to have a consistent practice. Each General Counsel will have a different risk appetite and may ultimately need to make a decision about the level of risk with which they're comfortable. We may not achieve perfection, but we can achieve consistency.

Addressing the above considerations enables you to turn to technology to enhance and optimize your CIGR process. It can include simple mechanisms like spreadsheets, some incorporation of workflows, or more automated solutions such as auto-tagging, machine learning or AI. Some Firms use SharePoint workflows or capitalize on contract review software that analyzes provisions and identifies deviations.

There are now products on the market specifically designed for the CIGR process. Some, like Aderant's OCG Live, focus on specific pieces of the CIGR process. Others, like Intapp Terms and HBR CounselGuide, focus on the entire CIGR process. You may have other tools in your organization, such as Kira or Luminance that can be leveraged for the CIGR process. Many products tend to capitalize on tagging and AI to intake the CIGR, identify the key terms and deviations, route provisions to the relevant team for review if needed, and retain the entire collection for ease of reference going forward. Given the cross-functional collaboration required during the CIGR process, you may want to consider hiring a consultant to assist with implementation and/or requirements gathering. Bringing in a technology partner, with subject matter expertise, adds a neutral party to guide discussions,ensures that risks are being carefully considered and that technologies are being utilized to their maximum.

These CIGR products have benefits that can extend far beyond improved efficiency, depending on how your Firm implements them. For example, if you integrate the product with your billing system, you can notify partners 90 days before rate increase expiration dates. Non-billable items and time entry requirements are also important provisions that impact the financial value of the Matter. Careful consideration of these terms can help ensure the Firm optimizes Matter revenue and profits. In addition, if you have a Matter summary available for your partners (for example, a Matter page on your Firm's intranet), you could integrate and push the CIGR key terms there to ensure the entire Matter team has visibility of those requirements. You can give the attorneys and legal administrative assistants a user-friendly format that breaks down the structure of the relationship and their duties during the engagement. This may be helpful for partners to know, but also for associates who never get to see the guidelines or the engagement letter and are just basically told what to do. Such a depiction of responsibilities can be a useful tool to learn the rules of the road, ensure client expectations are met, and transition staff.

Before pursuing an AI-based technology solution for CIGRs, it is critical that you first consider the resources you will need to teach the tool and review and refine its accuracy. Depending on the scope of content and the volume of CIGRs, your Firm may only need one or two resources, or you might need an entire team. Since AI is only as good as the underlying data, your implementation journey may reveal additional data clean-up or migration efforts that need to be undertaken. These are important factors to include in the discovery phase of your project.

> WHILE TECHNOLOGY, WORKFLOW AND AUTOMATION TOOLS CAN ENHANCE EFFICIENCIES AND OPTIMIZE YOUR PROCESSES, THEY ARE ONLY AS EFFECTIVE AS THE UNDERLYING PROCESSES ESTABLISHED. EXPLORING BEST PRACTICES FOR MANAGING CIGRS WILL HELP ESTABLISH A SOLID PROCESS FROM WHICH TO BUILD YOUR TOOLS.

PROVEN PRACTICES

Standard Operating Procedures. While it's already been discussed, it's worth reiterating that one of the most effective best practices for managing CIGRs is to have a documented process that is well-advertised and followed. Having a process isn't enough if your attorneys at large do not know it exists. Make sure that someone within your Firm is regularly evangelizing your process or ensuring it has high visibility. It is imperative to communicate to your attorneys that it is inadvisable to sign any agreement with a client without a careful review with your compliance and approving authority.

Workflow. Your process should follow a standard workflow that ensures all stakeholders who need to review an OCG can do so in an efficient and documented manner. Generally speaking, the General Counsel (or their designee) or a compliance entity at the Firm has the final approval on an OCG and signs on behalf of the Firm. Automated workflow systems for CIGRs that guide the process and capture data for reference are becoming more prevalent. Research what may work best for your Firm - either an electronic workflow system or a consistent manual process could accomplish the same goals.

Roles & Responsibilities. If you choose not to invest in an electronic workflow system, you should consider designating a centralized role to shepherd all CIGRs through the review process for ultimate approval. This centralized position ensures every CIGR gets a review from stakeholders such as Information Security, Conflicts/Compliance, IG and Billing/ Finance. The findings should be consolidated and then presented to the approving authority for their consideration.

Reference Bank. Many CIGRs are fairly standard, with some exceptions. It is another best practice to maintain a reference "bank" of approved Firm responses. This reference guide can simplify the review process and ensure that there are consistent responses to client demands. Document what your Firm's capabilities are to provision for data management, access, retention and destruction and the level to which your Firm is equipped to comply. With this documentation, you can create templated response statements on approved retention schedules, billing options and practices, security measures and any other topics you would generally flat out decline.

Breach Notification. Pay special attention to any short response time for breach notifications, such as within 24 hours. Since breaches can be open to interpretation, you should clearly identify how the client defines a triggering event. Ensure the provisions are reasonable and that your Firm is able to comply.

Indemnification Clauses. Prudently negotiate such things as Indemnification Clauses. Understand any implications to malpractice insurance.

Tracking Key Provisions. Implement a process and platform to capture and track key provisions to help aid with compliance and expedite the review and approval of any new CIGRs. Ideally, provisions should be grouped or categorized so they can be easily sorted. Establishing a process for distributing key provisions helps ensure that all who need to be aware have current and up-to-date information.

Central Repository. In addition to tracking key provisions, it is helpful to establish a central repository for CIGRs. This allows for quick access and/or re-distribution when there is a need to reference. There is no one way to accomplish this. Some Firms have leveraged their DMS, some have used SharePoint, or another internal collaboration platform. Ideally, whatever repository you choose should allow for security to be applied and provide the ability to easily search and find content using a variety of parameters.

Managing Policy Exceptions. If possible, leverage the new business intake process and systems to automatically apply any policy exceptions to content stored in Firm repositories. Some of the security/ethical screen or records management applications already in use at most Firms have the ability to accomplish this. Automation brings efficiencies and reduces the likelihood of human error when tracking and complying with various CIGR terms.

Privacy Considerations. While there are many criteria that need to be tracked, an increased focus remains on privacy compliance. Thus, it is increasingly important that you engage your privacy attorneys (or whomever is your internal subject matter expert) to ensure that any requirements and requests are not in conflict with any laws, rules or regulations and that they are appropriately tracked.

Documentation. Consider having the client sign an engagement letter in addition to the acceptance of the CIGR. Having the Firm engagement letter tends to supplement sections that may not be covered in CIGRs and billing requirements to benefit the Firm.

Let's now expand on the best practices to discuss the value, importance and impact of standardization and guidelines.

REMOTE WORKING ENVIRONMENTS AND THEIR IMPACT ON CIGRS

Remote working was not a new concept within law firms prior to the COVID-19 pandemic. Attorneys were often expected to be immediately responsive, regardless of geography or time zone. What was unprecedented was the immediate loss of access to office buildings and the corresponding services typically inherent within those locations – including onsite IT and IG support, printers/scanners, shredding services, and in-person meeting/collaboration areas and opportunities. Moreover, administrative staff members (many of whom had never worked remotely) were also forced to quickly adjust to a virtual environment, while at the same time being responsive to the needs of both attorneys and clients. The ability for Firms to adjust and adapt fluctuated from organization to organization, which resulted in varying degrees of service to clients – many of which were struggling with similar challenges. The need for e-signature software, collaboration platforms, and other means of communication with clients became paramount, which meant cloud-based platforms that may have otherwise been discounted suddenly became critical.

This "next normal" is likely to find its way into the CIGRs of the future, both in terms of additional IG-related requirements that a client could impose, as well as client requirements that will ultimately have an impact on a Firm's IG program. The following are examples of what the IG practitioner should consider and be prepared to incorporate into the practitioner's governance protocols.

REMOTE WORKING ENVIRONMENTAL SECURITY

In 2020, the perception of remote working transitioned from a temporary inconvenience to a long-term benefit, and many organizations (including law firms) are preparing for flexible working to be ingrained into their daily cultures even after the pandemic ends. As such, CIGRs will likely encompass additional security considerations through the lens of working from a personal residence, especially with regard to data access, data disposition and data portability. If not already incorporated, CIGR security provisions will likely include requirements on how data is to be secured in a home residence when not in use. This could include shorter screen timeouts, additional restrictions on shared personal devices, and additional employee security training on how to store and secure data when not in use. Clients may prohibit printing their data, and/or require Firms to provide further documentation of destruction when the data is being destroyed by the individual as opposed to an established shredding program and vendor. Fortunately, Firms have most of these facets incorporated into established policies and training, and it will simply be a matter of modifying the messaging, expanding the audience, increasing the frequency of training, or a combination of all three. Enforcement will be a larger challenge, however, and likely where most Firms will need to focus their attention.

COLLABORATION

As mentioned above, collaboration tools became a necessity for attorneys and their clients. Microsoft Teams, in particular, became a primary channel through which attorneys communicated with their clients, and vice versa. Clients will likely continue to leverage collaboration platforms as a means to work with their attorneys and to share/obtain associated work product, which may ultimately be incorporated into their CIGRs. While Firms will need to be accommodating, they will equally need to ensure that their attorneys and staff understand where established Firm policies must still be adhered to, including the storage of Matter work product in the document management system, or the retention of data within the collaboration tool and its impact on what and where certain data can be stored.

DIGITIZATION AND OWNERSHIP OF CLIENT FILES

Many clients have already established expectations in their CIGRs regarding when and how records will be returned to them at the conclusion of the Matter. However, as mentioned earlier, clients of unprepared law firms likely experienced delays in response time due to the inaccessibility of certain records, especially in situations where the documents were a) in paper format, sitting in a now-restricted office building, or b) in digital storage, but not readily accessible to an attorney who relied on his or her now-remote assistant to locate files for him or her. Clients may not only expect that their Matter files remain digital throughout the course of the Matter (including the digitization of records not already in that format), but also that they are stored in a way that allows the client direct access to them throughout the entirety of the Matter. Again, accommodating this potential new guideline should not deter a Firm from its established IG protocols regarding official Matter repositories, but, much like COVID-19 itself, it could also serve as an opportunity for outstanding IG digital initiatives to get the necessary funding and support.

RETENTION

While many clients assume or expect that their Firms have established retention policies and programs, still others expect Firms to retain their Matter files indefinitely, and/or at least be able to provide a quick answer to them based on the history of Matters they worked on. As Firms continue to look for opportunities to reduce unnecessary costs and/or ways to leverage cloud-based systems, the opportunity to reduce physical and digital data for closed Matters will become more attractive for Firms to implement. This may require additional negotiations with clients that mandate longer retention periods that may have otherwise been readily accepted in the past.

STANDARDIZATION AND ASSOCIATION OF CORPORATE COUNSEL ("ACC") GUIDELINES

As illustrated in this and prior reports, CIGRs have been part of the legal vertical for more than a decade. However, their evolution tends to be a reflection of current client challenges, and range from regulatory compliance (i.e., security and privacy requirements) to general cost-reduction efforts often stemming from an economic downturn. Therefore, it is presumed that the COVID-19 pandemic and, specifically, the temporary-to-permanent remote working structure, will also find its way into future CIGRs. Fortunately, with the ACC data steward program, law firms may also find new opportunities to demonstrate to clients their ability to consistently align and comply with requirements commonly found in CIGRs, thereby reducing or eliminating the need to address numerous CIGRs with similar controls and requirements.

ACC DATA STEWARD PROGRAM

While CIGRs may touch on general themes of security and could include some specifics, sophisticated clients typically also perform a comprehensive audit of their legal counsel. The process is costly for the clients and the law firms, where multi-day, on-site evaluations are not uncommon. In advance of the on-site evaluations, clients usually send all-inclusive audit questions regarding the Firm's security and governance profiles. Collectively, law firms can have a bank of thousands of individual responses to the audit screening questions, possibly strewn across multiple Excel charts or databases, that continue to grow. As discussed above, we are expecting that these audits and screening questions will elaborate on the new issues that COVID-19 response has introduced. Clients that have the resources to perform these audits usually do this on an annual basis, providing a snapshot of the status of the security and governance profiles of their legal providers. But the process is cumbersome, costly and not standardized across clients.

On the other hand, other clients may not have a way to assess the security and governance profiles of their legal services providers. They may not know where to start, or do not have the internal resources to perform the sophisticated audits.

The ACC recognized that many of its members were faced with these situations and decided to come up with a solution -- the ACC data steward program -- that was borne from the needs of members themselves.

LEGAL INDUSTRY-SPECIFIC STANDARDS ROOTED IN INFOSEC FRAMEWORKS

The ACC facilitated the collaboration of both law firms and in-house counsel to create the standards and controls for the data steward program framework. The working group consisted of cybersecurity attorneys, CIOs, General Counsels and technical experts from both the corporate legal department and law firms, basing the agreed-upon controls on common frameworks, standards and regulations, such as GDPR, HIPAA, NIST and ISO 27001[2]. While some law firms might already have their ISO certifications in place, having a focused approach to select and manage standards that are specific to the legal industry maximizes the time and value spent to assess these benchmarks. Additionally, having the relevant parties in constant communication on this topic and building willingness to efficiently address new issues that might arise sets the stage for continuous improvement on these controls. They are housed and presented to participating law firms in a web-based portal, negating the need for additional tracking charts. The first step is a self-assessment, working through the various controls, which in turn translates into a compliance score. A law firm can then share as much or as little of the results of the self-assessment, available in downloadable reports or dashboards, with a client, or provide the client read-access rights to the platform. Having a dynamic platform where controls are updated by the ACC continuously and made available to participants allows the law firm to maintain and manage these controls and provide its clients with real-time insight into its security and governance posture, as opposed to an annual audit snapshot.

CLIENTS ARE STILL IN THE DRIVER'S SEAT

We can foresee that clients will start to reference the ACC data steward program specifically in CIGRs, especially since the ACC is trying to socialize the platform and standards heavily among its 10,000 members, taking advantage of the fact that the assessment was created by their peers. There is no charge for corporate legal departments. Instead, the costs of participating in the program are shifted to the law firms and legal service providers. Furthermore, clients may ultimately want an independent verification of the self-assessments performed by participating law firms. To that end, the ACC offers an accreditation process whereby ACC-accredited assessors validate the results, and, if satisfactory, designates the Firm as "ACC Accredited." Currently, the platform offers a "core" module, which pulls from the above-mentioned standards, and the ACC is planning an "advanced" module in the future.

FACTORS FOR ACC DATA STEWARD PROGRAM SUCCESS

Acceptance of the ACC data steward program by both clients and law firms as a suitable set of controls and standards will ultimately determine the success and adoption of the program. Clients will need to affirm that the program offers all of the controls they deem necessary. For example, there may be ISO 27001-specific controls that were not incorporated by the working group into the ACC program, but are still important to certain clients. If this is the case, clients will likely continue to try to meet more comprehensive, specific and stringent standards, and might reply to the law firm that compliance should cover the ACC program as an umbrella.

Additionally, for sophisticated law firms, there may be other valid reasons to comply with security standards beyond trying to meet client-driven directives, Firms simply want to be prepared to secure data as best as possible. Again, if there are efforts already underway, Firms might incorporate any ACC standards within the more stringent assessment.

For those Firms and corporate legal departments that might not know where to start, the ACC programs seem to hit the mark. There seems to be no downside for a client to request that its legal services providers assess their security postures using these standards, assuming they are sufficient. From the law firm perspective, there might be an initial cost, but ultimately winning the work and future work, while validating the security posture, is a compelling argument for participating.

Lastly, the ability to efficiently incorporate issues that need to be addressed by new threats or circumstances will be very attractive to clients and law firms alike. Giving the clients the platform to call out specifics, such as any of the issues mentioned above related to remote working, and having the law firm address them in real time (as closely as possible), will surely give both parties confidence that the appropriate measures are in place.

CONCLUSION

As we evolve into a post-pandemic world, and are increasingly subject to changing laws, rules and regulations with regard to privacy and security, the landscape and requirements associated with CIGRs will be dynamically changing. There is no one-size-fits-all approach. It is important to understand varying aspects about your Firm and your Firm's clients, such as geographical footprint, culture and risk tolerance. That said, it is imperative that Firms dedicate time and resources to implement a CIGR program that can adjust as needs and requirements change. IG professionals can play a key role in driving this process, and are uniquely positioned to bring all the various stakeholders together to ensure the development of an agile, all-inclusive program.

If you'd like to read more from LFIGS about CIGRs, please refer to our past reports:"Staying in Compliance with Client Conditions" and "Practical Solutions to Implement Client Information Governance Requirements."

ENDNOTES

[1] ACC 2017 Guidelines (Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential Information) define the following as company confidential information: Attorney-client privileged; Confidential information which, if disclosed, could damage the company; Material non-public information concerning publicly traded companies; Personally Identifiable Information (PII) for any company employee, contractor, customer or supplier; Protected Health Information (PHI); Information related to physical security of company operations; Information related to company's cyber security; Information that may incriminate the company (e.g., lead to fines/penalties/litigation/reputational damage); Information that is required to be protected under applicable data laws and regulations. The ACC guidelines direct outside counsel to return, delete or destroy such information when no longer necessary to service the matter, but carves an exception for day to day email exchanges that do not contain confidential information and outside counsel work product.

[2] https://www.accdatasteward.com/service/.

IRON
MOUNTAIN®

800.899.IRON | IRONMOUNTAIN.COM

ABOUT IRON MOUNTAIN

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

USLGL-RPT-072821A