IRON MOUNTAIN®

PRACTICAL SOLUTIONS TO IMPLEMENT CLIENT INFORMATION GOVERNANCE REQUIREMENTS

2018 LAW FIRM INFORMATION GOVERNANCE SYMPOSIUM

CONTENTS

TASK FORCE LEADER & AUTHOR

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

TASK FORCE AUTHORS

DERICK ARTHUR
Director of Records & Information Governance
King & Spalding LLP

SCOTT CHRISTENSEN
Vice President
Olenick & Associates

KELLY FARMER
Director of Information Governance
Latham & Watkins LLP

MICHELE GOSSMEYER
Global Director, Information Governance, Risk and Compliance
Dentons US LLP

LEIGH ISAACS
Director, Records & Information Governance
White & Case LLP

SHARON KECK
Lead Consultant; Records, NBI, and Information Governance
eSentio Technologies

SAMANTHA LOFTON MOSS
Chief Risk and Information Governance Officer
Ice Miller LLP

RANDY OPPENBORN
Director, Information Governance
Foley & Lardner LLP

ROBERT WEAVER
Chief Risk & Security Officer
Blank Rome LLP

KATHERINE WEISENREDER
Information Governance Compliance Manager
Cooley LLP

TASK FORCE ADVISOR & AUTHOR

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

INTRODUCTION

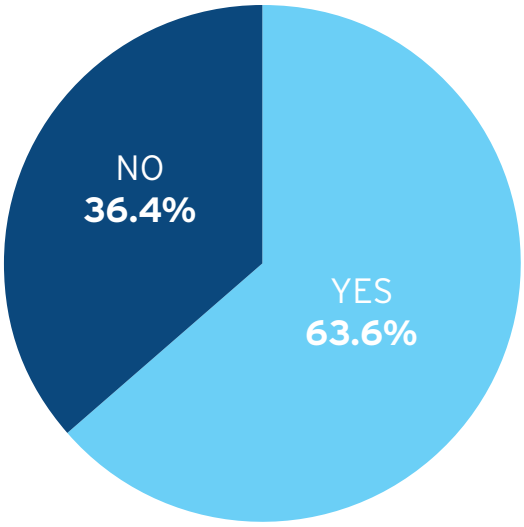
As discussed in the two prior Law Firm Information Governance Symposium (LFIGS) reports, Outside Counsel Guidelines and Staying in Compliance with Client Conditions, client Information Governance requirements (CIGRs) provide an opportunity for law firm Information Governance (IG) practitioners to promote and obtain support for their various initiatives. Additionally, they illustrate the importance of firms having established policies and procedures regarding IG-related processes such as retention, destruction, security and third party-relationship management. In firms with more mature information governance programs, CIGRs typically provide IG practitioners a "seat at the table" to review, identify and assess which client-related IG requirements the firm is asked to implement. At the highest level, IG efforts can provide valuable client collaboration opportunities to further strengthen relationships and fortify future business opportunities.

However, CIGRs can also be challenging to incorporate into a firm's overall infrastructure. Firms may incur significant costs to repurpose real estate or purchase new technology to secure a client's physical and electronic information. They may have to create exceptions within their standard policies, schedules and workflows to accommodate a CIGR. Vendor relationships may be impacted, either by implementing new requirements or securing new vendors to handle specific client work in its entirety. CIGRs can trigger significant changes within the firm's culture, particularly when a culture has deep roots that have grown over many years.

Critical to any CIGR implementation is proper communication with clients and auditors regarding status and any approvals needed; with vendors so that they are aware of and can meet expectations; and with internal personnel, so that they not only understand what they need to do to comply with a CIGR, but ultimately what benefit the firm may receive by incorporating the CIGR into their environment. Equally critical is ensuring that once the CIGRs are implemented, the firm takes steps to monitor and audit that they remain in place. Over time CIGR requirements may change, or additional requirements may be provided to the firm based upon the current security landscape and possible risks to client data; as such, the overarching practice of periodic review should be constant, and firms must remain adaptable.

This paper identifies the IG processes that are often impacted by CIGRs, and some of the challenges and cultural concerns with incorporating them into the firm's environment. This paper provides examples of how the firm would implement these CIGRs even in situations where they may deviate from the firm's standard culture. Additionally, this report gives examples of how technology may ultimately help the firm manage various requirements efficiently.

HAVE YOU CHANGED YOUR IG POLICIES OR SECURITY PROCESSES IN RESPONSE TO SUCH DOCUMENTS IN THE PAST YEAR?



SOURCE: ILTANET.ORG, 2017 STUDY OF THE LEGAL INDUSTRY'S INFORMATION SECURITY PRACTICES, (LAST VISITED FEB 2018), HTTPS://WWW.ILTANET.ORG/VIEWDOCUMENT/2017-STUDY-OF-THE-LEGAL-INDUSTRYS

It is important to note that each firm will need to address CIGRs differently, even within client industry verticals, so there is no universal solution or one-time application of firm guidelines or processes to ensure compliance with CIGRs. Factors such as firm size, geographic landscape and client base impact an IG program's structure and approach. Implementing a control framework can help ensure that all the standard controls are in place, but each client's assessment process is generally going to have their own approach, scope, depth and breadth. Each firm needs to have the capability to receive these guidelines, parse the data and boil it down to the specific controls that are needed. Governance teams who analyze the requirements need to work together with risk, information technology ("IT") and other parties to identify the items; if a firm does not have a governance team, then someone will need to ensure this work is completed.

TO READ OTHER REPORTS WRITTEN BY THE LAW FIRM INFORMATION GOVERNANCE SYMPOSIUM, PLEASE VISIT: SYMPOSIUM.IRONMOUNTAIN.COM

INTAKE, REVIEW AND ORGANIZATION OF CIGRS

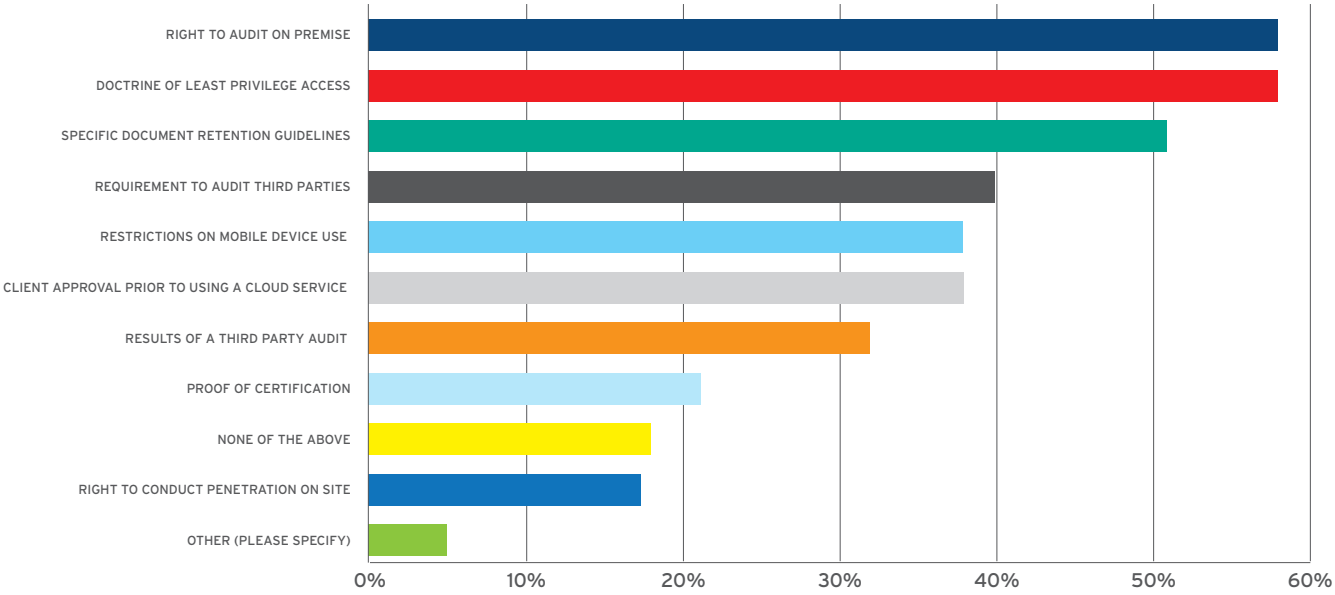
CIGRs come in many forms: most often, they are incorporated into outside counsel guidelines or negotiated as part of the client engagement letter. However, they also come in the form of security questionnaires, onsite audits, RFPs and business associate agreements. Moreover, they often arrive at the firm's doorstep via multiple avenues and at various times during the course of the matter, e.g., to the business development team during the RFP process; to the billing attorney in conjunction with new matter intake; to the lawyers during the course of the matter; to the security team during an audit, or to the finance team in connection with billing.

Because CIGRs can impact many different constituencies within a law firm, a well-communicated, effective intake procedure for dissemination and review of CIGRs is crucial. This ensures each impacted group is notified of and has access to the requirements, can advise on their capacity to meet those terms, or offer alternatives that work for both the firm and the client. It is also important that each group knows who within the firm is responsible for communicating with the client to come to agreement on the terms.

To assist with ongoing compliance of the requirements, a firm ideally should have a centralized depository that accounts for: access for all impacted groups; version control; ease of updates and ability of each impacted group to identify and pull the section of the requirements that directly affects them. The form of this depository can vary based on the needs of the firm and its policies on storing information. It could be a SharePoint site, a dedicated workspace in a document management system, or access to a due diligence platform that enables users to search and track various agreement clauses based on their needs.

SPECIAL RECORDS CLASSIFICATIONS/HANDLING

CIGRs are increasingly calling for special requirements for handling information. These requirements can include: (a) least-privilege requirements (i.e., securing documents solely to the team working on a matter); (b) classification scheme requirements (i.e., requiring firm personnel to label documents according to the client's classification scheme; (c) restrictions on where data may be stored and transferred; (d) encryption of data at rest; and (e) encryption of data in transit. The following diagram highlights the type and frequency of CIGR requests.



SOURCE: ILTANET.ORG, 2017 STUDY OF THE LEGAL INDUSTRY'S INFORMATION SECURITY PRACTICES, (LAST VISITED FEB 2018), HTTPS://WWW.ILTANET.ORG/VIEWDOCUMENT/2017-STUDY-OF-THE-LEGAL-INDUSTRYS

"LEAST PRIVILEGE" REQUIREMENTS

Some clients require firms to implement a "least privilege" security model. In other words, the firm is required to lock down the clients' documents so that only individuals working on their matters can access them. There are several challenges posed by these requirements that firms need to work through.

First, clear parameters are not always provided. Make sure that you work through details with clients to ensure their requirements can be executed as intended. Examples of areas for discussion/clarification:

- Does the requirement apply just to documents the client provides to the firm or also to the work product the firm creates? (These types of documents may be stored in different repositories and handled differently.)
- Can rights only be granted after approval by someone on the matter team? If so, who on the matter team can approve? The billing attorney? Relationship partner? Other?
- Instead of pre-approval, is it sufficient to notify the billing attorney or someone else on the team so that they may object and have access removed after the fact?

- How do requests for least privilege apply within your staffing structure? Clarify which teams within your firm are authorized to work across matters for key support and service delivery (e.g., document support staff, knowledge management professionals, etc.)

- Will the client allow the work product to be shared if it has been "cleansed"? If so, consider who is able to cleanse the document – it may need to be individuals on the authorized matter team if others (e.g., knowledge management team, third-party vendor) are not permitted to see the uncleansed documents.

- Is there a requirement to "recertify" rights after a certain number of days/months and remove rights for individuals who have not billed time during that period? Some document management systems limit the ability to modify and/or remove rights from the author of a document for record-keeping or historical file-tracking purposes.

Once you clarify the intended outcome, it is important to devise a way to alert technology support staff to the client's specific requirements. If you do not have processes in place for this purpose, a user may call the help desk and be inadvertently granted rights. A potential way to avoid this situation is to name security groups in a particular way that signals the technologist that additional steps must be taken before adding the person's name to the group. Another possibility is to flag a client who has special requirements in the firm's help desk software.

Finally, a least privilege model may present challenges if it is antithetical to the firm's culture. If lawyers are used to being able to search across all documents looking for precedent, they may find a least privilege model limits their ability to leverage existing work product. This historically has benefited clients by reducing the number of hours they are billed.

Even if the firm has a strong knowledge management team to help create precedent materials, lawyers may still feel handicapped if they are unable to search across all documents, especially if they are looking for an obscure piece of work product. Highlighting client requirements often helps with these discussions. Additionally, partnering with your knowledge management teams (or similar groups) is key to successfully facilitating collaboration and balancing security with workflow efficiencies.

CLASSIFICATION SCHEME REQUIREMENTS

Another popular condition in CIGRs is a requirement that the law firm follow the client's data classification scheme. This poses a number of practical challenges for a firm. First, how do you ensure that everyone who works on a matter knows what the specific classification requirements are for the particular client? From whom do they seek guidance if they do not know how a particular document or set of documents should be classified? If a lawyer works on matters for several different clients, all of whom have imposed unique classification schemes, how will the lawyer remember and apply the different requirements? These are hard challenges to overcome, but it may be helpful to periodically communicate to the timekeepers on the matter reminding them of

the classification scheme requirements (with a link to or attachment that includes the requirements).

PRACTICE TIP:

YOU MAY BE ABLE TO COLLABORATE WITH THE CLIENT TO DETERMINE IF THIS KIND OF REQUIREMENT IS NECESSARY, GIVEN HOW THE FIRM TREATS ALL INFORMATION AS CONFIDENTIAL. ALTERNATIVELY, YOU MAY BE ABLE TO LIMIT THE SCOPE OF THE OBLIGATION TO IMPLEMENTING THE CLIENT'S CLASSIFICATION SCHEME'S REQUIREMENTS ONLY FOR INFORMATION PROVIDED BY THE CLIENT.

JURISDICTIONAL RESTRICTIONS ON WHERE DATA IS STORED/ TRANSFERRED

Clients may require that certain information not be sent to a particular geographic location, or that information be stored in, and cannot leave, a particular geographic location. Understanding the reason for the restriction is critical: is it to avoid seizure of documents or data that is physically located in a particular jurisdiction? Or is it to avoid having a governmental body obtain jurisdiction over the client, expanding the client's potential liability? It is also important to understand very clearly which information poses the concern so that you can focus on the appropriate repositories – is it the information the client supplies the firm? Or does it also apply to the work product that the lawyers generate? All of this must take into consideration compliance with rules and regulations regarding cross-border transfer of data. Knowing what the concerns are will help you determine the appropriate solutions.

In our ever-connected world, it can be difficult technologically to actually limit the geographic locations where the data is stored. The network architecture for many firms is designed to make it easier for individuals to work across offices. Cloud storage can make knowing when data is stored more complex. In addition, there are technology administrators who need to have rights to many locations in order to support systems. You should work with your technology team to ensure that the permissions are set correctly and that you train administrators not to grant themselves rights to "restricted" data.

Email is particularly problematic because of the way it is routed: email servers may be centralized or regionalized and contain emails for individuals across multiple jurisdictions. Moreover, depending on how email is configured, the messages may be cached onto an individual's laptop computer which the individual may then take with them on a trip to the prohibited jurisdiction. Ensuring that matter team members understand the restrictions is critical.

All of this becomes increasingly important for firms dealing with EU data as part of the new General Data Protection Regulations (GDPR), effective May 25, 2018. As a result of new data handling requirements, violations will result in significant penalties/fines.

PRACTICE TIP:

WHEN DISCUSSING A JURISDICTIONAL RESTRICTION WITH A CLIENT, BE SURE TO POINT OUT PRACTICAL LIMITATIONS POSED BY THE REQUIREMENT. FOR EXAMPLE, IF THE CLIENT REQUIRES PRIOR NOTICE BEFORE INFORMATION CAN BE SENT OUTSIDE A JURISDICTION, EXPLAIN THAT IF IMPLEMENTED COMPLIANTLY, A LAWYER WHO WISHES TO COMMUNICATE ABOUT A DRAFT WITH ANOTHER LAWYER IN THE SAME FIRM LOCATED IN A DIFFERENT COUNTRY WOULD FIRST HAVE TO GET CLIENT APPROVAL, WHICH COULD IMPACT CLIENT SERVICE AND DELIVERY TIMELINES.

ENCRYPTION OF DATA AT REST

Many clients request that their data be encrypted at rest. This means encrypting data stored on workstations, servers, tapes, DVDs and CDs, thumb drives, hard drives, etc. This requirement poses several challenges, one of which is slowness to encrypt, retrieve and search encrypted data. The encryption method used may cause data compression efforts to fail and could impact eDiscovery efforts

to analyze data. Other challenges to consider include: encryption key management, safeguarding of keys, costs to replace hardware (particularly if not in line with budget cycles), addressing unencrypted tapes stored offsite and technical inability of software to encrypt.

To meet these challenges, the firm can consider moving data to an offsite storage vendor or colocation (colo) site, where an organization can rent dedicated space for servers and other hardware. Most new data centers encrypt data at rest. As you vet SaaS vendors, you should ask about encryption at rest. Vendors may have enhanced data security options that include encryption at rest or this may be a special request to be included in a service level agreement.

When discussing encryption requirements with the client, include controls such as routine reviews of data center access logs, video camera alerts for unusual activity, monitoring and logging to determine who is accessing what data, etc.

ENCRYPTION OF DATA IN TRANSIT

Other challenges include encryption of data in transit which is the requirement to encrypt data during transmission. Often clients require that all communication relating to their matters leaving the firm be encrypted which can present a series of challenges. The easiest way to cover this requirement between the firm and the client is to use a Transport Layer Security (TLS) solution which encrypts all email sent between two domains. It is easy enough to set up forced TLS with the client by connecting the technical email teams of both parties. As an alternative, third parties may be engaged to implement forced TLS. There are a few ways to tackle this:

- the client matter team identifies all of the email domains they will correspond with and provide technical contacts to get TLS set up,
- TLS is set-up to push a firm's standard certificate to a domain, that when accepted by the recipient creates the secure connection,
- use an e-mail feature such as Mimecast and train users on secure send features,
- as a compensating control, deploy Data Loss Protection (DLP) or other rules-based software tracking of e-mail. The DLP application, dependent on the sophistication, could either prevent and/or report flagged data movement such as keywords (e.g. 'confidential') or particular syntax (e.g. social security number, credit card number, etc.). Options 3 and 4 are typically used in conjunction with policy. A notice to the client matter team of the requirement and compliance reviews of data leaving the firm should be in place to coincide with the technical controls.

Another challenge is ensuring that all members of the client team are aware of the requirements being requested of their law firm. If individuals at the client ask the firm to send data unencrypted, the law firm's IG and Technology staff need to ensure compliance of agreed requirements while meeting deadlines and not frustrating the firm matter team or client. Staff should be empowered to push back, with the basis for the encryption requirement and have an escalation path through the firm's Risk Counsel. A compensating control could be to use a provider to send secure files to the client or other parties on the clients' behalf.

It is a balance to ensure that the client's technology and security restrictions are compatible with encryption options. Some secure methods of transfer are blocked; for example, downloads to the firm's secure file transfer, reading from encrypted flash drives and executables running from a software-encrypted DVD.

INFORMATION RETENTION, DISPOSITION & MATTER MOBILITY

REQUIREMENTS TO RELEASE OR DESTROY THE CLIENT FILE

Some clients have concerns about how long law firms retain their information. Many law firms have records retention policies that indicate how long records must be kept past the close of a matter. The retention periods are based on state and federal regulations, statutes of limitations for a legal malpractice action and jurisdictional opinions and rules (e.g., ABA, law societies, etc.). Increasingly, clients are imposing different retention periods which may be shorter or longer than the firm's retention periods, and instructing their law firms to return or destroy information at the close of the matter. Shorter retention periods can become a concern because the firm may be left without evidence to defend itself in a malpractice suit by the client. It also could be potentially problematic if a dispute arises with the client with respect to fees.

When discussing these requirements with the client, it can be helpful to have an actionable records and information policy and a retention schedule, along with procedures for consistent compliance monitoring already in place. It is also helpful to include explicit language regarding these issues in the engagement letter.

A client requirement for any retention period different than the firm's own established retention periods adds complexity to the records disposition process. If any different retention periods are agreed to, it is crucial that the applicable firm team is notified so that they can take steps to ensure that the client's requirements are carried out. These may sometimes be trackable in the firm's records management system. In addition, to the extent that the CIGRs provide a particular timeframe in which the information is to be returned or destroyed, the team should be consulted to make sure that the timeframe is realistic. The volume of data may be so large in some situations that a short deadline would be unrealistic. If possible, firms should try to negotiate a provision that is more flexible – e.g., within a reasonable period of time.

Most often CIGRs related to Information Governance fall into two types: retention and access control.

CIGR	SUGGESTED ACTION
Retention of client files is shortened or lengthened	Set up tickler in RMS or other tracking system
Certain information, for example Personally Identifiable Information (PII), should be destroyed immediately after completion of matter (remaining files are retained as per usual)	Set up tickler in RMS or other tracking system
Method of file destruction is specified by client, e.g., cross-cut shredding, DOD5015	Collaborate on options to implement; ensure applicable evidence once in place (e.g. destruction certificate from vendor)
Materials created throughout the course of an engagement should be available on request to the client	Store material in firm-approved repositories with applicable client/matter and other metadata
Client information should be deemed confidential and proprietary with or without markings to the same	Set up physical and electronic data access controls
Information provided by and/or gathered or generated in the course of work should be stored in secure facilities with controlled access and made available to personnel on a least-privilege need-to know basis only	Set up physical and electronic data access controls

Resources that firms have available to them to handle the varied Information Governance related demands vary from tracking via simple spreadsheets to setting up ticklers on matters in a records management system (RMS) or other tracking system. Leveraging privacy controls or setting up walls around information are also useful tools allowing firms to comply with access control requests.

FILE OWNERSHIP

Some clients are including provisions in their CIGRs that the client owns everything the firm creates as part of its representation. In the absence of these provisions, the question of who actually owns the file can be complicated. The answer depends on local ethics rules and bar opinions, as well as local case law. When a matter has files in more than one jurisdiction, the answer is even more complicated: which law applies to which parts of the file?

In most jurisdictions, at least some of the documents created as part of the representation are owned by the firm, not the client. Moreover, some firms' engagement letters state that internal firm communications and memos belong to the firm, not the client. The concern for firms is the potential for second guessing decisions that were made during the course of the representation. If a client requests this kind of provision in their CIGRs, ensure that the Information Governance team is notified about it so that they can ensure that the correct scope of materials are released, since it may be different than their standard approach.

For example, there may be internal discussions about potential strategies to recommend to the client. If the strategy recommended is ultimately unsuccessful, the client (when they request their file) may discover that the lawyers had discussed other potential strategies and argue that it was malpractice to have recommended the losing strategy.

CLIENT COMMUNICATION

Communication with clients in the CIGR process can be loosely categorized into two areas: 1) specific requirements as part of OCGs, audits and assessments and 2) collaboration opportunities to enhance client relationships and further strengthen your IG / Security program. These areas will intersect at various points in your processes. The following are a few examples of these two areas to provide insights and options for your team.

REQUIRED NOTIFICATIONS

Required notifications are fairly specific items that your clients include in OCGs, audits and assessments to ensure that your firm is able to meet compliance and/or key operational requirements. Examples include:

- **Notification of a Security Incident** - Often clients request a 24-hour notice for a breach or incident. While this may work in some scenarios, oftentimes it is unrealistic for a firm to have identified enough detail of an incident or breach to effectively and/or accurately report back to a client. Prompt notification is in the best interest of both parties, and helping navigate communication of an incident is critical to effectively managing impact and mitigating risk. However, providing premature or inaccurate information for the sake of communicating quickly can be even more damaging. Work with your internal teams to reach an agreed timeframe with which you can reasonably and responsibly provide valuable information to clients. Sample language could include:

We will provide notice as soon as practicable after we become aware of a security incident affecting your data, and in no event more than three (3) business days following such date.

- Change to law firm relationship contacts, key staff and/or critical processes - It is typical for clients to request that internal changes be communicated to them. Be sure to review these in light of your structure and processes. For example, it is very reasonable for you to ensure that your client is notified if their relationship partner changes or if you make a major change to the retention policy impacting their materials. However, some requirements do not translate as well to law firms. A request to notify the client whenever you hire an outside contractor for some of your IT functions may be unrealistic and/or unnecessary. Discuss these types of requests with the client to understand the key control they are trying to satisfy. In the IT contractor example, it may be sufficient to ensure that all contractors are under an NDA, undergo background checks and that logons are disabled immediately upon termination.

- Confirmation of annual testing of incident response plan, BD/DR testing or external security audit - The frequency with which client audits and assessments are happening is increasing at a fairly rapid pace in many industries (e.g. financial, healthcare, government contracts), so many 'annual attestation' requirements for testing or auditing are now covered as part of the assessment. However, in many instances, requirements to provide an annual validation of key testing is still in place. You will need to log such requirements and ensure that you have a process to proactively provide your client with needed confirmations. Should something slip through the cracks on your end, your clients will likely reach out with a reminder, but being proactive and taking this task off the list of your client shows that you have an organized IG/Security program and that you take client commitments seriously.

COLLABORATION OPPORTUNITIES

Collaboration opportunities are typically more general ways for you to communicate with your client and work with their assessment teams to highlight the breadth or depth of your program and further enhance it. Strong, experienced assessors welcome the opportunity to engage with their vendors (which include law firms) to have more in-depth discussions around best-practices, new technologies and innovative processes. Security

posture can be a competitive advantage for firms and leveraging the assessor relationship is a valuable way to strengthen the legal industry and its overall client collaboration focus. Examples include:

- **New technologies** - If a general requirement is to ensure that system activities are identified and logged, this may be a great opportunity to review a system or technology that the firm has been exploring or recently implemented. Oftentimes, clients have larger security teams and budgets and have insights on technologies fairly new to law firms. One example of this is threat deception technology which takes the concept of creating 'fake' information on your network so that should a threat actor penetrate your systems, their chances of getting your most valuable data are minimized. This technology also captures and reports on the source of the penetration to further close your attack surface. Discussing these types of technology options with your clients can strengthen their views of your security program, give you contacts for 'bouncing' ideas around and open collaborative dialogue for future risk management opportunities.

- **Extra steps in processes** - If you have taken extra steps or put in additional safeguards beyond the basic requirement, consider sharing them. This shows your focus not only on core controls but that the firm has assessed the risks and determined how further mitigation adds value to your program and ultimately to your client. There is always a balance to the level of sharing versus 'over-sharing', and opening an additional stream of questions regarding your program. Determine the comfort level of both your processes and the assessor to determine the appropriate level of sharing.

- **Asking questions or raising concerns** - many clients conduct numerous assessments. Some are more tailored to the recipient while others are generalized. In some instances, a client's floral vendor will get the same questionnaire as their law firms. There are times when questions are not applicable or when providing the answer to the exact question being asked clearly does not provide the intended or valuable results. In these instances, take the opportunity to communicate (politely and respectfully) your insights and/or suggestions for revisions or alternate approaches. Oftentimes, assessors appreciate the thoughtful review of the question and quickly realize the importance you are putting into the process. Key examples here could include more in-depth discussions around definitions of terms and expectations of processes related to them. Things such as scope of 'breach' notifications and limiting scope to that specific client's data allowing for manageable expectations and the right balance and frequency of updates.

Taking this approach even one step further, if you are being asked to provide something or follow a process that just does not seem right, follow your instincts and raise the question or concern. For example, if you join a screen sharing session with an assessor who indicates at the beginning of the call that they are home with a sick child and taking notes on their personal laptop, you may want to request that the session be rescheduled. Or if your client is using a new third party cloud assessment tool, it is quite reasonable to perform due diligence on the security posture of the third party. As much as it is important to be responsive and follow client requests/processes, always remember that you are ultimately responsible for where you are putting firm-sensitive data. If you have concerns with sharing your data in a way that compromises your security, you need to raise those concerns with your Office of General Counsel or firm management. This could ruffle a feather or two initially, but should the data become compromised, there will be far more feathers ruffled and much more damage to mitigate.

OFFICE OF GENERAL COUNSEL CONCERNS

CIGRs that are contractual in nature should involve review by the firm's Office of General Counsel (OGC) or delegated legal representative. As a general matter, agreeing to any requirement that adds complexity carries the risk of non-compliance, which, in turn, gives rise to potential liability if the agreement is breached.

There are some provisions that raise particular concern for the OGC because they increase the firm's exposure to legal liability. These include indemnification provisions and requirements to comply with laws that do not apply to the law firm directly, but to the client.

INDEMNIFICATION PROVISIONS

One provision that clients often include in their outside counsel guidelines is a requirement for the law firm to indemnify the client for any losses associated with a security breach. This poses concern for a firm's OGC, even if the firm is covered by cybersecurity insurance. The provisions may attempt to shift all responsibility to the firm regardless of who is at fault. In fact, these provisions potentially shift liability to the firm even if the breach is caused by the negligence of the client (e.g., if someone at the client insists that information be sent to him or her unencrypted). You may wish to try limit the provisions to breaches that are the result of the firm's own conduct or lack of reasonable security controls.

> A KEY POINT TO NOTE IS THAT OFTEN INDEMNIFICATION NEGATES INSURANCE COVERAGE AND MAY ACTUALLY BE DISADVANTAGEOUS FOR THE CLIENT.

REQUIREMENTS TO COMPLY WITH PARTICULAR LAWS OR COMPLIANCE REGIMES

Many outside counsel guidelines require the firm to comply with "all laws" or with various specified laws or compliance regimes that apply to the client, e.g. the Gramm-Leach-Bliley Act (GLBA); the Health Insurance Portability and Accountability Act (HIPAA); the European Union (EU) data protection laws; the International Traffic in Arms Regulations ("ITAR"); and the Payment Card Industry Data Security Standard (PCI DSS). Moreover, while the lawyers representing the client may be aware of the nuances of those laws, this is less likely the case for the para professionals who work on the matters or for the staff who support the lawyers (e.g., administrative assistants, document support, practice support, technology support). This can be incredibly difficult for the law firm to navigate, particularly because it may not be clear which pieces of information given to the firm by the client (or created by the firm itself) are covered by these laws. The OGC should make sure that relevant parties are trained in special legal requirements for information handling. IG professionals can assist by developing processes that help ensure requirements are met and providing training on these processes. It also may be advisable to send periodic emails to the matter team reminding them of the requirements.

THIRD-PARTY RELATIONSHIPS

Outside Counsel Guidelines (OCG) often include third party vendor management requirements. Best practices include limiting unnecessary vendor exposure to client data and ensuring that third parties are made aware of the OCG requirements that affect them. Firms should consider tracking these requirements centrally as a part of a vendor management program. Requirements to be tracked include:

- which vendors have access to specific client data
- what type of notice a firm gives the client regarding their third parties
- which requirements vary based on third party terms.

Vendor contracts should be evaluated on items such as, confidentiality, security and data breach notification requirements.

Outside Counsel Guidelines may also include vendor selection protocols which pertain to services such as eDiscovery, imaging/copyservices, facilities management, document services, offsite storage, data centers, SaaS applications, contractors, etc. They may also include an overly broad requirement to approve any vendor prior to use on their matters. An approach to managing this it to create workflows to notify in-house eDiscovery staff of these requirements. Include billing requirements to ensure you do not engage someone the client is not willing to pay. Alternatively, as firms move more toward fixed fee arrangements and legal project management and budgeting, the firm may elect to provide the client a reverse letter with their practices, vendors and pricing to get advance approval before the services are engaged or needed.

Tie OCG management to vendor management to have all new and revised outside guidelines, engagement letters, other client agreements or reverse engagement letters sent to a centralized group that is responsible for an administrative review of these types of agreements. This review would include the following areas: Billing, Diversity, Security, Retention, Notification/Communication, Compliance requirements among others. The individuals responsible for this review should have a good working knowledge of firm policies, procedures and compliance requirements and have the ability to coordinate and collaborate with key stakeholders and departments to ensure that the firm can comply with the control, has the control documented and will hit future targets such as reporting or necessary system audit requirements. This group should also be responsible for escalating to firm Counsel and the Relationship Partner when the firm is not able to comply or needs to further negotiate. One method of doing this is having the relationship partner verbally communicate the firm's capabilities and document that conversation or alternatively send a reverse letter to the client with the firm's capabilities and what the firm will do as a compensating control. Ideally these terms would be negotiated up front and the OCG's would reflect those agreements.

The most critical pieces to OCG compliance relating to vendor management are to actually manage the vendor, to audit the vendor for compliance and to query the vendor regarding agreed terms. This can be accomplished through the firm's vendor management program. A master list of agreed-to terms that map back to ISO/NIST/SANS top security controls relating to various clients is a good tool to use to benchmark against to ensure compliance. Some clients require you to name vendors who may have access to their data in an audit. This is a first step to see if you are in compliance with the OCGs the firm has agreed to. They may then require you to not only produce a vendor management policy but also show evidence of vendor audit questionnaires, onsite visits, etc. It may be best to balance requirements of notifications regarding vendor changes by agreeing that significant changes to terms of the OCGs will be communicated for review and/or appropriate alterations.

STRATEGIES FOR RESPONDING TO CLIENTS' INFORMATION TECHNOLOGY REQUIREMENTS

The majority of client security questionnaires and audit topics involve IT technical controls. Involving your firm's IT group can often help facilitate a smoother process. In many firms, the IT team may even manage the client security control process. Here we outline some of the key lessons learned from IT teams regarding client requirements.

SYSTEM/PROCESS INCOMPATIBILITIES

Clients may require a control that is inconsistent with your firm's existing policies. For example, a client may want you to implement a password control that does not match that of your firm, such as a 15-day password expiration when yours is 90 days. You can establish communication channels with the appropriate teams in the firm who are in a position to best leverage negotiations. It is important to explain the parameters of the situation to the billing/relationship attorneys so they understand the importance of the control differences and the best way to approach client collaborations that will result in the best outcome for both parties. Aspects such as cost to implement, user impact, incompatibility with firm systems or multiple, varied client requirements are key factors to consider.

Keep in mind that in large organizations, the client's Legal department may not be driving the level of oversight required of outside counsel; the client's assessment program is likely driven by audit, governance, or procurement people. It is possible that in-house counsel may not be fully briefed on the controls their risk people are requiring, particularly in light of the type of work and sensitivity of data involved. Your ability to negotiate these terms may depend largely upon the internal structure of the client. Leverage your in-house relationship partner to advocate if terms seem misaligned with legal work being performed for the client.

SCOPE DIFFERENCES

Different control recommendations may have different scopes associated with them. Some controls may apply specifically to the work your firm is doing for the client and the associated systems. Other controls may be intended for the entire enterprise. When you implement controls, make sure the appropriate scope is addressed. Auditors may choose random offices, servers or workstations to look at, so ensure that scope is aligned with your audit evidence prep. You can implement a control across the enterprise even though the client only requires it to be applied to their information if it is a best practice that adds value to your firm overall.

SECURITY AUDITS AND AUDITORS

Security audits come in a variety of forms: some may only require an attestation, some consist of questionnaires to which you must supply answers, and some require an onsite audit. Onsite audits vary in intensity, as each auditor has his or her preferred method and style of auditing. You may be able to glean something about the auditor's approach during the introduction and prep interactions you have by phone as well as email leading up to the audit. Try to find out what approach the auditor will take ahead of time to help you prepare.

First impressions can set the tone for the entire audit engagement, and the more prepared, organized and in control you are, the more confident the auditor will be in your responses. Conversely, if you appear to be disorganized and unsure of the controls, they will be more likely to need to dig deeper into your processes.

One of the key objectives of your program should be to make the process as streamlined as possible for the auditor. Be prepared to answer their questions with evidence as quickly as possible, without making them wait while you fumble to present evidence.

Unfortunately, some organizations view the auditor as an adversary, viewing audit requests as unreasonable or un-actionable. Audit processes are typically far more effective and valuable for both parties if viewed as helping to ensure the firm is delivering quality, valued service to the client.

AUDIT EVIDENCE

During a security audit, you will be asked to provide evidence that controls are in place. If you can find out what they expect ahead of time, great; if not, plan to have screenshots available to demonstrate the control. The control evidence may be to view the actual written policy or technical evidence that the policy is actually implemented. Good evidence examples may be a screenshot of the password complexity policy (GPO), the message a user receives when they try to do something they shouldn't, or a configuration screen demonstrating the control.

The evidence that you gather should be fresh for the audit cycle. If the client audits you every year, they will expect that the evidence you show them is current; update screen shots as appropriate. Make sure that screen shots do not have extraneous data in them. Many auditors will want to see that policies are reviewed and approved by management annually. It is best to have a cyclical review process in place. It may take time to get policies approved, depending on review processes in your firm.

If the auditor wants to interview engineers or technicians, prepare the potential interviewees for what to expect. Advise them to answer the questions truthfully, accurately and succinctly. Answer questions at hand without adding color commentary or expanding beyond the scope of the question. If possible, have a management team member in the interview so that they can help make sure the process stays on point.

If the auditors have a list of controls with index numbers on them, label your evidence to correlate with their

control list. If you follow a framework, you may want to tag or name your documents to align them with the outline of that framework. If they ask to have evidence ahead of the actual audit, you will need to confirm if this aligns with your firm's policy - it is typically best practice not to send materials outside the firm. However, you may be able to prepare packets for their review onsite, having them clearly named and indexed so the auditor can easily review the documentation without the need to explain what evidence goes with what controls. This can potentially reduce the amount of onsite audit time.

It is best practice to have a non-disclosure agreement (NDA) in place between the client and the law firm. Often times the firm has already agreed to secure handling of client data. However, in a security audit, the client should agree to secure handling of firm data based on the nature of detail now being shared about the firm's systems and processes.

Have your own processes in place to validate controls, including those that are requested year-over-year or from client to client. There is nothing worse than proudly presenting an auditor with a control you thought was in place, only to find it is not working because it was uninstalled during the last upgrade.

AUDIT FINDINGS

At the conclusion of the audit, there should be a findings or summary report. Make sure that you document your response to the findings, what you commit to doing, and by when you plan to do it. Some clients will ask you to provide specific dates by which findings will be completed, and may even require some findings be resolved in risk-aligned timeframes. For example, the auditor may require a critical finding be remediated in 30 days, while an important finding can be done in 60 days. When making commitments to remediating findings, leave room for unexpected challenges or issues implementing the remediations in order to prevent missing deadlines.

FACILITIES SECURITY MANAGEMENT

Clients are asking increasingly sophisticated questions with regard to hard copy records management, including facilities and building security and handover procedures (such as transferring to and from third parties, releasing to other firms for matter mobility purposes, returning to the client, etc.). It can be challenging, especially for global, multi-office firms with decentralized operations to provide a satisfactory one-size-fits-all approach.

Policies and operational procedures are an integral part of any records and information management program and are of great importance when providing needed evidence in response to CIGRs. Clients are generally interested in understanding whether processes and procedures are in place to ensure that any information is handled in accordance with either their requirements or other legal or regulatory requirements. It is common to receive a request to comply with a client's specific retention schedule, that information be returned or destroyed upon request, or that some other action is taken once it is no longer needed.

Security and record keeping practices should be identified up front. Records and other supporting staff members should have a clear understanding of their role in supporting the policies and procedures. In addition, all members of the firm should be aware of their own responsibilities with regard to proper file maintenance and security; this includes understanding escalation procedures and knowing who to go to with records management questions. Ideally, there should be a named person responsible for Records and Information Management.

Evidence of training and communication of policies and procedures is also a common request. Training should occur on regular, repeated intervals, typically at least once annually.

There should be a process in place for the identification and management of records management risks and incidents. Regular monitoring to identify where risks may not be sufficiently mitigated should be a part of the compliance program. Any corrective actions should be documented and tracked to completion, including having dedicated levels of resources to mitigate records management risks effectively.

Primary areas regarding records management security are:

RETENTION (INCLUDING STORAGE AND ACCESS)

Processes and procedures should be in place to ensure that all client data, regardless of storage location, is retained and disposed of in accordance with client, legal and regulatory requirements. A Clean Desk Policy can help support retention/security requests in addition to having secure collection containers for confidential waste.

Clients commonly seek evidence that their records, including paper files, are segregated and stored separately from other clients. Oftentimes, noting that files are stored logically by client/matter number and in a secure records center or other location satisfies this request.Controls should be in place to ensure client data cannot be removed without authorization. Often, clients request that any files containing their information be placed in a physically secure environment such as a locked desk drawer, filing cabinet or other secured storage space when leaving the desk. Preparations should be made for these requests in advance.

It is becoming increasingly common for clients to request regular reviews of an inventory of files and media to ensure compliance, thus it is important to maintain an inventory of physical files and media. Ideally this is accomplished by using a Records Management System that allows for the assignment of a unique barcode identifier and maintains a detailed history of any actions taken with the files and by whom. Any reviews should be documented as evidence. Labeling is an important component of this and a process should be established to ensure that standards are followed. Clients may ask that the labeling be consistent with their own classification scheme. However, generally speaking as long as files can be uniquely segregated and secured, the law firm client/matter numbering schema has typically been acceptable.

STORAGE

A common requirement is to ensure that records are protected using physical, environmental and logical controls to prevent unauthorized loss, modification or damage throughout their retention and disposition. Physical/logical controls to grant access only to those personnel who are authorized should be in place. Common criteria asked to be captured in any index/inventory include: a) box owner, b) box number, c) description of contents; d) destruction date or from date/to date.

RETRIEVAL

Clients commonly are setting forth expectations on the timelines in which records can be retrieved. Standard procedures should already be established for support of firm operations and can be leveraged for providing evidence to clients for this request. Any processes should be tested on a regular basis.

Processes should be in place to protect records during transit via appropriate controls (physical, environmental, logical). It is important to work with any third party providers such as offsite storage vendors, to put in place established, documented chain of custody protocols that provide evidence of protection throughout each step of the movement of files.

DISPOSITION AND DESTRUCTION

Having documented procedures that provide detailed audit trails documenting the destruction of electronic and non-electronic media is imperative.

These procedures should, at a minimum, ensure that the media location and who has custody of the media can be determined at all times.

Disposal procedures should also include detail regarding the type of disposal method used (e.g. cross-cut shredding). Evidence of the authorization and destruction of records should be maintained, using controls such as a) physical certificates of destruction; b) electronic records audit trial/reports of records purged/deleted.

Before disposing of any records, you should make sure to understand whether the client has set forth any specific requests that obligate you to provide notification or obtain the client's consent. It is helpful to include record-handling protocols in your engagement letter. Conversely, clients may ask that you agree to destroy records within a certain timeframe upon their request. Standard operating procedures should already be in place for activities such as mandated destructions and can be leveraged for this purpose.

HOLDS

Controls should be in place to ensure that upon notification, records covered by a hold are promptly suspended from destruction and that confirmation can be provided to the client that requirements have been applied. Likewise, controls should also be in place to ensure upon notification from a client that a hold has been lifted, that the retention/disposition schedule has been reinstituted.

COMPLIANCE

Once all your policies and procedures are in place, you need to be able to provide evidence as to how your firm measures and monitors compliance. Records should be protected from loss, destruction, falsification and unauthorized access or release in accordance with legislative, regulatory, contractual and business requirements.

If your firm receives a subpoena or other demand for client data, do you have the ability to ensure that only information that is related to the client named in the demand and responsive to the demand is disclosed? You should prepare for this up front by having roles, responsibilities and standards in place.

Of growing importance is how personal data is handled. In particular, it needs to be appropriately identified, classified and protected in accordance with any relevant legislation. Regulations such as HIPAA, PCI and GDPR have particularly significant impact on the handling of health, credit card and EU citizen or resident personal data. Experts in this space should be engaged or consulted (internally or externally) to ensure proper compliance.

ASSET MANAGEMENT

Firm-owned property associated with terminated/departing employees or contractors should be returned. Employees should be asked to read and accept an Acceptable Use Policy before gaining access to information. A Clean Desk Policy and Clear Screen Policy should be established and enforced.

Clearly defined policies and procedures for the management of removable media, such as tapes, disks, cassettes and memory cards should be established and properly communicated with staff.

In addition, a documented policy that details how information assets may be reused, and the controls for securely wiping data before reuse or disposal (particularly from storage media such as hard drives, CDs, USB drives etc.) should be established.

PERSONNEL SECURITY

There should be a documented process for terminating or changing employment duties. The responsibilities for performing employment termination or change of employment should be clearly defined and assigned.

PHYSICAL AND ENVIRONMENTAL SECURITY

Considerations to ensure that any requests regarding physical and environmental security are met include:

1. Ability to restrict access to authorized personnel through locks, barriers or the use of an access control system and that access control can uniquely identify each person entering the area and the date and time they enter.

2. The list of persons with access to sensitive areas where client data is stored transmitted, processed is reviewed on a regular basis and/or when there are changes to personnel.

3. Standard operating procedures to ensure that any visitors to areas where client data is stored, transmitted or processed are escorted at all times and required to sign/check in when they enter the facilities.

4. Physical access control events (e.g. door forced open, door propped open, malfunctioning device) must be monitored or investigated immediately.

5. Any areas where client files are stored are protected by fire detection and suppression system.

6. If you internally develop, and/or outsource the development of source code which is used to provide services to the client, controls should be in place to protect the source code from unauthorized duplication or modification.

7. Physical and environmental security policies and procedures should be in place to protect client files.

8. Sensitive or critical information areas are segregated and appropriately controlled.

SUPPLIER RELATIONSHIPS/THIRD PARTIES

Third party suppliers should be audited on a regular basis using a risk-based approach. Evidence of these activities should be maintained. Third party vendors' disaster recovery/backup continuity plan should be regularly reviewed. You should also take appropriate steps to ensure that vendor's actions do not result in unauthorized access to client data. Oftentimes this can be mitigated by offering evidence of any industry certifications held by the vendor, such as ISO or SOC2. Vendors should contractually agree to abide by the firm's established procedures with regard to the secure storage and disposal of information assets.

OFFSITE STORAGE

You should be prepared to provide detailed information regarding your relationship with your offsite storage provider who may handle paper records as well as electronic media such as backup tapes. Provider information to prove chain of custody should include: a) location and provider name and the access controls implemented, b) physical security plan for your offsite storage facility, including fire authority certification, c) controls to

safeguard and retrieve any media received from the client during storage and evidence that controls are implemented during the transfer to and from the vendor location.

A detailed documented process for the pick-up and delivery of media should be established, including the container used for transport (e.g. lockbox with double key system, sealed-locking pouch) and chain of custody protocols (e.g. scanning/sign off of files during pick up, transport and receipt at destination). Controls in vehicles used to transport media containing client-related information should also be included.

You may be asked to provide information from the vendor that evidence:

- Drivers' training (re: leaving the vehicle, pick up procedures, etc.)
- Whether vehicles carry any markings advertising the vendor's services
- If vehicles contain alarm mechanisms
- Window/door type (e.g.. reinforced windows, mirrored glass, no windows in storage area, reinforced doors)
- Environmental controls appropriate for magnetic media (fire extinguishers, air conditioning, etc.)
- If drivers carry cell phones.
- Vehicles are electronically tracked? (e.g. GPS). If yes, is this in-house or third party supplied, and is there a maintenance contract in place?
- Do you have a documented process for emergencies or abnormal events such as:
    - Accident - How are emergency services engaged, and ensure the integrity of the media?
    - Late, lost or stolen vehicle (use of GPS?)
    - Breakdown - Are there breakdown recovery and contingency vehicles?
    - Lost records or data

Access protocols should be established up front that address whether access to the warehouse is restricted to only authorized personnel, what sort of security checks/bonding the personnel must go through, etc. You should be prepared to provide information about whether vehicles are loaded and unloaded within a controlled environment and whether all external access points (e.g. windows, fire doors, etc.) are secured.

CONCLUSION

The number of requirements found in protective orders, business associate agreements (BAA), outside counsel guidelines (OCG), client security questionnaires and similar documents are not likely to diminish anytime soon. In response, firms can better position themselves to proactively address such situations by identifying and establishing a process and team to review these IG requirements. After the review, firms can educate the case teams and staff, making them aware of what was agreed upon and how it is being implemented. They can ensure the client's requirements align with the firm's own initiatives and environment, and address any contradicting requirements. Furthermore, they can determine what policies and procedures need to be created or modified in order to fulfill what the client is requesting.

These are just the initial steps of what must be a "lifelong" process throughout the client relationship. Firms must:

- establish procedures and internal control processes to ensure that systems, policies and procedures, and personnel remain in compliance
- consider what technology is available to assist them in complying with client requirements, and whether the projected revenues from the client relationship outweigh the costs of investing in these tools.
- optimize their position by considering certifications, aggregating standard audit responses to more efficiently respond to questionnaires/onsite inspections, and ultimately leveraging their security protocols as a means to market their business.

In the past, the Law Firm Information Governance Symposium (LFIGS) produced a paper called Outside Counsel Guidelines Management: An Information Governance Issue. That paper discussed the management of the Outside Counsel Guidelines (OCGs) as an IG issue. Another paper that has been mentioned is Staying in Compliance with Client Conditions which addresses the data management and security requirements found in OCGs. It explores ways in which the law firm can gather and review CIGR's, as well as implement controls to satisfy the IG requirements with the end result of putting the law firm in a better position to manage information in accordance with agreed upon IG requirements.

USLGL-RPT-080918A