IRON MOUNTAIN®

STAYING IN COMPLIANCE WITH CLIENT CONDITIONS

2016 LAW FIRM INFORMATION GOVERNANCE SYMPOSIUM

CONTENTS

EXECUTIVE SUMMARY

For years, many clients have provided their outside counsel with guidelines that must be followed in order to obtain, or retain, their business. More recently, these guidelines include instructions on how law firms are expected to manage and protect client data - either because organizations are more conscious of security risks, or because they are being forced to do so by regulatory bodies. In some instances, they may feel the need to stringently audit service partners, including legal providers.

Unfortunately, these guidelines are often not communicated to the legal teams providing service to the client, a fact often brought to light when clients conduct an audit to confirm the protocols are in place. Moreover, implementation of such requirements can, at times, create a financial burden for the firm, conflict with the firm's established organizational culture or even conflict with requirements provided by other clients.

This report provides practical guidance for the creation of a cohesive process with which law firms can respond to, and deliver on, client requirements for the governance and management of their information. It addresses steps for gathering requirements along with their analysis, communication, implementation and maintenance, including suggestions for responsible roles.

SYMPOSIUM STEERING COMMITTEE

BRIANNE AUL, CRM
Firmwide Records
Senior Manager
Reed Smith LLP

BRIAN DONATO
CIO
Vorys, Sater, Seymour
and Pease LLP

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

RUDY MOLIERE
Director of Information
Governance
Morgan, Lewis & Bockius LLP

CHARLENE WACENSKE
Senior Manager Records and
Information Governance
Morrison & Foerster LLP

STAYING IN COMPLIANCE WITH CLIENT CONDITIONS TASK FORCE

BRIANNE AUL, CRM
Firmwide Records
Senior Manager
Reed Smith LLP

MAUREEN BABCOCK
IT Business Operations Manager
Snell & Wilmer LLP

BRIAN DONATO
CIO
Vorys, Sater, Seymour
& Pease LLP

BETH FAIRCLOTH*
Director of Risk Management
Seyfarth Shaw LLP

JAMES FLYNN, CRM
Director of Records & Docket
Winston & Strawn LLP

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

NORMA J. KNUDSON
Director of Compliance Support
& Space Planning
Faegre Baker Daniels LLP

ROBERT WEAVER
Director of Information Security
Blank Rome LLP

****Task Force Leader***

IRON MOUNTAIN WOULD LIKE TO THANK THE FOLLOWING INDIVIDUALS FOR PARTICIPATING IN THE PEER REVIEW SESSIONS OF THE 2016 SYMPOSIUM EVENT AND FOR SHARING THEIR PERSPECTIVES AND EXPERTISE DURING THE CREATION OF THIS TASK FORCE REPORT.

ANGELA AKPAPUNAM, IGP
Director, Information Governance and Records
WilmerHale

KAREN ALLEN
Manager, IG Technology
Morgan, Lewis & Bockius LLP

DERICK ARTHUR
Firmwide IG Operations Manager
Cooley LLP

BRIANNE AUL
Firmwide Records Senior Manager
Reed Smith LLP

MAUREEN BABCOCK
IT Business Operations Manager
Snell & Wilmer LLP

BRYN BOWEN
Director of Information Services
Schulte Roth & Zabel LLP

SCOTT CHRISTENSEN
Senior Associate
Olenick & Associates

TERRENCE COAN
Senior Director
HBR Consulting

GALINA DATSKOVSKY
CEO
Vaporstream, Inc.

BRIAN DONATO
CIO
Vorys, Sater Seymour and Pease LLP

BETH FAIRCLOTH
Director of Risk Management
Seyfarth Shaw LLP

STACEY FIORILLO
Managing Director
Information Governance Consulting Group

PATRICIA FITZPATRICK
Director of Information Governance & Compliance
Katten Muchin Rosenman LLP

LEIGH ISAACS
Director of Records and Information Governance
White & Case LLP

NORMA KNUDSON
Director of Compliance Support & Space Planning
Faegre Baker Daniels LLP

SAMANTHA LOFTON
Chief Risk and Information Governance Officer
Ice Miller LLP

FARON LYONS
Director of Enterprise Sales
Zia Consulting

LISA MARKEY
Director, Information Security
Shearman and Sterling LLP

RUDY MOLIERE
Director of Information Governance
Morgan, Lewis & Bockius LLP

RANDY OPPENBORN
Director, Information Governance
Foley Lardner LLP

ALEXANDRA PROPHETE
KM Operations Manager
Cleary Gottlieb Steen & Hamilton LLP

DEBORAH ROBBINS
Records and Conflicts Coordinator
Jones Walker, LLP

SUNNY SANGHANI
Associate Director
Robert Half Legal, eDiscovery, Managed Review and Consulting Services

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

SUE TROMBLEY
Managing Director, Thought Leadership
Iron Mountain

CHARLENE WACENSKE
Senior Manager Records and Information Governance
Morrison & Foerster LLP

ROBERT WEAVER
Director of Information Security
Blank Rome LLP

JOHAN WIDJAJA
Assistant Director Records and Information
Morgan, Lewis & Bockius LLP

JOEL WUESTHOFF
Senior Director
Robert Half Legal Consulting

INTRODUCTION

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 information governance (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, of course, 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. Firms must 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. Eventually, firms may want to 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.

Two years ago, the Law Firm Information Governance (LFIG) Symposium 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. This paper addresses the data management and security requirements found in those OCGs, in addition to other engagement contracts, governmental regulations and court orders. It explores ways in which the law firm can gather and review requirements, 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.

I. GATHERING CLIENT INFORMATION GOVERNANCE REQUIREMENTS

WHERE TO FIND CLIENT INFORMATION GOVERNANCE REQUIREMENTS (CIGR)?

A CIGR is any IG requirement the firm must meet to manage client data. There are several possible sources that might contain CIGRs. Examples include:

- OCGs are a very common source for these types of requirements, typically found under section headings such as confidential information, information security, or records retention.
- Some clients require firms to sign an engagement letter that contains confidentiality and other data security and management terms.
- Healthcare providers who are covered entities under HIPAA may require the firm to sign a business associate agreement (BAA).
- Many clients ask firms to agree to a non-disclosure agreement (NDA), and sometimes, these agreements extend to data of a third party involved in a case.
- Litigation matters may have protective orders that contain stringent court orders which have IG implications for the firm and the client.
- In some industries clients send "security" questionnaires that contain a wide variety of CIGRs. Even request for proposals (RFPs) from prospective clients may contain binding requirements if the firm is successful in obtaining the business.

For purposes of this paper, CIGR is used as an overarching term to reference all of these sources that may contain IG requirements.

RESPONSIBILITY FOR REQUESTS - WHO ASSISTS WITH THE PROCESS?

There should be a well-defined entry point and distribution process within the firm to ensure consistency and accuracy when responding to CIGRs. While there are many methods that can accomplish this goal, most are categorized as either a decentralized or centralized approach. As explained more fully below, this task force recommends a centralized process whenever possible. Regardless, as many CIGRs contain requirements that impact many functional areas within the firm, representatives from these areas described below must be accounted for in the distribution process.

Information Technology: Enterprise architects, database administrators and others with comprehensive knowledge of the firm's data map can be very useful in assembling accurate responses.

Information Security: Information security professionals with knowledge of the firm's overall security policy, practices for meeting the specific security controls referenced in the requirements and the necessary protocols for granting exceptions to the policy.

Legal/Risk: General Counsel, risk director or manager, or equivalent may be the authority to weigh in on conflicts provisions and other requirements often found in CIGRs.

Facility Security: Facility management or physical security managers can provide information regarding physical access controls and surveillance of sensitive facility assets (file rooms, server rooms) and general facility perimeters.

Records Management/IG: Records Management and/or IG director or manager can be the authority to review client retention schedules to determine alignment with the firm's own schedule. They can also assist in identifying data ownership, workflows and security.

Human Resources: Director, manager or other HR professional can respond

to client requirements about demographics and diversity of legal teams as well as hiring procedures such as background checks and training.

Accounting/Finance: Pricing specialists and/or billers familiar with firm billing guidelines which are often addressed in CIGRs.

Marketing/Business Development: Marketing managers and others responsible for preparation of materials for client RFPs are logical recipients of client requirements as part of new business pitches.

Practice Group Management: Practice group support specialists assisting with the implementation of protocols related to the representation processes that support IG, such as methods of ingesting, storing and sharing client data, redaction of draft documents and sharing client feedback with the appropriate team members.

Procurement / Contract Reviewers: Some firms have designated contract reviewers to review all firm contracts before final approval and execution. These procurement / contract reviewers may be able to identify additional IG requirements from eDiscovery or other third party vendors.

In addition to the identification of members of the response team, firms should also consider, and incorporate, departments and roles which are natural collection points for intake of client requirements. These areas can also act as a backstop by flagging documents that may have bypassed the standard approval process. For example, marketing is often the first area to receive requirements as part of the sales process for new business to a potential client. Information technology may receive security audits directly from a client rather than through an attorney. Similarly, accounting may receive requirements from the client directly in response to an invoice, or just as the point of contact for billing matters. These collection points, typically in a responder role, should also serve to initiate the process under such circumstances.

DECENTRALIZED RESPONSIBILITY

In a decentralized approach, CIGRs are sent directly from the point of intake to those with the knowledge to respond to the requirements. A decentralized approach places more responsibility on the attorney or other original points of intake to not only track down and collect responses, but also to ensure the agreed upon process is followed. As such, all possible entry points must be educated as to the necessary steps to ensure a complete and accurate response. Appendix A includes an example checklist to assist attorneys and others in meeting all process requirements. Each attorney, as a potential point of intake, needs to know who else should review the CIGRs.

Because this approach is less likely to efficiently produce consistent results, a decentralized approach is generally less desirable. However, depending on the size of firm and/or the number of CIGRs received, a decentralized approach using one of the following models, buttressed by a strong education component, may be sufficient:

- Individual Respondents
  The firm designates individuals with knowledge of the firm's capabilities in areas typically covered by CIGRs. The individuals analyze their portion of the CIGRs and respond to the point of intake. This might be appropriate for a smaller firm where individuals wear multiple hats in terms of areas of responsibility.

- Designated Departments
  This model is similar to the above, except that departments, rather than individuals, are assigned responsibility for different subjects covered by CIGRs. Depending on the size of the department and skillset of its members, this approach may provide greater flexibility and result in faster response times. It also provides other benefits, such as the ability to work around employee absences and the opportunity to collaborate on difficult questions. It does necessitate a commitment of more than one resource to engage in the process.

CENTRALIZED RESPONSIBILITY

A centralized approach attempts to reduce the effort required by the point of intake to respond to CIGRs, while ensuring an efficient, timely and accurate response. This approach provides the point(s) of intake with a single contact who is responsible for CIGR distribution and follow up. As the point of intake is often the matter-responsible or client attorney, the centralized approach can reduce the amount of otherwise billable time an attorney may expend tracking the progress of CIGR responses across multiple individuals or departments. A centralized process also helps facilitate collective analysis of CIGRs to identify opportunities for standardized responses, potentially leading to faster and more efficient processing.

The centralized process is accomplished in several ways:

- Individual Custodian
  The firm identifies one individual to receive CIGRs from the point of intake and to work with other individuals and/or departments to obtain the requested information. All follow-ups, whether from the original point of intake or the department members providing responses, are channeled through the individual custodian. The custodian can maintain a central repository of CIGRs received by the firm.

- Task Force or Committee
  This can be 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 either case, the collective is a single point of contact, typically through an email distribution list or automated workflow solution.

Section II of this paper details possible approaches for building a repository of CIGRs and responses.

Establishing a centralized process has a number of advantages, providing a firm receives a sufficient number of CIGRs to warrant the investment. It provides a single contact for the point of intake and consolidates responsibility for collecting responses which should lead to faster and more consistent answers. It also provides a capture point from which to create a central repository of CIGRs and responses, which can lead to further efficiencies when answering audits or monitoring compliance.

CASTING A WIDE NET

No process is perfect; each firm will differ in how compliant the attorney population is with a given process. Therefore, it is wise to take efforts to cast a wide net beyond the established intake process. For example, senior management issuance of regular reminders about the necessity that CIGRs are vetted fully using the firm's process, including examples of CIGRs, can help prevent lapses. Additional coordination with other firm processes related to CIGRs may become visible as the practice continues. For example, the new business intake process may surface various types of CIGR's that are included as part of the onboarding of a new client. The billing department almost certainly receives outside counsel guidelines to ensure that bills are sent to client specifications, occasionally outside of the formal process. Finally, searching the document management or records system for key terms may yield CIGRs not previously submitted via your process.

THE END RESULT

Once a process is decided on and implemented in a firm, all participants must be educated on the process specifics, including how to identify source documents containing CIGRs that fall through the cracks. The end result will be a number of source documents with a variety of client requirements that need to be addressed. Effectively parsing documents for such requirements is critical in determining an efficient, consistent response to each CIGR.

II. SYNTHESIZING AND MAINTAINING REQUIREMENTS

Once a firm's efforts at gathering documents that contain CIGRs are successful, the next potentially daunting challenge is to determine what exactly each document is requesting of the firm. This section discusses a general approach, with specific suggestions, on how to identify, classify and track CIGRs included in these documents, with the goal of turning them into clear, actionable instructions for people and machines. Because many CIGRs contain variations of the same requirements, a good starting point is to define an efficient review checklist that provides a concise summary of the IG provision requirements in a given CIGR. This section also describes techniques and options for tracking this information and the steps to consider before determining what action, if any, is required.

IDENTIFY THE IG PROVISION CHECKLIST

CIGRs can be as varied as the requestor – in content, format and even the preferred method of response. To ensure a firm is utilizing its resources efficiently (human or otherwise), they need to create internal standards for determining requirements to analyze the content before replying. Each source document identified contains one or more IG requirements. Firms should set up an efficient review process that allows the reader of the document to identify, classify and record the IG requirements in the CIGR. If the resources and skills are available, an eDiscovery review tool could be used to sort through the data collected provided the historical volume is significant at the start of the project.

The firm should decide in advance which data elements to use to track each type of requirement. As a starting point, a firm should gather a selection of each type of CIGR source document (e.g. outside counsel guidelines, security audits, protective orders, business associate agreements, etc.) and examine each for IG requirement themes. The likelihood is that several consistent themes are represented in these sample documents. Using this information, along with experience, a firm can create an initial chart of IG requirement categories.

For example, a very common CIGR is the need to deny data access to any firm member that is not part of the client matter team. Another common example is a requirement to honor the client's records retention policies. As the firm creates the chart, they should look for themes rather than specifics. For example, clients will have varying records retention periods, but they all share the same theme: honoring the clients records retention schedule policy. Appendix B contains a list of sample IG categories, with brief descriptions.

Once a firm completes the initial subset review and creates a chart of IG requirement categories, the next steps are to 1) create a collection method to record the document review and 2) establish a tracking mechanism to report the requirements by client, matter or IG requirement type. Depending on an individual firm, taking into account its size, culture and other factors, there are a variety of methods to accomplish collection and tracking. They include:

- Utilization of an existing contract management solution that fulfills both requirements.
- The development of an application whereby the collection method may consist of a form or input screen, while the tracking mechanism is a database with appropriate queries and reports.
- Employment of SharePoint options: from a basic list to a database, supplemented by time-saving workflows.
- A spreadsheet with predefined columns to record the information the firm wants to track may be a suitable option.
- A custom SQL database or other database options they may already own or license.

- A sophisticated agreement management system.
- Modification of the use of common software, such as document management systems or other third party solutions.

What information should a firm track in order to make the reviewed information useful for future reporting purposes? Some of the items are obvious, such as client number, matter number, name of document reviewer, something to identify the document being reviewed and the date of the review. Additionally, it is necessary to track which of the IG requirement types occur in the reviewed document and the specifics of the IG type (for example, the retention schedule provided by the client.) A more complete list of potential items to track can be found in Appendix C.

HOW IS THE REPOSITORY SECURED?

While some of the information gathered may be "public" knowledge within the firm and therefore less stringently governed, firms should create a comprehensive summary of their most sensitive data responses. Access to the repository should be secured to the team or individual responsible for parsing the documents, as well as to the attorneys responsible for a given client or other authorized outside party requestor. Access for additional individuals should be carefully evaluated on a case-by-case basis.

IMPLEMENTING THE REVIEW PROCESS

Once the firm's tracking system has been implemented and tested, the review process can be initiated. Often, the first obstacle to implementation is determining who is available (and qualified) to review the various CIGRs, and the capture of necessary information. This task may fit nicely with the firm's IG team or in other areas of the risk management function. For many firms, it may be less a matter of where to put the function than it is to find the appropriate person with the capability and available capacity to perform the work. An important aspect of the review process is to ensure that the final executed documents are received by those tasked with gathering the information. Without knowing the agreed upon terms it is impossible for the IG team and other firm administrative functions to execute the needed controls for implementation of the CIGRs.

REPORTING AND DISSEMINATING THE IG PROVISIONS

The end result of the review checklist list is the ability to report by client or client matter the specific IG requirements to which the firm agreed. This report serves as the basis for determining what information must be disseminated to various departments, systems and ultimately, to the attorneys working on the matter. In order to ensure compliance, many client-specific IG requirements stipulate that the people working on the matter know about the requirements and the controls put in place to fulfill the requirement. For example, if a client restricts access to its information exclusively to people working on the matter, then the approved people must know how to add new members to the group. This may be as simple as adding them to a group in a document management system or calling a help desk to have them added to an established security group.

Additionally, the tracking system must help identify the frequency of any specific IG requirement mentioned in the various CIGRs. This information is of value in forecasting the firm's future IG needs and to continually improve IG processes which might include revised procedures and enhanced tools.

Finally, because CIGR documents change from time to time, the tracking system should generate an aging report to ensure that the firm revisits the IG requirements for clients at least annually.

With a fully operational review process, a firm should be able to track requirements by client, by requirement type and even by date, which provides the raw material to ensure that appropriate controls and education are put into place based on that information.

III. ANALYSIS, IMPLEMENTATION AND COMMUNICATION

Firms should develop a process to take the appropriate action for each type of CIGR in a given source document. Note that different source documents may require different types of responses. For example, outside counsel guidelines (OSG) may require only that the firm document the controls currently in place, while a client questionnaire may require the firm provide specific details about how a requirement is met. In almost all cases, the firm will want to provide education to the attorneys and support staff involved in a case to ensure that they take advantage of appropriate controls or follow client specific procedures.

As a firm prepares to respond to each set of CIGRs, the requirements will fall into one of several categories:

- CIGRs that the firm already satisfies via policy or available technical control
- CIGRs that the firm can satisfy by implementing new procedures
- CIGRs that the firm can satisfy by implementing new technology controls
- CIGRs that the firm can satisfy by changing policy
- CIGRs that the firm cannot satisfy as requested.

For the first category of common requirements that are satisfied by existing policy or technology, documenting compliance and providing education for the legal team is critical. When the firm must implement new policy, procedures and/or technology controls, a more formal project management approach may be necessary to appropriately handle the given CIGR.

CONSIDERATIONS FOR RESPONDING TO COMMON REQUIREMENTS

Answers to commonly requested CIGRs should be documented in the firm's tracking database. These answers serve as a starting point when evaluating a new set of CIGRs and should typically cover CIGRs already satisfied via a policy or available technical control. When looking at these answers, firm policy or process-based answers are less likely to change significantly between responses. Answers on data security (especially its technical aspects) are best reviewed for accuracy

by the internal subject matter expert. Regardless, unless the custodian or task force is sure that the information forming the response is still accurate, they should seek confirmation from the responsible personnel.

Analysis should be conducted to ensure that what is being requested does not conflict with other client CIGRs. Additionally, a firm may have certifications that apply or can take place of an assessment, such as ISO 27001 certification for security or HITRUST certification. ISO certification is the subject of another LFIG paper ISO 27001 in Law Firms which provides additional education regarding the benefits of certification as it relates to the process of responding to CIGRs.

Firms generally do not sign an NDA between themselves and their clients. This can be a security concern in instances where responses may provide specifics regarding firm policies or procedures that contain confidential information about the organization. This becomes even more of an issue when the client has retained a third party data security auditor to gather information on their behalf. The client may have signed an NDA with that third party; however, it is unlikely the agreement would protect the confidentiality of firm-held information. Therefore, prior to providing responses to any questionnaire, it is best to request an NDA with the client, the third party auditor, or both.

It is critical that a firm understand what it is being asked to answer. It should resist giving away details that may not need to be provided, even though it may feel compelled to do so. The person responding to the CIGR has an ongoing responsibility to maintain the security of the firm's and all of its clients' information. It is often better to craft initial answers in a summary format rather than a detailed descriptive format. If the requestor wants additional explanations or documentation, they will ask for it.

PLANNING AND EXECUTION USING A PROJECT MANAGEMENT APPROACH

For wide-ranging and challenging requirements which may necessitate significant activity for compliance, firms should consider using a project management approach. Once requirements and necessary steps for compliance are understood and agreed upon internally, move into scoping, planning and execution. It is necessary to pull together the appropriate teams to develop a solution and, more importantly, set expectations and a timeline. Based upon the type of control (technical, policy, etc.), the responsible managers should determine what needs to be done and prioritize the effort with the necessary resources. Once a scope and process has been defined, develop a project plan to help keep the team informed and on task. This also facilitates the documentation phase.

New requirements involve different levels of effort and participation to implement controls for compliance. In some situations an existing control may be easily modified to satisfy the new requirement, requiring the involvement of only a few people for full implementation. Most often though, implementing or modifying controls, or even capturing compliance documentation, involves multiple people and several steps, similar to implementing a system security control that impacts all technology components, or getting a firm-wide policy approved.

At times, a client asks the firm to provide a resolution date, even though they have provided expectations based upon the risk rating of the requirement, i.e., that a "high risk" rating must be remediated within 90 days of reporting. If the firm's planning efforts determine that the requirement can be completed in a shorter timeframe, they may find it beneficial to maintain the remaining "cushion," should there be unexpected issues.

In the case of a client assessment, ideally a firm is provided with the CIGRs (such as an appendix to outside counsel guidelines or other agreement) ahead of any assessment process. A firm should capitalize on that situation utilizing the advance notice to comply with the CIGRs before an assessment is scheduled. CIGRs provided ahead of time may not define explicit settings or compliance reporting, but will at a minimum provide an idea of the types of controls expected.

Even if the firm does not fully have the requirements in place at the beginning of a project, it will likely be easier for them to make small adjustments by the client due dates.

If the team determines that the firm is not able to meet the date required by the client, it is best to inform the client responsible attorney of the issue as soon as possible. The team should prepare a reasonable explanation of why the implementation will take longer along with a projected completion date. The explanation should include a description of any compensating controls already in place that provide at least partial mitigation of the risk at issue. The client responsible attorney should have a candid conversation with the client immediately explaining the situation and the compensating controls.

Certain types of controls may require showing compliance over a period of time. This requires implementation of the control well ahead of the due date, providing the opportunity to capture multiple cycles of evidence prior to the required completion date. This is rarely an expectation if the client knows the firm is implementing a control for the first time. However, if the control requires periodic reporting or monitoring, the firm is expected to demonstrate such reporting or monitoring during subsequent years of assessment.

In order to measure the continual success of a new control, the firm should consider including monitoring capabilities upon implementation. Future changes to the firm's infrastructure may disable part of a control, change settings or "break" the reporting mechanism. There are tools available to produce an automated reporting of settings or deliver logs on a regular basis. If a control results in a periodic report (such as an email that shows accounts that were disabled) a firm should design the reporting such that someone always gets the email, even if there were no disabled accounts, just to ensure it is working as expected.

While the technical solution is being put in place, the firm should implement procedures to capture and retain the related documentation used to implement any new control. The records/IG team should be consulted as to where to store this information and to apply the appropriate retention rule from the firm's records retention schedule. Upon achieving successful compliance, the newly developed responses must be centrally tracked to reduce administrative overhead when asked to reply to similar requests in the future.

In the client assessment process, the client defines when the assessment process has been satisfied. At the conclusion of the process, the firm should be able to close out any issues or "findings." The closure process is much easier if the client clearly defines the requirements for closure. Some clients are very specific and forthcoming; others are not. If a client is not able to clearly define what they are looking for, the firm needs to rely upon its good judgment and experience with other clients in responding to the assessment questions. In any case, the firm must identify the target outcome, hopefully as defined by the client, in order to shape the implementation.

CONSIDERATION OF CONFLICTS WITH EXISTING POLICIES

While many of the CIGRs align with current firm policies and procedures, there may be times when CIGRs deviate from the firm's current policy or the IG provision identifies a lack of appropriate firm policy to address a requirement. In these situations, a firm should establish a standard review process to address deviations. Depending upon the organizational structure and the subject of the deviation, this may include involving the general counsel, other members of firm management or working with the client relationship attorney to review and resolve the situation.

As an example, if the client is asking the firm to adhere to their records retention schedule, and that schedule is shorter or longer than the firm's retention schedule for specific information, there must first be a determination as to whether the firm can accept this provision. If the decision is to accept the provision, then the appropriate departments need

to be notified and a modification made for this client upon the triggering event for disposition. However, if the firm does not accept the shorter (or longer) provision, then firm management or the client relationship attorney needs to negotiate the modification with the client, and make sure it is documented.

As these situations arise, the firm may establish standard responses to certain requests which allow staff to work with the client relationship attorney in the initial negotiation phase. However, if the client will not change the provision, then an escalation process is needed to make sure the correct people are involved with the acceptance of non-standard provisions.

In some cases, a firm will need to make an exception to their policy. As such, they may want to negotiate with the client to see if the client can accept the firm's policy. However, if the firm receives enough requests for deviations, it may be time for the firm to re-examine, and possibly adjust, its policy currently in place.

EDUCATION

Providing education is critical to the overall success of any compliance effort, both from the client perspective and internally. When a specific CIGR requires the legal team to utilize an existing control or implement a specific procedure when handling client data, it is the primary responsibility of the IG team to coordinate with the client responsible attorney to educate the current case team, as well as subsequent members.

While some educational requirements may be specifically called out in CIGRs (such as mandatory security awareness training) in general, any control that requires a particular behavior or action from personnel should be included in a more formal training program. This includes not just IT staff but any individual who may be involved in an administrative or matter-related CIGR process.

When feasible, a firm should integrate the CIGR-compliance process into previously established educational programs or methods. This makes the process smoother and appears less of a new burden. Education related to controls that are specific to one particular client, or one particular practice group, may be provided differently than a firm wide education requirement. In many firms client responsible attorneys are already expected to ensure those working with the client are aware of the client specific requirements. In those cases, any new requirements can be inserted into the current method of monitoring compliance.

There are a variety of approaches required to analyze, implement and communicate compliance with CIGRs. As most firms can attest, compliance is a journey, not a destination. With each iteration, the client expects a firm to improve both processes and controls.

IV. PRACTICAL GUIDANCE

Exactly how a firm elects to establish teams or individuals to review and record CIGRs and how a firm maintains compliance during the client relationship, varies based on firm structure, culture and risk tolerance.

The following is a summary of practical guidance offered throughout this report:

1. Establish a uniform process through which all CIGRs are filtered. Ensure the points of intake are aware that they are not to agree to guidelines and/or respond to questionnaires without first completing the firm's established process.

2. Identify the appropriate teams or individuals within the firm that need to be made aware of, and agree to (or raise concerns about) the proposed CIGRs.

3. Identify a designated, secure repository in which to store CIGRs such that they are accessible to those that need to review and comply with them.

4. Establish a standard process and secure repository in which responses to client questionnaires, and supplemental documentation, is maintained.

5. Review a sampling of the CIGRs to identify consistent patterns amongst them in terms of requirements, and review current firm policies to identify whether they should be revised or modified to comply with recurring client requirements.

6. Identify specific requirements in the CIGRs that are exceptions to the firm's standard policy; communicate those exceptions to the necessary teams and follow up periodically for review.

7. Leverage certifications that the firm may have in place that address underlying concerns in the CIGRs or subsequent questionnaires, audits, etc.

8. Utilize the firm's existing educational programs and applications to instruct teams on specific client requirements, or on firm policies that the client has indicated must be reinforced on a recurring basis (e.g., information security policies).

9. In the event of an onsite audit, or in responding to a questionnaire, ensure that the necessary teams or individuals are "audit-ready." This includes proper demeanor, discretion in sharing policies or procedures, and identifying the necessary documents and answers that will give the auditor what he/she needs without excessive sharing.

10. Establish a process to address "findings" or areas of remediation. Ensure that the impacted teams are aware of the deadline provided to correct the concern.

CONCLUSION

Most CIGRs are the result of pressure being applied on the client by external forces and security concerns. It is important that law firms understand these pressures, and understand that meeting a client's IG requirements is an integral part of serving the client's needs. Additionally, as CIGRs become more commonplace in firms of all sizes and backgrounds, a well-defined approach to effectively address and maintain them will become more critical to establish. Taking proactive measures such as those in this report will better position firms to handle this challenge, and ultimately, help strengthen the overall relationship with the client. More so, firms should capitalize upon this opportunity to identify those security requirements most commonly required by their client base as a means to determine investment in certifications, technology and processes.

As with many IG processes, education and communication is critical in addressing CIGRs throughout the course of the client relationship. This awareness ensures that the appropriate teams in the firm are notified and agree to the requirements put forth, and that they have the opportunity to question, or possibly negotiate, the ones that do not "fit" their current culture and environment. It also ensures that during subsequent audits, firms can more confidently confirm that the necessary controls are in place and being followed. Lastly, and perhaps most importantly, it reflects the importance of a robust and well-organized IG program within the legal industry as a means for continued success.

APPENDIX A: SAMPLE CHECKLIST FOR INDIVIDUAL CUSTODIAN

CLIENT INFORMATION GOVERNANCE REQUIREMENTS PROTOCOL CHECKLIST

This checklist is designed to ensure that client information governance (IG) requirements are reviewed and addressed by those in the firm with the knowledge necessary to provide accurate responses. It should be completed each time the firm receives requests from clients.

Upon receipt of any document from a client that includes IG related requirements, take the following steps.

1. Circulate the document to the individuals/ departments listed below. Provide the recipients with a response by date and any other relevant information in addition to the document.

SAMPLE

_____ Accounting
_____ Information Technology
_____ Information Security
_____ Legal/Risk
_____ Human Resources
_____ Marketing/Business Development

2. Collect and document responses from each recipient.

DEPARTMENT	RESPONSE DATE	NO ISSUES	ISSUES TO BE ADDRESSED
ACCOUNTING			
IT			
INFORMATION SECURITY			
LEGAL/RISK			
HUMAN RESOURCES			
MARKETING			

3. Respond to client.

DATE COMPLETED: _____

APPENDIX B: CATEGORIES OF IG CONDITIONS TO TRACK

CLASS	TYPE NAME	TYPE DESCRIPTION
Access	Restricted Access	Only users who reasonably need access to sensitive Information should have access.
Access	Secure Configuration	Computer being used to access and manipulate sensitive information should have a secure configuration including malware protection, inactivity logging and similar controls.
Access	No Mobile Access	Sensitive information cannot be accessed by mobile devices
Access	Named Users Only	Only users named in an agreement can access sensitive information. Can include classes of users.
Access	Termination of Employee	If an employee who had access to sensitive information leaves the firm, the firm should notify the client.
Access	Deny Access	Certain users should not be allowed access to sensitive information, typically associated with a potentially adverse party or ethical wall.
Access	Home Access	Firm agrees not to store information on unauthorized computers or systems.
Audit	Audit of Firm's Books	Client reserves the right to audit books and records.
Audit	Audit of Firm's Security Practice	Client reserves the right to conduct on premise information security audit.
Availability	Disaster Recovery/Business Resumption	Firm is required to maintain and test DR/BC plans.
Availability	System fault tolerance	Firm is required to maintain backups adequate to resume business and sufficiently secured.
Awareness	Security Awareness Training	Firm agreed to ensure all users with access to sensitive information are provided security awareness training.
Destruction	Certificate of destruction	Party owning sensitive information required written certification of destruction.
Encryption	No unsecured email	Sensitive information cannot be sent unencrypted over email.
Encryption	External Media	Firm agrees sensitive information is encrypted if placed on external media.
Encryption	Data Transfer	Firm agrees that sensitive information is encrypted if electronically transferred to a third party.
Facilities	Physical Security	Firm agrees that facilities use appropriate measures to prohibit unauthorized entry.
HIPAA	Security Rule Safeguards	Firm agrees to implement safeguards described in the HIPAA Security Rule.

CLASS	TYPE NAME	TYPE DESCRIPTION
HIPAA	Breach Notification	Firm agrees to investigate any security incident and determine if a potential breach occurred, using HIPAA appropriate techniques and notify client as agreed.
HIPAA	Data Identification	Firm agrees to mark any PHI as such.
Human Resources	Background Checks	HR maintains appropriate procedures for vetting prospective and new hires.
Incident Response	Breach Notification	Notify owner or other party if there is suspected or unauthorized access to sensitive information.
Organizational	Security Organization	Firm must have a person accountable for information security and provide title and position description of personnel involved in securing client data including identification of a contact within the firm responsible for information or physical security.
Paper	Storage	Firm agrees that sensitive information on paper is stored securely when not in use.
Paper	Destruction method	Firm agrees that copies of sensitive Information are shredded.
Paper	Handling	Firm agrees that paper is stored securely during transfer outside of firm's facilities
Paper	Faxing	Firm agrees not to fax to transmit sensitive information.
Retention/ Destruction	Destruction on Termination	Firm agrees to return or destroy sensitive information within a given timeframe after the termination of matter. No provision for maintaining data until regular deletion.
Retention/ Destruction	Destruction or Maintenance on Termination	Firm agrees to return or destroy sensitive information within a given timeframe after the termination of matter or to maintain it securely until it can be deleted through normal course (typically for back up tapes).
Retention/ Destruction	Client Retention Guidelines	Client requires a certain retention period, or that the firm honor their retention guidelines
System Access	Extranet Access	Firm is required to disable account access to extranets if third party, vendor or client user is terminated or is inactive for a certain period.
System Access	Third Party Systems	Firm is required to ensure third party accounts are disabled for any firm member who leaves the firm if third party account provides access to client information.
Third Party	Vendor Access	Sensitive information should not be disclosed to third parties without written agreements in place to protect confidentiality.
Third Party	Vendor Access- Explicit notice	A party's sensitive information should not be disclosed to third parties without that party agreeing to disclosure.
Third Party	Minimum Necessary Disclosure	Firm agrees to disclose only the minimum necessary information for the intended purpose.
Third Party	Audit and Logging	Firm agrees to log use and/or disclosure of sensitive information.

APPENDIX C: INFORMATION TO TRACK FOR IG CONDITION REPORTING

NAME	DESCRIPTION
IG Type	Short name for type of IG requirement
IG Type Description	Full description of IG requirement
Data covered	Description of type of data covered for IG requirement
Source Document	Document number and name of source document reviewed to enter IG requirement
Date of document	Date of document reviewed to enter IG requirement
Last reviewed	Date IG requirement was last reviewed. Will initially = date the IG requirement was created
Last modified	Date IG requirement was last modified. Will initially equal date the IG requirement was created
IG Class	The family of IG requirement
Time period (days)	The number of days the firm has to take a given action described by an IG requirement once the trigger is received
Trigger	Event that triggers the IG requirement. Examples include termination of matter, written notification, start of matter, receipt of sensitive information
Notes of Specifics	Details not described elsewhere on type of documents, specific retention guidelines, types of security or other information necessary to comply with requirement.
Client Number Impacted	The client number of client impacted
All matters for client	Y/N - Yes if all matters
Client Name impacted	The client name of client impacted
Matter Name impacted	The name of the matter impacted
Matter Number Impacted	The number of the matter impacted
Who should receive notice	What parties should receive notice - probably a link to a separate table
Date of last notice	When was notice last sent to all parties
Notice Reminder frequency	How often should notice be sent
Systems	Systems impacted by IG requirement. Can this default based on the IG requirement or Data Type?

APPENDIX D: TYPES OF CLIENT ASSESSMENTS

Once a client communicates their need for an assessment, it is important to have a process in place to receive, analyze and respond in an organized and timely manner. Assessments, while often similar in content, vary widely in requirements. Whether the firm has a single individual or multiple parties required to review, provide information or approve the responses, it can be helpful to treat the assessment as a project and employ standard project management principles, such as assigning an overall project manager to help initiate and define the effort, plan the tasks and timeline, monitor and control the process to ensure things are completed accurately and timely, and to close the assessment and document the data, responses, findings and outcomes appropriately. The process should be communicated to the relevant parties listed earlier in this report to ensure requests are routed through the correct intake channel.

Generally, assessments are either conducted remotely or on-site, or some combination of the two.

- **Remote Assessment**
  Submitting Evidence Electronically

While this may be the "least pressure" scenario, a firm should be prepared that there may be some "back and forth" with the client if their submission does not meet the client's expectations. A firm may elect to send PDF versions of internal documents, making sure they are scrubbed of all revision marks and comments. If there is a form from the client that was completed, a firm should also make sure there are no internal comments or notes on the version that is submitted. If the firm has developed a repository of compliance information, they should make sure that dates on the documents they send are current, or that dates captured in screen shots are not outdated – some assessors may pick up on this, and request up-to-date evidence.

If there is an online portal questionnaire to complete, it is best for the firm not to wait until the response is due to answer all the questions; some portals can provide additional questions depending on their response or require additional information.

- **On-Site Assessment**
  Assessor or Assessment Team On-Site

The first hurdle in preparing for an assessment team coming on-site is to ensure the firm has the right approach for the event. The assessor is trying to find out information; there should be no reason for the assessment to be confrontational from either side. If the assessor feels that the firm is being difficult about sharing information, they may think the firm is hiding something and dig harder than they were planning to dig. A cordial and helpful demeanor with the assessor helps make the process smooth for everyone.

Preparing the team ahead of the visit can help keep everyone in this frame of mind. A training session should be held with anyone who may be called upon to speak with the assessors, and should review how the firm wants to handle the assessment. Whether the firm has a central point of contact handling the assessment, or a management team involved, some good reminders for the team members include:

- Not speaking with the assessors without having the point of contact or a management team member present.
- Ensuring all know that this is collaboration with the assessor to get the firm a clean assessment; no one should be combative or difficult.
- Cleaning up a system or office to prevent an accidental disclosure, including cleaning up paper, disks, storage devices, etc.

- Answering questions from the assessor honestly and completely, but not offering any additional information.

- Tell the assessor in the event that an answer may not be known that one is not sure of the answer, but he/she will find out and revert.

Some assessment teams may want to simply see the documentation that the firm has assembled. Some may want to interview team members. Some may want to be shown how a control actually works. While others may want to see a variety of these types of evidence, depending on the type of control. Ideally, the firm can find out ahead of time how the assessment will be conducted, but if not, they will have to be prepared for any of these requests.

If the assessor wants to view documentation, the process will go efficiently and provide the impression that the firm is "on top" of these controls if they have all of the documentation assembled beforehand – policies, screenshots captured, logs acquired – either electronic or in paper, or in both so they can meet whatever needs of the assessor.

A firm should identify ahead of time what data they do not want out of their custody. Documentation with technical specifications or practices are seen by some organizations as highly sensitive and while they show this documentation to the assessor, they do not allow the assessor to take copies. Some assessors accept redacted documentation, such as a technical diagram without IP addressing or defined at a high level, and having this prepared avoids conflict over the documentation.

Once this information is assembled, future assessments can be made easier by keeping all of the information available and up to date. Most assessments address the same basic issues, though the questions may be asked slightly differently, so your screenshots and policies can be re-used for more than one client.

USLGL-RPT-0815016D