IRON MOUNTAIN®

GOVERNANCE IN THE CLOUD

2017 LAW FIRM INFORMATION GOVERNANCE SYMPOSIUM

CONTENTS

SYMPOSIUM STEERING COMMITTEE

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

BRIAN DONATO
Chief Information Officer
Vorys, Sater, Seymour and Pease LLP

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

RANDY OPPENBORN
Director, Information Governance
Foley & Lardner LLP

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

TASK FORCE

KAREN ALLEN
Information Governance Technologies Manager
Morgan, Lewis & Bockius LLP

MAUREEN BABCOCK
Privacy Officer
Snell & Wilmer LLP

SCOTT CHRISTENSEN*
Senior Associate
Olenick & Associates

GALINA DATSKOVSKY
CEO
Vaporstream, Inc

BRIAN DONATO
Chief Information Officer
Vorys, Sater Seymour and Pease, LLP

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

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

FARON LYONS
Sales Director Enterprise Solutions
Zia Consulting

LISA MARKEY
Chief Information Security Officer
Shearman & Sterling LLP

ROBERT WEAVER
Chief Information Security Officer
Blank Rome LLP

JOHAN WIDJAJA
Assistant Director, Records and Information Governance
Morgan Lewis

* *Task Force Leader*

SYMPOSIUM PARTICIPANTS

ANGELA AKPAPUNAM
Director, Document Lifecycle Services
WilmerHale

KAREN ALLEN
Information Governance Technologies Manager
Morgan, Lewis & Bockius LLP

DERICK ARTHUR
Director of Records and Information Governance
King and Spaulding, LLP

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

PAMELA BARTOLI
Manager, Records & Information Management
Foley & Lardner LLP

BRYN BOWEN
Director of Information Services
Schulte Roth & Zabel LLP

SCOTT CHRISTENSEN
Senior Associate
Olenick & Associates

TERRY COAN
Senior Director in the Information & Technology Services
HBR Consulting LLC

GALINA DATSKOVSKY
CEO
Vaporstream, Inc.

BRIAN DONATO
Chief Information Officer
Vorys, Sater Seymour and Pease, LLP

BETH FAIRCLOTH
Director of Risk Management
Seyfarth Shaw LLP

PATTY FITZPATRICK
Director of Information Governance
Katten Muchin Rosenman LLP

RINA HUNTER
Global Information Governance Manager and In-House Counsel
Latham & Watkins

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

SHARON KECK
Senior Consultant, IG & Risk
eSentio

NORMA KNUDSON
Director of Facilities Management and Compliance Support
Faegre Baker Daniels

FARON LYONS
Sales Director Enterprise Solutions
Zia Consulting

CRAIG MACDONALD
Records Senior Coordinator
Latham & Watkins

LISA MARKEY
Chief Information Security Officer
Shearman & Sterling LLP

BRIAN MCCAULEY
Director of Information Governance
Drinker Biddle & Reath, LLP

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

DANA MOORE
Manager of Records and Information Compliance
Vedder Price P.C.

RANDY OPPENBORN
Director, Information Governance
Foley Lardner LLP

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

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

ROBERT WEAVER
Chief Information Security Officer
Blank Rome LLP

KATHERINE WEISENREDER
Firmwide IG Manager
Cooley, LLP

JOHAN WIDJAJA
Assistant Director, Records and Information Governance
Morgan Lewis

EXECUTIVE SUMMARY

This paper examines the impact and application of Information Governance (IG) when using public cloud services and reviews the considerations that a law firm needs to address when evaluating a move to the cloud. It is meant to provide guidance to assist the IG professional when evaluating cloud providers and offers suggestions for topics to be discussed within the firm and with providers. We include several checklists of questions to consider, as well as references to more detailed sources for further consideration.

INTRODUCTION

WHAT TYPE OF CLOUD IS THAT?

Gartner defines **private cloud computing** as a form of cloud computing that is used by only one organization, or that ensures that an organization is completely isolated from others. Gartner defines **public cloud computing** as a style of computing where scalable and elastic IT-enabled capabilities are provided as a service to external customers using Internet technologies—i.e., public cloud computing uses cloud computing technologies to support customers that are external to the provider's organization. Using public cloud services generates the types of economies of scale and sharing of resources that can reduce costs and increase choices of technologies. From a government organization's perspective, using public cloud services implies that any organization (in any industry sector and jurisdiction) can use the same services (e.g., infrastructure, platform or software), without guarantees about where data would be located and stored.

The cloud. A term often heard and all too often misunderstood. "The cloud" is used to refer to all sorts of outsourced technology arrangements, despite the fact that it actually refers to a specific set of technical capabilities. Hosted applications, which have been used for years and simply referred to as "hosted," are now referred to as if they are in the cloud. Maybe, they are, maybe they aren't; frankly it's complicated. At the same time, many organizations leverage cloud technology in their own data centers – a "private cloud,"as opposed to a "public cloud," (see callout) but this is likely not seen as a cloud service by management.

The Information Governance (IG) professional must have an understanding of the cloud and the potential implications and considerations related to records and information management and governance. There are many resources available that provide more broad, expansive detail, several of which are referenced in this paper. This paper does not attempt to address all of these considerations, but rather focuses on those areas related to data governance.

So what's all the hoopla? The pitch we have heard from cloud vendors has been "put your data/application/platform on our computers and it's easier, faster and cheaper for you; you don't have to have a data center, maintain environmental controls, hire engineers and buy all the computers. You don't have to wait weeks to get a new server ordered, delivered, configured and installed. And let's talk about security – the cost of securing your own infrastructure grows every year – we're doing it across thousands of customers so we can give you cheaper infrastructure security more cheaply than you can yourself."

Sounds like a deal. So why is the cloud not embraced by everyone? As usual, a firm's management has to look at the entire return on investment scenario. One of the key factors to examine is the cost required to have sufficient network bandwidth to connect to the cloud using a variety of devices with acceptable performance. Maybe your organization invested in a private cloud, generating significant savings already and moving to a public cloud would not generate as much savings.

One of the most common concerns raised about moving to a public cloud is governance of information. When a firm's data is in-house, we have plenty of challenges maintaining good governance. When it is in a public cloud, we still bear the responsibility of providing good governance, however, the data is at arms-length and we may not have as much visibility or control as we would like. In this paper, we examine the impact and application of Information Governance (IG) when using public cloud services.

We must first define what it means for a law firm to be "in the cloud." Much of that answer lies in what differentiates the business of law from other industries. Document filings, docket deadlines and court appearances run on absolute deadlines. Communications with clients and third parties are interdependent and not necessarily linear. At times, data must be handled, stored, secured and dispositioned specific to firm, client, government and international requirements. Attorneys must meet these deadlines and comply with these requirements bound by their professional rules of service, not the least of which is client-lawyer confidentiality. Cloud service providers must meet and exceed the critical business needs of the legal industry: service continuity and data privacy maintenance. Data must always be ready for access yet must always be as secure as possible against breaches or other unauthorized activities.

ORGANIZATION-LEVEL UNDERSTANDING OF CLOUD USE

The cloud has had much media exposure, not all of which is positive or accurate. The challenge for the conservative legal industry is to weigh the perceived risks against the potential benefits. Since law firms and lawyers are often cautious about embracing technology change, it is important that executive management, directors, managers and attorneys and their legal staff have a solid understanding of how using the cloud benefits the firm, as well as the attendant risks. Historically, attorneys (and law firms) have been concerned with the use of the cloud, making it a challenge for IG and IT professionals to address the attorneys' data privacy and availability concerns. This may be changing. ILTA's 2016 Technology Survey[1] (ILTA) showed increases over 2015 in the use of both cloud storage repositories and of high-availability solutions amongst law firms. Of the latter, cloud only and hybrid cloud configurations are in use by over 50% of law firm respondents. While some jurisdictions are addressing cloud requirements in ethical opinions, there is no hard, fast, universal rule regarding use of the cloud.

To establish a cloud strategy and approach, executive management benefits from an understanding of the growing trend to use of the cloud and how it may change the data access, transmission and storage practices in the near future. Further many of the firm's clients are already using cloud technologies and may be very comfortable and, in fact, demand the same from their legal services providers.

One way to promote and maintain your organization's use of the cloud is with a straightforward policy communicated to all personnel defining:

- The classifications of information that may be stored in the cloud
- Approved data transmission methods to and from the cloud, where appropriate
- Synchronization between devices and cloud offerings, such as Gmail mailbox synchronization
- Who may access the data in the cloud
- What method or device may that data be accessed
- What firm (and client) specific IG and security procedures must be followed
- Enforcement that all defined policies and procedures must be followed before entering into the cloud.

ADVANTAGES TO THE CLOUD

Are you investigating cloud solutions or deciding to expand your firm's current use of the cloud? There are advantages that should be explored and weighed in the evaluation and decision-making process.

The cloud may be used as a means to simplify your infrastructure. The configuration and support options you choose can eliminate or significantly decrease the number of onsite servers and storage devices that need to be purchased, upgraded or replaced. Accessing and storing data in the cloud can decrease the amount of human and technology resources required to support on premises devices. In addition, time and resources needed to test and apply updates to software and devices can be reduced or become

[1] http://www.iltanet.org/resources/publications/surveys?ssopc=1 published by the International Legal Technology Association www.iltanet.org

unnecessary. Already stretched IT staff may be reallocated to other areas.

Much has already been written on the various infrastructure, service and deployment models for cloud use. The National Institute of Standards and Technology (NIST) published definitions of the cloud including options for infrastructure design, service models and deployment methods [see NIST SP 800-145].[2] The Cloud Security Alliance's "Security Guidance for Critical Areas of Focus in Cloud Computing"[3] can assist in planning your migration to, or evaluation of, your cloud usage. Understanding these options and choosing those that best support your firm's short and long-term IG strategies is key not only to deciding whether to move to the cloud, but also whether you should continue to stay there.

Cloud services do not have the upfront capital and/or costs of implementation that normally come with the initial implementation or expansion of on-premises services. Cloud use can offer service and payment options vastly different than those found in on-premises solutions, shifting budgets from capital expenses (Capex) to operational expenses (Opex). Storage costs, which can balloon with the on-premises need to provide space for the largest anticipated amount of data, have the option to pay as you go. Use of the cloud for data storage can be scalable with the potential for costs to be adjusted based on the firm's actual access and storage needs (see ARMA guideline). Savings in personnel time may also be significant.

Cloud and software as a service (SaaS) products and services allow law firms new options to the traditional software licensing models used in on-premises software agreements. These can allow for rapid adjustments of scale in both infrastructure and storage parameters. There are real savings in time and money over the traditional approach of predicting just how much of either is needed to support the business. It is also reasonable to expect that as more businesses move more of their operations to the cloud, there may be less on-premises product offerings by vendors.

An advantage might also be gained should your firm decide to cancel a vendor agreement. With an on-premises solution, costs are paid upfront and maintenance fees are then paid annually. Should you choose to discontinue use of the service after year one, you are still generally out the entire cost. With a SaaS solution, even if you signed an annual agreement, your investment is limited to that year's payment. Thus mistakes and trials, as well as one-off applications, are usually less expensive when they are in a cloud or other SaaS solution.

[2] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[3] https://cloudsecurityalliance.org/download/security-guidance-for-critical-areas-of-focus-in-cloud-computing-v3/

ESTABLISHING A FOUNDATION

Accessing data in the cloud and using one of the many cloud-based collaboration tools gives lawyers, clients and other third parties the opportunity to move away from the less time efficient "send-receive-respond" world of email and transition into real-time collaboration environments that are available in the cloud. Benefits include decreasing the time it takes to manage the average inbox and decreasing the volume of email being transmitted and the associated security and other risks.

Any IG initiative requires a sound strategy. Establishing a framework and position regarding cloud usage is no different. Failure to have a strategy can impede any transition to the cloud, create inefficiencies or, more importantly, expose the firm to unnecessary risk by potentially exposing sensitive information or contradicting client mandates. There are several best practices to consider when evaluating and developing your cloud strategy.

- Review your proposed or existing policy for cloud use against your data handling policies and procedures to make sure that its controls are consistent with those already in place. It is probable that your organization has data in the cloud of which you may not be aware and may not have accounted for within your IG strategy.
- Close any loopholes by identifying this information and verifying that it is governed per your policies and client agreements. It is important to review your cyber insurance policy's coverage when it comes to your use of the cloud.
- Avoid overlooking any important clauses regarding liability and exclusions or conditions that trigger certain coverage to take effect and any associated limits. Have an attorney specializing in cyber insurance matters review your current contracts before renewals come due as well as any new contracts that come into your firm. Failure to perform proper and thorough due diligence may result in higher premiums or gaps in expected coverage.
- Ideally, all cloud usage for data for which your firm is responsible should be supported by documented, repeatable and reported processes within your overall IG plan. The Law Firm Information Governance Symposium's paper on "Building Law Firm Information Governance: Prime Your Processes[4]" is a useful resource.

A number of legal professional organizations actively monitor issues as well as publish best practices related to the use of the cloud. These resources are tools that may assist general counsel and others within your organization to communicate changes in law and best practices in IG and security when it comes to the cloud. The ABA and state bar association websites are worth referring to on an ongoing basis. Other resources include ILTA's many publications,[5] white papers and surveys; ARMA International's "Guideline for Outsourcing Records Storage to the Cloud," which includes checklists on essential tasks to complete and legal issues to assess before moving to the cloud; the Legal Cloud Computing Association's LCCA Security Standards[6] and the library of papers related to this topic created by the Law Firm Information Governance Symposium[7].

Finally, IG standards must ensure compliance with local, state, federal and international rules regarding storage, transmission or security requirements (HIPAA, European Union's General Data Protection Regulation, etc.). It is a better practice to include the attorneys specializing in these areas to verify that firm policies and procedures are in compliance with these rules and regulations. International points of concern are covered later within this paper.

[4] http://igsymposium.ironmountain.com/building-law-firm-information-governance/

[5] http://www.iltanet.org/resources/publications

[6] http://www.legalcloudcomputingassociation.org/standards/

[7] http://www.ironmountain.com/Knowledge-Center/Topics/Law-Firm-Information-Governance.aspx

ENSURING INFORMATION GOVERNANCE IN THE CLOUD

Before a firm stores potentially sensitive information in the cloud, concerns such as how information will be returned to the firm from the cloud provider should there be a need to change providers, how retention policies are enforced, and how legal holds are handled must be considered. A firm must be prepared to handle a worst case scenario of a security breach at the cloud provider. IG professionals should also consider the implications if extra copies of a firm's information are created to logistically enable the use of the cloud, as described in the "Extra Copies/Duplicates" section below.

This section examines a variety of practical examples of cloud usage and some of the concerns each presents and explores what an IG professional can do to help with cloud governance.

IG THEMES

While there are unique considerations to address when evaluating or transitioning to the cloud, many basic aspects and questions to be asked are universal regardless of where data is stored. Appendix 1 provides additional information on what themes are unique to the cloud.

UNDERSTANDING LAYERS OF CLOUD SERVICES

Often "cloud" is referred to very broadly as any data that is not behind your firm's firewall. However, there are several layers of cloud services such as software as a service (SaaS); Platform as a Service (PaaS); and Infrastructure as a Service (IaaS). The table below provides detail regarding each type of service.

TYPE OF SERVICE	DESCRIPTION
Software as a Service (SAAS)	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
Platform as a Service (PaaS)	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.
Infrastructure as a Service (IAAS)	The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

These layered cloud services allow users to scale their investments based on need. The most common use of cloud is SaaS, which allows consumers access to applications via the web, usually for a fee. The governance considerations around the layers of cloud services include an organization's ability to know what you have and where your investments are while ensuring that those data and information assets are secure and defensibly disposed of when they are no longer needed. The key for law firms is to ensure collaboration among administrative departments and practice groups so that compliance in the cloud is achieved.

An example can be seen in something as simple as a SaaS copy request form provided to the firm's Facilities Management (FM) group by an outsourced copy center. The FM group has two options when setting up a workflow: 1) attachments to the electronic copy/print workflow form are associated with their web-based application and stored on cloud servers, or 2) the application is set to store the data locally on a server so it never leaves the firm and the web-application houses a pointer to the source document.

Both scenarios have IG compliance considerations. A best practice would be to avoid making a third-party storage vendor responsible for oversight of the firm's data. If the data is stored on the firm's on-premises servers, the firm needs to establish the duration for which the data for this transitory request is retained on the network. The IG professional should be involved in these projects to ensure that the best approach to comply with firm and client obligations is considered. The best option for some projects may be to use a cloud-hosted service, in which case the vendor must be fully vetted and retention applied to the transitory documents stored with them. The IG professional has a need to know about any project that involves data movement inside or outside of the firm for the aforementioned reasons.

GETTING YOUR INFORMATION BACK FROM A CLOUD PROVIDER

There are key consideration to examine when outsourcing to a cloud provider. What happens when the firm must retrieve their information the provider? There are several reasons the firm might need to retrieve their data.

- The firm might simply want to change to a different provider and need the data back. What will it cost the firm, and does the firm have their rights clearly outlined in their contract?
- The provider may go out of business. What happens to the firm's information? Can the firm recover it, and what are the steps? What is the priority in case of a bankruptcy?
- The firm might face a legal hold. Read the Legal Hold section below for more details.
- There may be a need to extract and transfer data for matter mobility or eDiscovery purposes. Can third-party tools extract data in a manner that is consistent with policies and service level requirements? Make sure there are no gaps between the Firm's needs and the vendor's capabilities.
- The firm may dissolve or merge with another firm and necessitate getting the data.

There are issues that a firm must address when it outsources major systems such as document/records management and email. They may be less important when using the cloud for other services, such as expense reimbursement systems. There is an extensive check list and detailed considerations, including service level agreement considerations, available in the ARMA guideline for outsourcing records to the cloud.

ENFORCEMENT OF RETENTION POLICY

When the firm entrusts a cloud provider with their data, the firm is still responsible for executing its data retention policies. While most readers will be familiar with the basics of their firm's Records Retention Schedule along with its process to retain or dispose of information appropriately, the cloud can introduce some complexity to this task.

Start with the most basic question: What is the cloud provider's process for managing document retention and destruction? Does your firm have tools to allow for appropriate retrieval, review and the enactment of the necessary steps for either retention or destruction, or is the firm restricted to making requests of the provider to take action? Most cloud providers are incented to provide access to some tools for information and disposition, but it is important to make sure those tools are flexible enough to handle both the firm's basic retention policies and any exceptions made based on specific client requirements.

Cloud providers often create copies of the firm's data to facilitate access, disaster recovery or to simplify system upgrades. These copies are often beyond the firm's control but should also be subject to the firm's retention policies, since they might expose the firm and its clients to risk. It is important to both ask questions about and, where possible, get documentation on the processes that create copies, and how these copies will be retained and disposed.

This process can be even more complicated if the cloud provider you contract with in turn contracts with other providers creating a layered service. These relationships require extra due diligence because the firm does not directly contract with these service providers, and because they may also create administrative or archive copies of the firm's information.

Since vendors may go through mergers and acquisitions, it is especially important to examine your contracts carefully. In one instance, a large software company bought a smaller email archive vendor that outsourced its hardware to a data center for its SaaS offering. Unfortunately for the large acquirer and the archive vendor's clients, the data center vendor filed for chapter 11 bankruptcy. None of the contracts had any bankruptcy clauses, so the clients were unable to receive any data for months.

Whether your data is with a Cloud provider or solely within your possession, many basic tenets of disposition protocols apply. For additional information on this topic, please refer to [the 2017 Law Firm Information Governance Symposium Report – Defensible Disposition].

LEGAL HOLDS

Once a legal dispute is reasonably anticipated, a firm has the duty to preserve information relevant to the hold wherever it is located, including data that is located in the cloud. The firm should ensure that the vendor has a method to preserve the data in place. For example, the provider might change data to "read only" or make a preservation copy to meet the needs of the legal hold. It is imperative that the firm know where all the data is related to the issue, both inside of the firm and outside of the firm to ensure preservation. The firm's contracts should also require vendors to notify the firm of any production request they may receive directly.

As firms consider cloud-based solutions, it is important to determine if the prospective system or technology can enforce your retention policy, legal holds and other IG policies. If the cloud-based system cannot, another solution should be considered.

Firms should evaluate if the vendor has a process and the means to search, locate, isolate and preserve relevant data. Firms should know up front what fees are associated with these services. Questions to consider are if the preservation methods are built into to their standard processes for legal hold management, or is there some charge associated with complying with a legal hold. (Reference ARMA Guideline for Outsourcing Records Storage to the Cloud section 3.3.2 and Legal Hold and Data Preservation Best Practices).

ON-PREMISES COPIES

Locale, data access and system performance sometimes require that data is available in more than one region. A proposed system must ensure data sovereignty while meeting performance and accessibility requirements (Service Level Agreements or SLA). Hybrid-cloud systems enable both on-premises and cloud storage and may be effective in enabling compliance with regulatory requirements for multi-national practices.

A plan must be created to manage duplicates and updates in either system. Synchronization should be designed to meet service level requirements to ensure proper policy is applied in both cloud and on-premises systems. This approach is typically complex and expensive as it requires redundant systems as well as bi-directional synchronization and rules around conflicting changes (simultaneous edits on documents stored on-premises and in the cloud). When breaches occur in either system, notification processes must be planned according to the source/location of the exposed content.

Globally conflicting data requirements do not diminish the demands of staff to get their jobs done. A good understanding of tools and processes used in your organization is recommended. Discuss practical approaches to the reality we all face. Our organizations have data in the cloud, both sanctioned and non-sanctioned. We need to identify processes to manage it without making our current situation worse or creating new responsibilities for staff.

'EXTRA' COPIES/DUPLICATES

The LFIGS members' experience suggests that cloud solutions today are typically more secure than on-premises implementations, especially for smaller organizations. Risk is introduced when users work outside of established processes and vetted systems. This leads to duplicated and unmanaged content in systems or locations that are not secured, managed, or audited. The firm's workforce travels and expects data/content to be available, on demand, in the context of the process of work.

Collaboration and convenience copies are generated whether content is managed in the cloud or on-premises. Firms should determine how the risks created by these convenience copies are mitigated. Some approaches to consider:

- Watermarking of files makes it clear whether the user has a convenience copy or not and also helps to ensure proper handling
- File-level security or endpoint management solutions can be leveraged to automate users' rights to content based on time or other triggers even when outside of managed systems
- Collaboration platforms provide secure deal rooms and can limit the ability to create local copies; annotation of online docs as opposed to editing local copies is a common approach.

Business rules and policies should be automatically applied

to content according to a user's role, the type of content in question and the activity required (such as allowing a third party to edit, comment or view content). Workers who are engaged in a process are biased by their work demands and should rarely manage the availability of convenience/collaboration copies as well as what rights users are assigned and how long content is accessible (lifecycle).

An example of how data can proliferate can be seen when using an outside eDiscovery vendor. When a firm is selected as local counsel for a national litigation, they are often asked to use the client's national eDiscovery vendor to save on cost; often licenses are distributed and suspended based on need. Because today's workforce expects a certain level of automation, it is not uncommon for a firm that is serving as local counsel to save or download key documents, or production sets relevant to the issue(s) they are helping to defend. If a firm has its own eDiscovery solution, this data could be copied or duplicated in the firm's eDiscovery solution or litigation network share. The IG professional should have an understanding of vendor relationships in the firm, as well as the firm's obligations and have a handle on where data is stored on firm internal systems to assist with a plan to manage and apply the appropriate security and retention to this data based on its lifecycle.

Depending upon the needs of your firm and clients, it may be necessary or advantageous to maintain a hybrid approach: the combination of a public cloud provider with a private platform.

BREACH AND NOTIFICATION PROCESS

Security best practices, and many regulations, dictate that any cloud provider have a notification process in the case of a breach of security exposes the firm's information to unauthorized access. Key considerations include what constitutes a breach, what type of notification the firm should receive, when the law firm should receive this notification, and what role the law firm will play in the investigation. Most law firms have similar obligations to their clients, and these obligations often vary from client to client. It is important that the firm understand exactly what notification parameters they have agreed to provide clients, so that they can determine if the cloud provider can do what is necessary to allow the firm to honor their commitments. There may be certain situations where, subject to applicable law or jurisdiction, vendors may not need or be permitted to provide a notification of breach. It is important to identify these caveats up front and know what they are required to disclose and when. Make sure you are cognizant of what the client's requirements are (e.g. clients often ask for notification within 48 hours) and ensure there are no discrepancies between client mandates and what the cloud provider can provide.

As an example, it is common for clients to ask for "immediate" notification of any suspected or actual breach. However, it may not always be possible for a cloud provider to notify the firm. This ability depends on the kind of infrastructure the cloud service uses and buys from third parties. Before agreeing to notification terms, it is important to be clear on the ability of all used cloud applications to be compliant.

There is a detailed discussion of how to handle this issue contractually in ARMA's Guideline for Outsourcing Records Storage to the Cloud.

MULTITENANT RISKS AND CHALLENGES

There is another vendor-related factor that firms need to review: multi-tenancy. The multi-tenancy model allows multiple clients or organizations to store their information in a single instance of an application on the same server and/or in the same data store, or repository. Typically, in a multi-tenancy environment, security is in place to manage access to specific information. There can, however, be concerns regarding the ultimate security of "comingled" information.

A cloud vendor frequently uses a business model that leverages resources across a large number of organizations (users), thus keeping costs down and increasing revenue. The model provides a way to reduce a purchasing organization's information technology costs, as vendor platforms or services are pre-existing.

Firms must first understand what they have committed to do for clients and what guidance their own information security and privacy polices provides. If there is limited or no guidance, clarification on the issue will involve input from the firm's experts on information technology, records management, the General Counsel's office, and perhaps the firm's privacy and security practice. The organization's policy then needs to be compared to the vendor's policy and any differences negotiated contractually.

CONTENT AND COLLABORATION

Software products typically used in law firms that are either generally offered as a cloud service, or have been offered as such in recent years are Deal Rooms, Document/Records Management Systems and Document Sharing tools.

DEAL ROOMS

Deal Rooms are often set up during merger and acquisition activity, and are frequently hosted in the cloud[8]. These products provide the opportunity for all parties to upload and share documents used in acquisition and to keep them from being emailed around. Of course, not all deal rooms are created equal, and when examining deal room software, all the considerations that are outlined in the ARMA guidelines should be taken into account. Some pertinent questions to consider when looking at deal room offerings:

- What is the authentication model offered? Is it a separate log in, where people have to remember yet another password, or is it a pass through and therefor easier to use?
- Can you edit documents right in the room easily, or is it too complex and will entice people to download the information and therefore help proliferate sensitive information?
- What happens with the documents once the deal is done, how is the deal room disassembled? Are the documents wiped clean? Returned to client? This should be clearly defined.
- What kind of auditing is available? Will the product track exactly who has read, edited and/or downloaded content? Is downloading even allowed? If downloading is, in fact, allowed, some of the benefits of document control and confidentiality may be defeated.

DOCUMENT MANAGEMENT AND COLLABORATION SOLUTIONS

Microsoft SharePoint Online

Microsoft offers Office 365™ and SharePoint™ (SharePoint Online) in the cloud. It is a very convenient system, allowing for easy sharing and collaboration. If the firm is using SharePoint Online as a document management system, there are several issues that should be considered.

- How are folders or sites set up for each client and matter?
- How are ethical walls enforced in this system?
- What happens when information is dispositioned or returned to client? Are all copies removed and how?
- What happens to the information if the firm chooses to unsubscribe?
- What are the international office considerations that a law firm needs to consider as it considers cloud storage?
- How are cross-site duplicates managed?
- Is lifecycle of content considered? Legal Holds?

DOCUMENT MANAGEMENT SYSTEMS (SUCH AS NETDOCUMENTS AND IMANAGE)

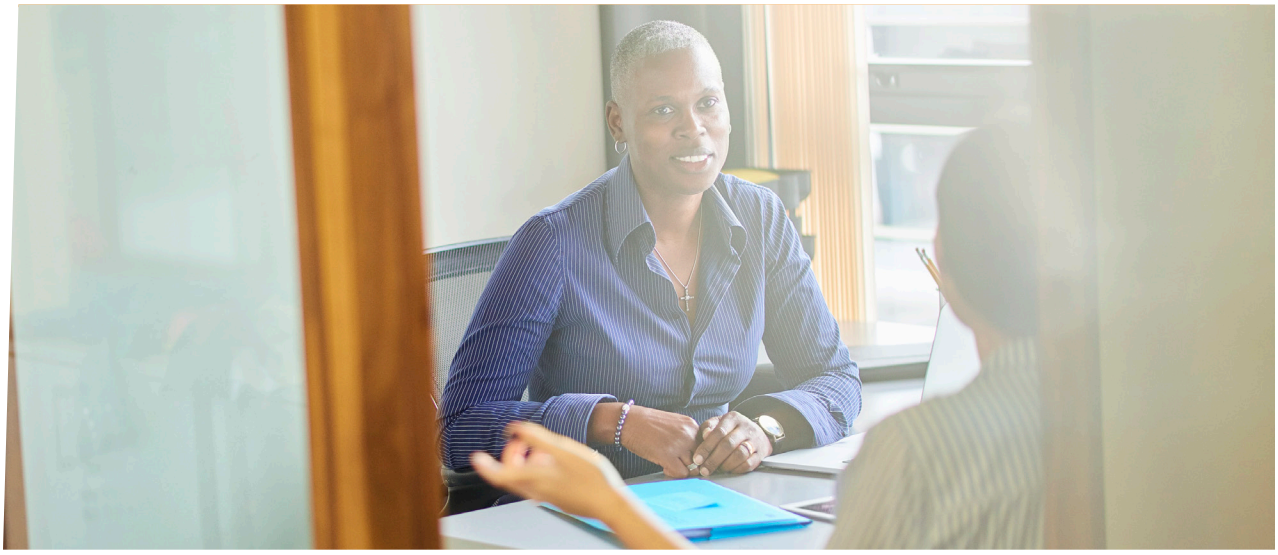
NetDocuments is a cloud-based DMS offering targeted specifically for law firms. When considering this system, the questions above should also be asked. However, since it has been designed specifically as a law firm technology, many of the issues above were directly designed into the system. Vendors such as iManage are offering cloud services combined with cloud infrastructure. Firms are encouraged to perform their own due diligence using the guidance discussed in this paper.

DOCUMENT SHARING TOOLS (SUCH AS SHAREFILE AND BOX)

Document sharing tools are a good way to share information with counsel and clients without resorting to email. These are excellent alternatives to both email and unsecure ftp sites. When choosing such a product, however, considerations similar to those discussed earlier come into play:

- Is there another password to remember? If so, it will be harder to use.
- Usually people download information, so security is only as good as the last download.
- What happens to the files after the work is done? When and how are they disposed of? Are local copies tracked or managed? Does that activity show up in audit reports?

[8] Note that it is common that Deal Rooms are entered into individually and often not within the purview of Information Governance. This should be mitigated if possible and incorporated into the information governance program.



- What protocol is followed in case of breach or unauthorized access?
- How is access synched with other sources, like workgroups and ethical walls?
- What happens to the information if the account owner leaves the firm?
- What tools exist for the IG function to monitor what data exists in the document sharing site?
- Does the vendor allow you to impose metadata tracking, such as client/matter numbers?

DATA CLASSIFICATION

Convenience copies on local and shared drives as well as collaboration platforms (both corporate and consumer) have been a consistent struggle for IG professionals for decades. The strategy of recognizing, classifying, labeling and managing convenience copies furthers the IG cause. A process should be identified for marking convenience copies as such and ensuring they do not outlive the final disposition of the official record. It is critical to classify content at its creation or ingestion so policy can be applied before duplicates proliferate.

Firms should leverage workflow automation for repeatable processes and to further enable knowledge workers by making their tasks easier and less complex. For example, content ingestion within a business process allows for automatic classification of the content within the context of the activity. Policy can be automatically applied, leading to the efficient flow of downstream work processes in an organization. OCR and auto-classification technologies should be used when content is not machine-readable or otherwise classifiable before resorting to manual processes.

ETHICS AND COMPLIANCE

Before you make the move to the cloud or before you expand your cloud use, ensure that there are no ethics issues with cloud use in the states and countries in which your lawyers practice. The American Bar Association (ABA) has published "Cloud Ethics Opinions Around the U.S."[9] that identifies states with written opinions on cloud usage and including opinion summaries. Although all states that have published opinions consider cloud usage acceptable, the ABA includes a qualifying statement on that webpage that "in most opinions, the specific steps or factors listed are intended as non-binding recommendations or suggestions. Best practices may evolve depending on the sensitivity of the data or changes in technology." Compliance with ethics requirements is not limited to attorneys. Involve general counsel or loss prevention to identify ethics and compliance requirements involved in cloud use and to communicate them as needed with firm personnel.

[9] https://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html

INFORMATION SECURITY AND HANDLING AGREEMENTS WITH CLIENTS

The degree to which clients approve of their data being moved to or accessed within the cloud can differ widely. Clients may have organization-specific cloud storage, security and transmission requirements instead of—or in addition to those—in common use. Details of these preferences are usually found within outside counsel manuals, engagement letters and other similar agreements. Attorneys and staff handling data for those clients must be informed of any procedural changes in data handling. It may be necessary to identify alternate storage and access arrangements for certain sub groups of client data.

Commonly seen client-specific data handling requirements with cloud usage can include:

- Prevention of comingling of client data with that of your firm or of other clients (such as data storage within secured containers)
- Encryption specifics by condition (transfer, at rest, restore), strength or software brand
- "Need to know" access limitations and ethical walls
- Third-party compliance with security, privacy and access controls for the cloud service provider comparable to those with which the law firm must comply
- Return or destruction of client data when the matter has concluded
- Breach notification
- Compliance with local data privacy laws and regulations
- Confidentiality, indemnification and insurance.

CONTRACT REVIEW

Cloud service agreement provisions need to address these areas that are core to the operational success of a law firm: data availability, security, compliance and maintenance of ethical standards. Many service providers and vendors that sell to the legal industry typically have cloud service level standards that support these business needs addressed in their agreements and products, however, it remains a buyer beware market. You are your best resource in determining if the service will secure your data based on firm policy and client requirements. Taking the time to review all details of the service/product agreement, the terms of service and the privacy policy of each service provider is well worth your time.

Understand all the pricing and payment options available up front. Ask the cloud service provider for a list in writing of all services and related costs that they offer. Request that those that which will be billed as part of your base cost be identified separately from additional services that are billed á la carte. Be aware that lower priced options may come with less flexibility and more risk.

For an organized approach, consider using a contract review check list. ARMA has a recommended check list within their "Guideline for Outsourcing Records Storage to the Cloud." The Cloud Standards Customer Council has included one such list in their "Practical Guide to Cloud Service Agreements."[10] For additional checklist items specific to the practice of law, see Tom Zuber's list "Limiting Risk in the Cloud: Smarter SaaS Agreements10."[11]

[10] http://www.cloud-council.org/deliverables/CSCC-Practical-Guide-to-Cloud-Service-Agreements.pdf

[11] https://www.attorneyatwork.com/limiting-risk-in-the-cloud-smarter-saas-agreements/

HOW CAN THE IG PROFESSIONAL HELP?

When dealing with Firm data in the cloud, the IG professional has an opportunity to help fill what is often a gap or afterthought relating to security management, classification, disposition and compliance with client obligations. It is best practice to have an established cloud vendor management program. The IG professional can play an instrumental role in that program and ensure that all of the IG principles are addressed appropriately. Often, many of the issues discussed in this paper are not fully vetted. In today's climate of client audit and the necessity for firms to provide evidence of best practices to sustain client relationships, the field is ripe for IG professionals to shine.

The following are some examples of where the IG professional can assist:

OPPORTUNITY	DESCRIPTION
Vendor Oversight and Compliance	Third-party vendor management is a key component to a successful cloud solution. The IG professional should take an active role in vendor risk assessments, audits and policy/procedure review. With some vendors, site assessments may not be possible. Assessments are easier if the vendor has certifications such as ISO certifications, SOC2 compliance reports and other documents relating to their best practices for handling, securing and disposing of the data on file.
Auditing and Tracking	Often in firms there is inconsistent tracking of who has access to cloud services on behalf of the firm in various groups. The IG group needs to know if a practice group has data in the cloud in order to assist with ensuring compliance with the firm's obligations to manage the vendor and its data.
Outside Counsel Guideline Compliance	Outside counsel guidelines often set forth various requirements that include not only billing but also Retention and Security requirements. See the Law Firm Information Governance Symposium Outside Counsel Guidelines Report (2014) for additional information.[12]
Security	Security requirements often detail that users should only have access to client information on a need-to-know basis. For example, imagine a practice group has a SaaS database to manage corporate entities. The firm has a paralegal that has just changed departments and no longer should have access. How is that change communicated to the administrator for that database? How is the security group updated? The same example can be used for terminated users. Often Active Directory (AD) is used to terminate users via a workflow from HR to IT.
Contract Review	The IG professional has a need to know and understand vendor SLAs relating to the vendors responsibilities for the movement of Firm data, data localization and data breach notification. Confidentiality terms (e.g. who can see what) should also be addressed in the contract.
Use of Cloud for Firm Business Records	It is becoming more common that firms are engaging with cloud vendors to meet the needs of administrative departments (e.g. recruiting, marketing, payroll). The IG professional should be involved in these efforts to ensure all IG requirements are met.

[12] http://igsymposium.ironmountain.com/outside-counsel-guidelines/

PRE-PLANNING CHECKLIST

An ounce of planning is worth a pound of cure. There are a variety of questions an individual tasked with procuring cloud services should ask before engaging with a vendor. After considering the ethics and client data handling requirements, you must consider issues specific to data storage, access and transfer in the cloud. Some of which are:

1. Are your existing application/services able to be integrated with or used within a cloud environment or will they being replaced?
2. What types of data will be moved to the cloud? This is a good time to decide on how to classify your data if that has not already been decided.
3. Who will be allowed to access to client or firm data in the cloud service or repository that you administer?
    1. All or subsets of your firm's personnel?
    2. The client?
    3. Approved third parties?
    4. The cloud service vendor?
4. If you plan to move or store firm data to a cloud-based service or repository which is administered by the client or a third party, who will be allowed to access your data?
    1. All or subsets of your firm's personnel?
    2. The client?
    3. Approved third parties?
    4. The cloud service vendor?
5. How is access rights management applied in the cloud? Will your data need to be secured to specific personnel within the above groups?
6. What access rights should be assigned to each group?
7. Does the cloud provider support multi-factor authentication?
8. Will cloud vendor personnel have access to the equipment holding your data?
9. Is your data encrypted?
    1. Is it encrypted at rest?
    2. Is it encrypted while in use?
    3. Will it be encrypted in transit?
    4. Will the cloud vendor have the ability to encrypt your data?
    5. Will the cloud vendor have the ability to unencrypt your data (e.g. who holds the key?)?
    6. Is the encryption method something you have applied or is it applied by or through the cloud vendor?
10. What methods/devices will you allow to be used to access the data?
11. Has the cloud provider detailed their security strategy in writing up front? Compare that with the firm's security systems (such as AD or LDAP) and confirm how they with integrate with each other.
12. Are there ways to utilize the security options within your application that will further support the security of your data while in the cloud?
13. How dependable is your current internet connectivity?
    1. How much of the bandwidth is used on average compared to the size of your pipe?
    2. Do you have a means to test deployment to the cloud before going live?

The ARMA guideline cited previously in this paper provides cloud technology and legal issues checklists and a vendor concerns questionnaire that can prove useful in this evaluation.

INTERNATIONAL CHALLENGES SURROUNDING THE CLOUD

The two main issues addressed by international regulations are data localization and data transfer. Data localization laws provide that data needs to be stored within a specific jurisdiction's boundaries. Data transfer laws typically establish that the recipient of data, if in another jurisdiction with data protection that is deemed inferior to the sender's jurisdiction, needs to take measures to ensure equal data protection. Law firms, especially those with international offices, face these two issues frequently, particularly when attorneys from various jurisdictions need access to information in order to represent the client. Uninterrupted access, while still complying with any international regulations is a primary challenge for law firms and is distinguishable from firm administrative data (such as employee or financial data) that might flow from a branch to the home office across borders.

Although the cost savings and easier maintenance benefits of cloud storage are great, these two issues need to be investigated and the chosen cloud provider must be able to comply with both. It is important to note that the cloud provider itself might not necessarily bring up these potential issues, but most cloud providers probably do have specific privacy and security compliance sections in their SLA's.

Prior sections discussed the importance of classification of data, a necessity to comply with various ethical rules and U.S. federal and state legislation. Because data at a cloud provider could be stored at different data centers, including in foreign territories, it is equally important to confirm the locale of where the data is actually stored and understand its implications.

For a law firm with international offices or that handles client data originating in countries outside of the United States, a concern is data segregation and where the data resides. Most of the concerns focus on the locale's privacy and security regulations. On the administrative side, a law firm's international offices collect personal data from its international employees for human resources, finance, and marketing purposes. Of course, the law firm might also receive data from an international client for purposes of providing legal advice. It is important to understand what type of data is being received, where it is stored, whether it is transferred, and whether it is accessed and by whom.

For example, a client might send data to a firm's German office, which then sends it across borders to its United States headquarters. This is obviously a transfer of data. In addition, even if the data is stored locally in the cloud, U.S. attorneys might have to access that data from U.S. soil. This type of data access is considered a "transfer" for purposes of a data flow analysis to comply with any local regulations. Another example might be that Russian regulations require that all data needs to be stored locally prior to any transfer. Thus, the firm needs to make sure that the cloud provider has local data centers. Cloud providers should provide the options to segregate the data and store it locally.

There are two reasons to keep things locally: (1) the governance and compliance of the country the data resides in that might require you to keep things locally and (2) the stability and governance of the place where the data center is located.

Another concern relates to a provider's the infrastructure in countries, such as India, where data protection regulation is not as robust. If a provider is hacked, litigation against the provider to recover damages might not be an option. A firm should realize what the recourse options are in a given country and determine whether those options are sufficient. In the United States, a firm could sue the provider if the data is hacked and there is recourse and a court system to litigate, which might not be available in other countries, especially in developing nations.

There are also concerns about government actions to combat terrorist activity. In Italy, it is much easier to get an impound order for terrorist activity. If your firm has data on a server in Italy and there is question of terrorist activity or drug trafficking that pointed to that server because of a co-located client of that cloud provider, the government can impound the entire server with no recourse. Thus, it is important to understand the landscape and the implications of where the data centers are.

THE ISSUES RELATED TO YOUR FIRM

The firm needs to conduct an analysis of data flows. This includes identification of the data subjects and the data recipients and a determination of whether these two groups are data controllers or processors. Further, the data that is transferred (including accessed remotely) needs to be put into classifications, and a purpose for the transfer should be attached. For law firms, the types of data typically consist of client data and the firm HR, marketing, and finance data that may contain personal information. The latter are typical categories of data that could flow internally within locations of an organization. The former, client data and data necessary to serve the law firm client could also trigger the need to obtain consent from the client. In addition, part of that analysis needs to include any existing or potential cloud providers. The analysis also is helpful with classification and business needs, which might be a consideration in making the determination in the future whether to work with a cloud system.

THE SOLUTION FOR DATA LOCALIZATION

As mentioned above, a variety of concerns could require data localization, such as privacy, security, compliance, corporate confidentiality, and, to a lesser extent, technical need. To meet the requirements for data localization, a cloud provider needs to offer its customers the option to place their data in any of the regions where that cloud provider might have data centers. The customers need to have complete control over that data and the cloud provider should not copy or move any of that data to another region. The cloud provider could offer tools to manage that data in place. Although cloud providers should have sophisticated solutions to mediate any potential localization law, it is the responsibility of the customer to demand specific solutions and select providers appropriately.

THE SOLUTIONS FOR DATA TRANSFER

Multinational firms and ones that service clients in the European Union and worldwide need to implement a satisfactory instrument to account for inter- and intra-organizational transfers of personal data across borders in compliance with international data protection laws. The most robust data protection laws are within the European Union, which also houses a significant portion of the world's data centers. Thus the solutions for data transfer will focus on the European Union, and three current options are binding corporate rules, privacy shield, and model clause agreements.

SCHREMS, SAFE HARBOR, MODEL CLAUSES, PRIVACY SHIELD AND BINDING CORPORATE RULES

In the Fall of 2015, the European Court of Justice ruled that the Safe Harbor program was invalid. (See Schrems case). It also ruled that EU data protection authorities have powers to investigate complaints about transfer or personal data outside of Europe and suspend data transfer until investigations are complete. Many companies then relied on the model clause agreements for proper data transfer to cloud providers.

Model clause agreements ensure that the data importer agrees and warrants to process the personal data received in accordance with processing principles that allow enough safeguards. For example, the agreements include the purpose limitation principle, restrictions on onward transfers, and adequate protection, rights of access and deletion. Law firms should enter into controller-to-processor agreements with their cloud providers and ensure that the data protection standards are met after a transfer.

Privacy shield is a new transfer agreement that was announced in February 2016 and the European Commission adopted it in July 2016. The privacy shield put stronger obligations on companies handling EU personal data and enacted a stronger enforcement of rights. With respect to third parties, the privacy shield provides that:

- The U.S. companies must inform individuals (data subjects) about a variety of facts, such as the type or identity of any third parties to which it discloses personal information and the purpose of it.
- Individuals must be granted an opt-out (with some exceptions) whether personal information will be disclosed to a third party.
- Agreements between the data importer and third parties must cover assurances from the third parties to protect the data.[13]

[13] http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm

As of January 2017, there were 1558 organizations registered with privacy shield. All the major cloud providers were listed (Amazon, Microsoft, Google, etc.). Although the major cloud providers are currently registered with privacy shield, it is recommended that firms still enter into model clause agreements with their vendors that process data. For example, AWS reverts back to the model clauses to comply with the EU regulations for data transfer, rather than solely relying on the privacy shield.

Lastly, binding corporate rules cover any intracompany transfers, but few major law firms have implemented this because of the tremendous resources and costs involved. However, for those that do have them, it is a good standard to show any cloud provider and ask whether it complies with the corporate rules standard.

In order to address international concerns, a check list should address the following:

- Where does your data originate?
- Is personal data collected?
- Is the data transferred or accessed across jurisdictions?
- What current local regulations are applicable to the jurisdiction where the data originated?
- Can the cloud provider comply with any local regulations and are they accounted for in a contract?
- What are the recourse options in the jurisdiction where the data resides in the event there is a privacy or security breach?

The Legal Cloud Computing Association has provided samples of standard contract provisions to account for many of these, such as location of data, privacy, and data breach policies. The Information Technology Industry Council (ITI) maintains a current snapshot of data localization laws across the globe. Finally, there are also tools available to help with identifying potential local issues with data transfer, such as Data Guidance, providing a comprehensive view of a country's constraints that might impact the transfer and the requisite solution. Free online resources provide a good start for the analysis. Links to all of these resources can be found in the Appendix.

The state of privacy law across the globe is in a constant flux. As we saw with Safe Harbor, legal constructs that we relied on previously could become invalid quickly. Luckily, there are still model clauses to rely on, but certain European DPAs have alluded to challenging their validity as well. Change in political regimes in both the United Kingdom and the United States could also impact how privacy is viewed and regulated. The May 25th, 2018 deadline for implementing the General Data Protection Regulation (GDPR) in the EU is looming. In short, when deciding to enter into an agreement with a cloud provider that will store data with international ramifications, one should be mindful of the latest developments surrounding this area of law.

CONCLUSION

There are many compelling reasons to harness the Cloud in a law firm, and most if not all firms have, or will have, solutions that rely on or leverage repositories and services in the Cloud. However, there are also multiple hurdles to overcome in order for the IG professional and the leadership of a firm to be comfortable that they have equal or greater controls in place than are possible on-premises. Even if the security controls are strong and encryption exists that surpasses Department of Homeland Security levels, compliance with client requirements (and the regulations which clients may be subject to) may be another matter, especially when cross-border issues are present. You must document any associated risks with your intended use of the cloud and include steps for mitigation of each within your IG plan which needs to address risk as well as cost. Review any potential significant risk ahead of time with executive management and secure their approval in advance of implementation. The better an IG professional understands how demands for efficient collaboration and limited time leads to potentially risky IG situations, the better the IG professional can help manage the risk.

Perhaps automation offers an answer to some of these monotonous and un-challenging tasks. With advances in auto-classification and document centric workflow, we have access to tools to improve our work product, get more done and reduce the overall risk to our institutions. These tools are available for systems implemented either in the cloud or on-premises, however this is not a silver bullet; there is cost involved in purchasing and maintaining these tools, and significant user training and cultural changes may be needed. This reminds us that there is always the human element, and to be successful we must ensure that governance processes are used consistently. Many a classification program has stumbled due to its requiring user input. Ultimately, the success of the governance program will be improved by genuine automation, requiring little or no user intervention. This is dependent on mature business process, well implemented technology, and significant support from firm leadership.

As always with information security and governance, the key to success is to follow the data; know the sensitivity of the data sets; understand the risks that are faced and the environment in which the firm is operating. Once firm and client information is in the cloud, governing it successfully is an ongoing process. Information governance strategies that account for data security, ease and dependability of access, compliance with federal and other regulations while continuing to meet the needs of the client have the best chance of ongoing success.

APPENDIX

APPENDIX 1 – IG THEMES TRANSFERRED TO THE CLOUD VENDOR

THEME	DESCRIPTION
Infrastructure	Depending upon the type of cloud, vendor may be responsible for the infrastructure on which the data resides. This may include, amongst other things, upgrades, patches, back-ups.

CHECKLISTS

- ARMA Guideline for Outsourcing Records Storage to the Cloud, 2010 ARMA International
- ILTA LegalSec Vendor Risk Assessment
- Cloud Computing Checklist, Law Society of British Columbia, Canada
- Cloud Computing Checklist, Florida Bar

BIBLIOGRAPHY

Ensuring Successful Cloud-Based Deployments, Galina Datskovsky, Ph.D., CRM, FAI; Information Management (September/October 2016)

Guideline for Outsourcing Records Storage to the Cloud, 2010 ARMA International

Retention And Business Practices in the Cloud, Galina Datskovsky, Ph.D., CRM, FAI; Archive Systems User Conference 2015

REFERENCED MATERIAL

The Legal Cloud Computing Association samples of standard contract provisions

Information Technology Industry Council (ITI) snapshot of data localization laws

Google "global data protection map" for more information.

ABOUT IRON MOUNTAIN

Iron Mountain Incorporated® (NYSE: IRM) is the global leader in storage and information management services. Trusted by more than 220,000 organizations around the world, Iron Mountain's real estate network comprises more than 85 million square feet across more than 1,400 facilities in 46 countries dedicated to protecting and preserving what matters most for its customers. Iron Mountain's solutions portfolio includes records management, data management, document management, data centers, art storage and logistics, and secure shredding, helping organizations to lower storage costs, comply with regulations, recover from disaster, and better use their information. Founded in 1951, Iron Mountain stores and protects billions of information assets, including critical business documents, electronic information, medical data and cultural and historical artifacts. Visit www.ironmountain.com for more information.

USLFIGS-CS-090817A