IRON MOUNTAIN®

OFFICE 365 AND AGILE IG

2019 LAW FIRM INFORMATION GOVERNANCE SYMPOSIUM

CONTENTS

LFIGS OFFICE 365 STEERING COMMITTEE:

BRIAN DONATO
CIO
Vorys, Sater, Seymour and Pease LLP

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

MIKE ENGELS
Principal Consultant Strategic, Consulting Services
Netrix

REGGIE POOL
Senior Director
HBR CONSULTING

MICHELE GOSSMEYER
Global Director, Information Governance, Risk & Compliance
Dentons

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

WORK GROUP PARTICIPANTS:

JIM MERRIFIELD
Director of Information Governance & Business Intake
Robinson & Cole LLP

ROB WEAVER
Chief Risk & Security Officer
Blank Rome LLP

KATHERINE WEISENREDER
Senior Information Governance Compliance Manager
Cooley LLP

MADELINE LA COUR
Director, Business Intake and Records
Baker Botts LLP

INTRODUCTION

If your firm is pondering the Office 365 or not question, you are not alone. And you are certainly in good company in the legal industry. But why is this MS upgrade different from those of the past? And why is there such a difference in views between firms that jumped in right away and those that remain hesitant?

A group of Information Governance (IG) professionals gathered at the Law Firm Information Governance Symposium ("LFIGS" or "the Symposium") for two days in June 2019 to dive into the O365 debate and determine how to provide those struggling with this question with helpful guidance on how to approach the issue.

So, what's the big deal?

If your firm is a Microsoft shop, there is a good chance that you are already paying for Office 365 (O365). Your firm may already be using SharePoint, Exchange Online, Teams or OneDrive for Business and/or any of the other dozens of tools available in Microsoft's cloud. If not, your firm's tech savvy users might already be using it at work, or, if you have prevented that, at home. Even if you have no vestige of O365 in your shop, your clients do, and may have already invited your lawyers or staff to collaborate on SharePoint or in Teams. But even if, like Neo in The Matrix, you have dodged all these bullets with the skill of a super ninja, it still won't matter. So much of Microsoft's resources are devoted to developing this platform, that eventually it won't make sense to do anything but embrace O365.

So, what is an IG professional to do? The good news is that there are a wealth of processes and systems designated to hold records content, such as your records system or document management system (DMS), most likely already in existence at your firm. So if you can simply make sure that O365 content eventually ends up in those systems, you are golden! The problem is that strategy only addresses a small part of the issue, because some of the constructs in O365 simply don't translate well into static documents that can be stored in a records or document management system. And worse, any attempts to constrain the use of O365 tools will cripple the very features that make the tools so attractive.

But, that's okay. You have had to handle new systems before. Generally, IG principles still apply, so you only need enough time to engage in careful design with those implementing O365 so that you can give the proper guidance. Except, O365 projects rarely happen in a manner allowing for that kind of lead time. And due to the interconnectivity of O365, the implementation of a relatively simple part of O365, such as Exchange Online, can rapidly lead to the use and adoption of more complicated tools that present several IG challenges to which you don't have answers. But even if you do find answers, O365 rapid changes means that today's approach may not handle tomorrow's reality. You may grow concerned that O365 will create unmanageable risk for the firm and advise strongly against implementation and adoption. But then you would be perceived as a roadblock and risk being excluded from the conversation altogether. What a dilemma!

Einstein allegedly[1] said that "The significant problems we have cannot be solved at the same level of thinking with which we created them." While this paper won't propose the O365 dilemma is quite that dramatic, we do suggest that this new challenge requires a new approach. One where, much like an "IG MacGyver", we use the tools available within O365 in creative combinations to facilitate whatever IG is obtainable given the time and technology constraints, and then work to continually improve in small increments. We must seriously consider where O365 will emerge in the document repository space and how it will integrate, interconnect or align with the DMS and other records systems—or how it won't! It will require IG professionals to adapt rapidly, using a deep understanding of the technology and a willingness to embrace new levels of uncertainty. This paper proposes that to be successful with O365 and similar technologies, IG professionals must embrace "Agile IG."

We set out the Agile IG approach and discuss how it can be used to initially survive and eventually thrive in an O365 environment. We walk through several IG processes and discuss how this approach can help deal with the uncertainty while finding ways to help the business mitigate risk.

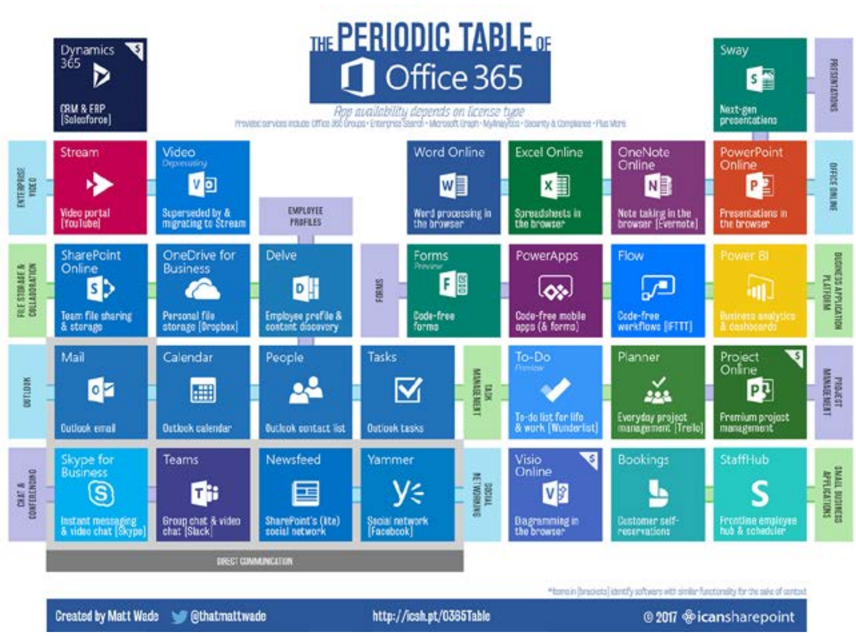
But to start, you must become familiar with this new IG arena, perhaps gaining deeper familiarity with this tool than tools you have known in the past. And that requires a commitment to what we call deep learning.

OFFICE 365 AND DEEP LEARNING

IG professionals are no stranger to learning. Understanding new technology and new processes is a required part of the job. So why should O365 present a different challenge? We see three main reasons: complexity, rate of change and speed of adoption

COMPLEXITY

Software is software. There are menus, features and functions. Why should O365 be different? Well, O365 isn't just software, it is an entire ecosystem. For example, most people, if you mention O365, think of Word and Excel. Some more savvy folks think of Exchange Online, SharePoint Online and maybe even Teams. Consider the diagram below:



This illustrates that there are an enormous number of applications in O365 and an enormous number of configuration settings, each of which potentially changes how you think about governance of the information on the platform. Yet, this is only part of the picture. Office 365 tools are designed to work together. So, for example, if someone creates a Microsoft Team, they are actually using several O365 apps, and perhaps even external apps, each presenting a set of potentially unique IG challenges. Because it is so large and complex with so many data configuration options, you may not have anyone in your firm that understands it all. It is likely that you will have trouble finding a person who can inform you adequately enough to make the types of judgements you need to make about IG and O365. All by itself, this complexity would be an overwhelming challenge, but O365 doesn't stay static.

RATE OF CHANGE

Microsoft has designed O365 to be able to quickly adapt to changing needs of its users; so it changes, constantly. And often in significant ways. Keeping up with all the changes in O365 could be a full-time job. Consider the graphic below of Twitter feeds to follow to stay up to date on changes (from the very useful http://icansharepoint.com):

There is an overwhelming amount of information, because there are a very large number of changes to this very complex product. And often, these changes impact how you solve certain IG problems. But, unfortunately, you don't have a lot of time to consider all these options.

SPEED OF ADOPTION

A recurring theme for this paper is how quickly the use of O365 apps can spread in your environment. It's not unlike a viral cat video, expect that once a tool is deployed to one set of tech consumers, others will rapidly follow. Since many of these tools are easily available, interdependent and quick to deploy, you can't wait for others to become experts on the software. Because adoption might be spreading like a wildfire at a gas station if you do wait, with similar disastrous results.

HOW DO I GET STARTED?

The conclusion is that the IG professional needs to learn more about this technology than perhaps any before. While the proposition is scary, the good news is that there is lots of help available.

GET ACCESS

A very good starting point is to get access to as much of O365 as your IT department permits. There is no substitute for firsthand experience.

MICROSOFT OPPORTUNITIES

Microsoft offers many different options to help with training and user adoption. Customers with Enterprise licensing have access to:

- training material
- online videos
- training vouchers which can help their teams understand the new O365 offerings
- customer Immersion Experiences, via Microsoft partners, at no cost to help understand how to leverage these technologies in your environment.

CONSULTANTS

O365 is not a new technology, and there are a variety of very qualified consultants who make their living understanding and implementing O365. Many even have law firm experience. If your firm can afford it, spend money to at least have a planning and brainstorming session. While you may not emerge with an airtight IG plan, you will emerge with a deeper understanding of the issues involved and the tools available to help you solve them.

WHERE DO YOU DIRECT YOUR INITIAL FOCUS?

We have established that O365 is big and complicated, but you need to start somewhere. Here are some recommendations:

LICENSING

Start by working with your IT department to understand what O365 licenses you have. Most likely, you have E3, E5 or a mixture of both (as an example, you can purchase an E3 license and add Compliance to get access to IG features such as Advanced eDiscovery and Advanced Data Governance at a lesser cost than the full E5 license). Understanding what your licensing options are and what you already have helps you understand what tools you have in your IG tool kit.

OFFICE 365 SECURITY & COMPLIANCE CENTER GOVERNANCE FEATURES*

GOVERNANCE FEATURE	O365 ENTERPRISE E1	O365 ENTERPRISE E3	O365 ENTERPRISE E5
Access to the Security & Compliance Center	Yes	Yes	Yes
Office 365 Cloud App Security	No	No	Yes
Threat management such as mail filtering and anti-malware	Yes	Yes	Yes
Advanced threat management, such as threat explorer for phishing campaigns[6]	No	No	Yes
Customer Lockbox	No	No	Yes
Mobile device management	Yes	Yes	Yes
Data loss prevention for Exchange Online, SharePoint Online, and OneDrive for Business[7, 9]	No	Yes	Yes
Data loss prevention for Microsoft Teams chat and channel messages	No	No	Yes
Information barriers	No	No	Yes
Data governance[1]	Yes	Yes	Yes
Advanced data governance[2]	No	No	Yes
Content search	Yes	Yes	Yes
eDiscovery cases	Yes	Yes	Yes
eDiscovery holds (including query-based eDiscovery holds)	No	Yes	Yes
eDiscovery export	No	Yes	Yes
Advanced eDiscovery[5]	No	No	Yes
Archiving	Yes	Yes	Yes
Unified auditing[8]	Yes	Yes	Yes
Manual retention policies	Yes	Yes	Yes
Supervision policies	No	No	Yes

*Features listed are as of the publication of this paper. Options may change.

SOURCE: https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-platform-service-description/office-365-securitycompliance-center

YOU WILL PROBABLY NEED TO INVOLVE YOUR MICROSOFT REP OR YOUR VALUE-ADDED RESELLER TO GET ALL YOUR LICENSE QUESTIONS ANSWERED. AND NOTE THAT SOME OF THE DISCUSSION LATER IN THIS PAPER MAY REQUIRE SPECIFIC LICENSING.

COMPLIANCE TOOL

Microsoft has put serious thought into how to handle security and compliance. Start at https://docs.microsoft.com/en-us/office365/securitycompliance/ to view the wealth of information they provide.

UNDERLYING STRUCTURE OF VARIOUS COMPONENTS (WHAT DATA IS CREATED AND WHERE)

While Microsoft provides extensive documentation on all things O365, it might help to start with something a bit more friendly. The aforementioned icansharepoint.com provides excellent infographics to explain difficult concepts, such as file storage locations and SharePoint vs OneDrive. Examples are here http://icansharepoint.com/infographic-the-document-circle-of-life-in-office-365/ and here: http://icansharepoint.com/wp-content/uploads/2017/05/Office-365-Groups-1400px.png .

As you become more and more educated about the O365 platform, you are preparing yourself for the next step, becoming an Agile IG ninja!

OFFICE 365 AND ADOPTION WITH AGILE IG

As an IG professional invested in deep learning, you completely understand the appeal of O365. It can do so many different things to aid productivity that it makes sense people are shouting "I want it now!"

It's only logical that the legal industry is not immune to a global culture steeped in instant gratification. As quickly as our lawyer population learns about a new tool that can improve their ability to do their jobs, they're requesting access to it. After all, this convenience translates into efficiency, and efficiency is a competitive advantage.

So, many readers will find themselves under great pressure to quickly deploy O365 tools, ready or not. They have limited time to plan governance and limited ability to lengthen the deployment.

In the introduction, we discussed the necessity of a new approach, Agile IG. But like most new approaches, Agile IG is based on something well established.

A (VERY) BRIEF HISTORY OF AGILE

The use of Agile principles goes back many years, but perhaps most notably, Agile made its mark in the world of software development. Traditional software development called for a long, multi-stage planning cycle that focused on documentation and identification of the requirements before any actual software was developed (sound familiar?). However, over time, this process, while thorough and mature, still often produced software that didn't meet the needs of those who requested it in the first place. Why? More often than not, what the person requesting the software thought they wanted changed when they started using the software, because humans are generally bad at anticipating what they will need in a new set of circumstances.[2]

Agile solves this problem by focusing on developing in very small chunks, starting with the minimally necessary functionality to get feedback from people using the software. The goal is to get feedback and rapidly incorporate that feedback into a new version. This iterative process is repeated multiple times until the program reaches a mature state (or beyond). In this way, the software evolves as the software user gains experience with the process of using it. The end product actually has a much better chance of serving a valuable purpose.

AGILE PRINCIPLES

So, as IG professionals, what do we take away from this approach? Let's start with the most important principles:

LIVE WHERE YOUR CUSTOMER LIVES

As an IG professional, you have a responsibility to minimize risk for your firm. However, if your answer is always "you can't do that" then you are likely ignored by those who have the clout to ignore you (in many organizations, that would, at a minimum, be all lawyers.) To make recommendations that your lawyers can accept while also protecting your firm, you need to deeply understand how they intend to use O365, how it will benefit them and, ultimately, how it will benefit their clients. Be willing to invest significant time in watching and learning how they want to work.

ITERATE RAPIDLY, FAIL FAST

Once you have some idea of what makes O365 appealing and effective to those using it, think about the types of controls that will protect that firm without disrupting the usefulness of O365. Then, implement a very few of those controls, focusing on those that have the best combination of high-risk reduction and minimal work disruption. After implementation, quickly focus on how the controls impacted lawyers. Ask questions such as:

- Did the controls work?
- If so, why? If not, why not?
- How did it impact the overall experience of using O365?

Use the information you gather to change the controls you implement. If the controls you started with are a complete disaster, learn from them, remove them and try a different approach. If they worked well, build upon them. After each new release of controls, ask your questions again.

Of course, to make this approach work, you must relentlessly communicate what you are doing to the legal team and collaborate with your GC's office to ensure you have their support. Some approaches won't work depending on a firm's risk tolerance, but you likely have many options and can find one to fit your needs. As your wins increase using this approach, you have a case study you can share with others interested in deploying similar tools.

FOCUS ON SIMPLICITY

The simpler a control is to implement, the better it is for the IG professional. The simpler it is to use a control, the more likely it is to have the desired impact. Use your experience with deep learning of the O365 toolset, combined with multiple observations of the people using the tools, to find the simplest controls possible, both for you to implement and for them to use. For example, a control that is already built into O365 and is transparent to O365 users is ideal, even if it doesn't reduce risk as completely as a custom-designed process requiring lawyer and/or staff to take proactive steps.

DON'T LET THE PERFECT BE THE ENEMY OF THE GOOD

IG professionals can be very focused on building intricate processes designed to protect the firm in a multitude of situations. Resist that urge! When IG professionals are being iterative, quick, focused on what is simple and mindful of the needs of the people using O365, they will choose to implement good- enough controls and constantly evolve those controls as both the needs and tools change.

Because IG professionals rely on tools and techniques that are in O365, and likely outside of their normal toolset, they likely won't have perfect solutions at their disposals anyways. Work closely with the leaders of the risk management function at your firm. You may have to convince them of the validity of this approach and perhaps occasionally accept that there are deal breakers, even for the Agile IG professional.

REFLECT. LEARN. IMPROVE.

Agile doesn't end. There are always lessons learned and opportunities to improve. Agile suggests breaking your efforts into small time chunks, such as two weeks or a month. After each of these chunks, a key part of Agile IG is continuous learning, about the tools, the environment and the people impacted by both. Keep up on key sources for recent issues, lessons learned, etc. from others in the industry or O365 community. Applying that learning to mature your processes eventually moves them from good to great. Sharing what you learn with the other governing bodies at the firm, such as your IG committee or others in the risk management function, spreads the greatness to other implementation efforts.

These simple principles create the framework that guides an IG professional's transition into Agile IG.

AN EXAMPLE:
IMPLEMENTING MICROSOFT TEAMS AT THE REQUEST OF A CLIENT

With these principles firmly in mind, let's walk through how we might apply Agile IG to a common occurrence: A client request that leads to the utilization of a technology before the firm can completely plan for its implementation.

In this scenario, a client has asked that the firm host a Microsoft Teams site for a set of transactions the firm is advising on. The partner in charge readily agreed to help the client, pledging to implement any tool required. When the lawyer called IT for help, IT involved Pat, our IG professional!

With limited time to plan, Pat considers approaches that make high-speed deployment more palatable. Fortunately, Pat has engaged in deep learning and knows quite a bit about Teams. She partners with IT to learn even more. Armed with this knowledge, Pat is ready to live where her customer lives, reaching out to the lawyer and asking to meet to discuss all of the different ways the legal folks might use Teams. Pat learns that the client wants to have threaded discussions about each deal, a document repository, calendar of key milestones, list of key players, a repository for deal knowledge and who knows what else. Currently, all this information is kept in various documents in the document management system. Pat learns a great deal about what drove the client to Teams, especially the desire to have multiple people that work for the client interact with firm lawyers and share their insights about the deal in a searchable format that either the client or the lawyer can use for future reference.

Pat leaves the meeting and starts thinking through some basic questions, trying to find the best set of IG controls to reduce risk and implement rapidly, without impacting what makes Teams so desirable to the client. Pat thinks about:

- Who can create Teams? Any user or a single delegate?
- Who will handle ongoing account / site administration?
- How might a naming convention work?
- What retention policies can be applied using native O365 tools?
- What risks does external access (people outside your organization) to Teams present? How can the firm mitigate these risks?
- Teams allows the installation of add-on apps. Should this be turned off?

After discussing with peers and after multiple conversations with the legal team, Pat decides to ask the legal team to use a basic naming convention for each channel to contain information for different deals. She warns about the dangers of having outside access to conversations that might otherwise be casual and agrees to monitor the situation.

After a few weeks, Pat checks in with the legal team and is pleased to learn that the naming convention is going well. However, external access is not. When talking with the legal team, she discovers that the client really hasn't participated in many Team-hosted conversations. She wonders if the risk is justified. After talking with the firm's security team and risk management leaders and discussing her concerns about external access risk, she asks if the legal team would be willing to experiment by turning external access off. They agree to try and fail fast if it is a bad idea. Fortunately, this is very simple to implement.

Perhaps predictably, everyone quickly realizes it is a bad idea. Right after implementation, a client tried to access Teams, couldn't and complained to the legal team. Pat works with IT and quickly re-establishes access for the client. After discussion with her Risk Management partner and the legal team, she believes she can mitigate the risk by having the client read and acknowledge a disclosure about the risks of have their Teams site open to external connections. The legal team agrees and goes about the task of notifying the client.

In the meantime, Pat reflects on this challenge and decides that she could do even a better job of restricting access if she could apply a security control. She researches and determines that there might be a way to make sure only the machines at the client's premises can access the Team site. After discussion with the Legal team, she learns that the client never accesses the Teams site away from their place of work. Therefore, she works with the security team to restrict what computers can externally access the Team site, based on their domain. The legal team is very happy with this approach, but during her follow up, she learns that they are struggling with the very cumbersome process of file sharing, which requires them to use existing tools.

Pat knows her organization already has several tools for file sharing and prohibits maintaining copies or creating data on those systems. She's aware of the firm's Acceptable Use Policy, which states that data can be transferred by approved SFTP systems or manual encryption. To align with the established policy, it is an easy decision for Pat to turn off the 'share files from cloud storage services' offered by Microsoft, which currently include ShareFile, Dropbox and Google Drive, services not approved by Pat's firm. This change is also very easy to implement.

Gaining confidence, Pat tackles the challenge of file retention within Teams. The firm has dictated that any record must be contained in the document management system as an official record. Pat knows that using the security and compliance center in O365, she can force the deletion of any file that has not been accessed for 30 days and then issue procedures to the legal team that they must move files from Teams into the DMS or risk them being deleted, similar to how the firm handles Outlook email. This seems like a very nice solution. Pat decides to run it past the legal team, where she learns that important files are often referenced and linked in conversations, and those conversations serve as an important archive for the client. If the files is moved to the DMS and removed from Teams, then the conversation link no longer works. Pat is glad she had this discussion, because it reminds her that Teams is not like Outlook, and her approach won't work.

Continuous improvement is dependent upon constant feedback and reflection about what's working or not. In many ways inviting the participation, assessment and reflection of our end users on how processes are playing out will support improved process over time. Planning reflection as a regular part of the process builds in those opportunities for continued improvement.

AGILE IG GOING FORWARD

By now, hopefully you have realized that there are elements of Agile IG that you already practice, day in and day out. However, by focusing on living where your customer lives, iterating rapidly and failing fast, focusing on simplicity, refusing to let the perfect be the enemy of the good and reflecting so you can learn and improve, will equip you to deal with the very significant challenges of O365. Next, let's talk about some of those challenges in the context of a few familiar IG processes.

OFFICE 365 & KEY IG PROCESSES

The following section discusses several key IG processes that leverage the native compliance features in O365. These were chosen due to their complex nature and to help you understand how the O365 federated SaaS environment can benefit your IG activities by centralizing the processes and activities you need to develop and perform to handle these common problems. In the following sections we discuss four of these key IG processes:

- eDiscovery – Preservation and Production
- Data Governance – Retention and Strategy Development
- Matter Mobility - Moving content into/out of O365
- Regulatory and Compliance – Compliance Tracking and Reporting

BEFORE YOU BEGIN – CLOUD, ON-PREMISE AND HYBRID CONSIDERATIONS

When considering options for managing content in O365, engage in deep learning about how the platform is implemented at your firm. It is rare to find an organization using O365 for only email and file storage. Most instances of O365 are hybrid implementations – a combination of O365 cloud services (Exchange, SharePoint, OneDrive, Skype, etc.) integrated with legacy solutions already in place (on-premise Exchange, SharePoint, etc.).

When attempting to manage content in email and SharePoint, you need to design solutions that address both cloud and on-premise content. Many features found in the O365 Compliance Center are only applicable to content residing in the cloud. As an example, Retention Policies and Labels (discussed below) can only be used to govern content that sits in the O365 cloud. Conversely, if you want to manage retention for content on-premise in Exchange or SharePoint, you need to develop a different strategy specifically for those systems. Live where your customer lives to understand how they might use these implementations differently. Then, iterate rapidly by designing and implement simple controls on each platform. Learn by gathering feedback and fail fast if necessary. The example on the next page highlights some of the simple controls already available for email retention in this hybrid situation.

EXAMPLE: HYBRID EMAIL RETENTION MANAGEMENT

Your firm has decided to implement email retention (the ability to retain/delete information in Exchange online) in a hybrid Exchange environment. There are two ways to do this. The first option is to deploy Messaging Retention Management (MRM), which helps save, archive and delete information in Exchange mailboxes. MRM works for both Exchange Online and Exchange on-premise for versions 2010, 2013, 2016, and 2019. The second option is to use O365 Retention Labels and Retention Policies (Labels/Policies). Unlike MRM, Labels/Policies will only work with Exchange content online. Luckily, the functionality of MRM and Labels/Policies can be combined to build a complete solution – you don't have to choose one or the other.

Once you understand your firm's balance of cloud and on-premise, you'll be better equipped for the key IT process planning and implementation. So, let's jump into a few of those.

E-DISCOVERY FEATURES

One of the most common challenges that IG professionals face when managing content with O365 is responding to discovery requests. The O365 Compliance Center offers the ability to prepare for discovery requests given your firm's current use of the platform. Differences in discovery capabilities become apparent when looking at the O365 licenses available.

A quick overview is presented in the below table, specifically the differences between the standard discovery features found in the popular E3 license versus the advanced discovery functionality available through the more robust E5 license.

E-DISCOVERY	E3	E5 / E3 + ADVANCED COMPLIANCE
In-Place Preservation	√	√
Case Management	√	√
Search	√	√
Export	√	√
RMS Decryption	√	√
Advanced Processing		√
Email Threading		√
Near Duplicate Identification		√
Themes		√
Predictive Coding		√
Processed Export with Load File		√

E-DISCOVERY	E3	E5 / E3 + ADVANCED COMPLIANCE
Search and Tagging		√
New: Custodian Management		√
New: Custodian Communications		√
New: Working Sets		√
New: Review and Annotate		√

Keep in mind that advanced discovery functionality is also available with an E3 license if your firm chooses to also purchase "Advanced Compliance," which provides specific compliance functionality such as advanced discovery and advanced governance at a lower price point than E5.

Before we go further, we realize that your firm likely already has tools and a process for preservation and other stages of e-Discovery, but as an Agile IG ninja, you should consider O365 capabilities. You may find that the integration of O365 tools with the content contained in O365 provides a simpler, more elegant solution for O365 data than what your firm is currently utilizing. If that is the case, the Agile IG principle "focus on simplicity" suggests that you use this native discovery functionality.

In addition to the different types of discovery functionality within the platform, there is also a specific order of operation that must occur to effectively leverage native discovery capabilities. To leverage the in-place preservation functionality, you must create a "Case" and identify custodians and data targets. These activities require appropriate case management permissions within the system. So, working with IT to develop your internal roles and responsibilities is critical.

Most organizations choose to leverage a mix of discovery capabilities within O365 through the development of an O365 Discovery Playbook. The Discovery Playbook lays out various options and decisions, such as the required roles and responsibilities (as mentioned above) as well as best practices for applying preservation and collection functionality, how to leverage advanced discovery capabilities like legal hold notification tracking, deduplication of responsive material, predictive coding of harvested information, review and annotation materials for production and so on. A well-thought-out Discovery Playbook helps you to decide when it makes sense to use all or part of the native O365 discovery features and when assistance from outside legal counsel is necessary (e.g., large-scale responsive production). Learning from each iteration of applying the Playbook and using that information to continuously improve the Playbook to make your firm even more agile when responding to complicated discovery requests.

DOCUMENT PRESERVATION

Any approach to preservation using O365 should be vetted with the General Counsel (GC) and Information Governance function within your firm to formalize a preservation strategy. Consider having a policy that covers preservation responsibilities and standards for all applications that house firm data. When using O365, the key is understanding available tools and how they fit in to your firm's overall preservation strategy. This should be outlined based on the substance of discovery requests received and ideas on how best to respond to those requests.

When thinking of preservation, begin with the end in mind. Provide clear guidelines for O365 use to allow the firm to benefit from the product while also drawing upon best practices for e-Discovery-related issues like litigation hold, case management and information governance.

Personnel managing these requirements and ensuring compliance must have clear visibility into the complete process flow of requests in order to see how preservation can be accomplished in O365. To do this, you need to vet options with your GC and the Information Governance team before selecting compliance modules to be included in your O365 licensing package. Engage in deep learning so you fully understand the implications of each module. And if purchasing decisions have already been made that don't include the needed functionality, remember the flexible options mentioned earlier in the licensing section of this paper.

To discuss preservation in O365, you must understand where documents and files are stored and what tools are available to you in O365 to preserve them. Consider the following when constructing a preservation policy:

- What does it mean to preserve a Team based on tenant residency (I.e. where the Team resides)?
- What should I do if the site is not hosted by the firm?
- What are preservation "gotchas" I should look for?
- What type of O365 content do we have (i.e., E-mails, Teams Files, Conversations, etc.)?

If the firm is subject to a Legal Hold, some options may include:

- Preserve in Place – Using the e-Discovery Module in the Security and Compliance Center gives firm's the ability to place identified custodians on "hold" to create an in-place preservation strategy.
- Sequester Somewhere Else – Identify custodians with potentially relevant materials, then migrate their files to a location outside of O365 for review and processing.

Ultimately, the policies, procedures and best practices firms put in place should cover all potentially relevant information, no matter the format and wherever located.

REQUEST FOR PRODUCTION OF DOCUMENTS

Whether responding to a subpoena requesting information, attempting to preserve information in connection with anticipated/threatened/pending litigation or preparing for an administrative proceeding, the firm's response plan should be formulated in advance with an eye to the options available in the O365 e-Discovery suite. In the words of Ben Franklin, "[A]n ounce of prevention is worth a pound of cure." In that spirit, prior to implementing O365, define the use strategy and map where data lives so efforts to collect data, regardless the type of request, are managed consistently.

The firm's collections efforts may be overly broad in the absence of a clearly defined O365 discovery strategy or working knowledge of where documents are stored. When data is not well classified and governed, it can cause e-Discovery costs to rapidly increase with large data sets that must be transferred to advanced e-Discovery tools for complex analysis. For example, collection efforts for data could be systematically directed to Exchange, SharePoint, One Drive and Teams, in that order. This is much easier if a matter-centric approach is taken in advance rather than setting up individual sites and managing individual document sets.

But what if you aren't given time to define the strategy prior to implementing O365? Rely on your Agile IG principles, especially focusing on simplicity, to utilize the tools already in place that can help you preserve despite your knowledge gap. Avoid letting the perfect be the enemy of the good by making choices that are simpler to implement, even if they might collect more than the targeted information. Of course, you must do this in concert with the attorney directing the response effort.

DATA GOVERNANCE

There are several Data Governance-related features found in the Compliance Center that address data retention and data disposition. Tools available to you as an IG practitioner vary depending on the O365 license purchased.

The table below describes the various Data Governance features available under the E3 license verses the advanced data governance functionality available through the more robust E5 license.

E-DISCOVERY	E3	E5 / E3 + ADVANCED COMPLIANCE
Retention Policies	√	√
Retention Labels	√	√
Governance Reporting & Analytics	√	√
Event Based Retention		√
File Plan Manger		√
Deposition Review		√
Automatic Data Classification		√
Supervision		√

Like the e-Discovery features, the advanced governance functionality is also available with an E3 license if the firm chooses to purchase "Advanced Compliance," which provides advanced governance for less than the E5 license.

MANAGING DOCUMENTS - DISPOSITION AND RETENTION

Given the rate of adoption by most law firms, it is easy to become overwhelmed by the number of features available for managing data in O365. Stay Agile. Focus first on what is most important to your day-to-day requirements for managing documents coupled with simplicity of implementation. Test various O365 "data governance" features listed below, and be prepared to change your approach as you learn more:

- file plans
- retention policies
- retention labels
- auto-classification and application of labels
- disposition reviews

If you think the previous list is nothing more than repackaged Records Management functionality, you are right. Records Management in O365 helps an organization manage legal obligations, provides the ability to demonstrate regulatory compliance and increases efficiency with regular disposition of items of little value (i.e., expired or no longer possessing of immediate value).

With the Records Management solution in O365, you can incorporate your firm's retention schedule into the file plan to manage storage, identify "Records" and dispose of content at the end of its lifecycle. The Records Management solution in O365 supports the ability to accomplish the following:

- Create a new file plan with file descriptors and expanding hierarchies or integrate an existing retention plan through migration with a file plan manager.
- Establish retention and deletion policies within the Record Label function.
- Define retention and deletion periods based on a variety of factors (e.g., date last modified or created).
- Trigger event-based retention once a condition is satisfied.
- Give end users the ability to label files as "Records" or automatically apply labels to items containing sensitive information (e.g., PII), keywords or content types.
- Deploy "Disposition Review" to confirm files intended for deletion.
- Export a disposition report for further validation and audit trail purposes.
- Set specific permissions for Records Manager functions so the right personnel have the right level of access

Microsoft has taken the most useful functions normally associated with a Records Management tool and incorporated them into the O365 environment. This allows the typical IG practitioner to leverage crucial functionality across the entire platform, touching everything from Exchange, SharePoint, OneDrive and Teams.

Again, it is worth noting that your firm certainly already has Records Management tools designed to manage content outside of O365. You may be tempted to determine how you can use that existing system. Agile IG suggests you work to utilize the tools already integrated into O365, because they are simpler to implement, less burdensome to staff and attorneys and more likely to adapt as O365 features change.

WHERE IS THE DATA?

Let's engage in some deep learning about O365 data. You can't develop an O365 Disposition and Retention Strategy without first understanding where documents are stored and how to manage them where they are. To do this, it is best to break down O365 into its essential elements of Exchange Online and SharePoint Online.

When viewing the platform from a high level, it becomes evident that most everything in O365 lives in either Exchange or SharePoint. Everything your firm is likely to utilize – OneDrive, SharePoint sites, Teams, Planner, Flow and even Yammer – store content in one or both applications. For example:

- **Exchange** – Consists of individual mailboxes, Tasks/To-Dos, Calendar items, Shared mailboxes, Group Mailboxes, Teams conversation threads and Skype chat session content.
- **SharePoint** – Provides document storage for other applications like departmental content, document libraries, folders, etc.
- **OneDrive for Business** – Replaces an employee's home drive and synchronizes local and mobile device content but is really just a dressed-up SharePoint site.
- **Teams** – Leverages SharePoint for file storage, relies upon OneDrive for file linking and storage when content is shared through conversations, links to Group Mailboxes when capturing conversations with external users and finally captures conversation threads in employee mailboxes. Other Teams features like Wikis are nothing more than hidden site libraries (yes, multiple) for wiki text, not to mention documents saved to a wiki end up in the document owner's OneDrive.

Understanding the what, where and how each application within O365 stores, shares and manages data could be a paper within itself… and very well might be in the near future.

KNOWING YOUR RETENTION OPTIONS – RETENTION POLICIES AND LABELS

Let's keep going with some really deep learning by diving into Retention Policies. Retention Policies either protect data from deletion or delete unnecessary items. They are effective because they can be applied across the entire platform – to a whole organization, to a group of employees, a single mailbox or an individual site (how agile is that?) If your firm needs to retain or delete content anywhere in O365, Microsoft recommends the use of a Retention Policy, although you can also use Labels with retention settings. Existing retention features (e.g., Records Center, Content Types[3], MDM tagging for email, etc.) will continue to work side-by-side with Retention Policies (and Labels) created in the Security & Compliance Center.

- A Retention Policy is applied manually at the site level. When a SharePoint site or OneDrive account is subject to a Retention Policy, a Preservation Hold library is also created. End users do not see the Preservation Hold from their interface because it is only visible to site collection administrators.
- Labels can be used to apply retention requirements and allow employees to manually apply existing Labels to content in Outlook on the web, Outlook 2010 and later, OneDrive, SharePoint and O365 groups. Other functions unique to Labels include alerting administrators to review upon expiration of a retention period, triggering the count-down of a retention period from the occurrence of a specific event (instead of the more standard creation date of the content) and leveraging metadata to activate a retention period.

When combining the two functions together, the Label linked to a specific Retention Policy can be used to:

- classify data across the organization for governance and enforce retention rules based on that classification
- mark content as a "Record", preventing end users from changing or removing the Label or even editing or deleting the content itself, and
- categorize content automatically if it meets specific criteria (with an Enterprise E5 subscription)

As an Agile IG ninja, these tools offer flexibility for you and simplicity for those in your firm using O365.

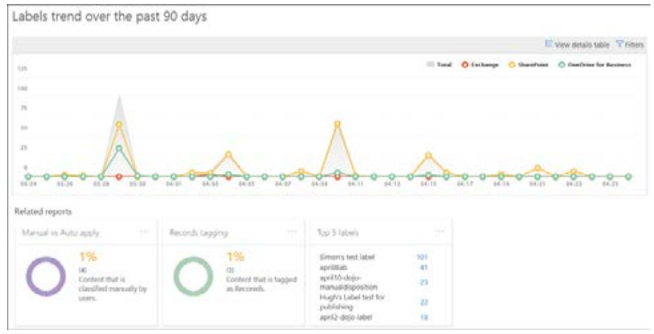
MANAGING LABELS

After you create your labels, you'll want to verify that they are being applied to content as you intended. With the data governance reports in the O365 Security & Compliance Center, allow you to easily review, reflect and improve on your content labeling approach. With these reports, you can quickly view:

- Top 5 labels: shows the count of the top 5 labels that have been applied to content. Click this report to view a list of all labels that have been recently applied to content. You can see each label's count, location, how it was applied, its retention actions, whether it is a record and its disposition type.
- Manual vs Auto apply: shows the count and percentage of all content that's been labeled manually or automatically.
- Records tagging: shows the count and percentage of all content that's been tagged as a record or non-record.
- Labels trend over the past 90 days: shows the count and location of all labels that have been applied in the last 90 days.

All these reports show labeled content from Exchange, SharePoint and OneDrive for Business.

You can find these reports in the Security & Compliance Center › Data Governance › Dashboard.



SOURCE: https://docs.microsoft.com/en-us/microsoft-365/compliance/view-the-data-governance-reports

MANAGE IN-PLACE

One option for records retention in O365 is to manage data in-place for the lifecycle of a matter. Law firms have traditionally directed users to their document management system as the most prominent, long-term storage repository. Traditional DMS usage challenges the Agile IG principles in two ways. First, living where your customer lives, since it is often impractical to move O365 data to the DMS. And second, focusing on simplicity, since O365 data can be managed in place using the same matter-centric strategy for client data in O365 as in the DMS.

RETENTION STRATEGY CONSIDERATIONS

When designing your disposition and retention strategy, a great way to fall victim to one of the "gotchas" mentioned above is failing to understand how each application in O365 stores content and the options for managing the content where it lives. Let's use the most rapidly adopted feature in O365 as an example: Teams.

Consider the impact of the use of a group mailbox, conversations threads in a channel and the ability to leverage an individual team member's OneDrive. If a user adds a document in a thread or shares a document, that document may be linked to that person and their individual OneDrive account and may not be accessible for discovery preservation. Governance professionals should plan for how this affects site collection and preservation within all collaborative groups

MATTER MOBILITY: REQUEST TO TRANSFER DOCUMENTS IN/OUT OF O365

When addressing matter mobility needs, such as transferring Teams client data outside the firm, don't panic. The fact that there are chats, channels and documents in Teams can be tricky. And, behind the scenes, all pieces within a Team "site" actually reside in both OneDrive and SharePoint.

We can find our way forward in this new world. O365 has several tools within the Security & Compliance Center to collect, review, and export information in support of existing firm policies on exports. Experiment with them and use your iterate and fail fast approach. Learn. Be Agile.

Determine the best tool or tools to review, copy and transfer the Team data identified for transfer. Each aspect may need to rely upon multiple tools. But as you reflect, learn and improve after each transfer, the process becomes more streamlined. Taking a deep dive into the tools available within Security & Compliance, like Data Governance and e-Discovery, pays off in the end.

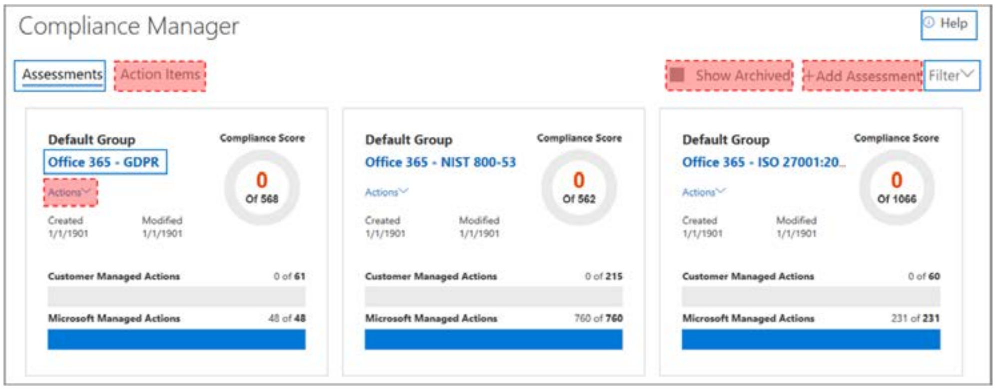
REGULATORY AND COMPLIANCE

MANAGING REGULATORY COMPLIANCE

Compliance Manager, a workflow-based risk assessment tool in the Microsoft Service Trust Portal, enables you to track, assign and verify your firm's regulatory compliance activities related to Microsoft Professional Services and Microsoft cloud services, such as Microsoft O365. It is available in all license models and can be customized to meet the needs of your firm.

Compliance Manager provides you with a dashboard view of standards, regulations and assessments that contain Microsoft's control implementation details, test results and customer control implementation guidance. It allows your organization to perform tracking, providing you a common framework to work with your security and IT teams when responding to client requests and performing internal compliance audits.

Compliance Manager provides certification assessment control definitions, guidance on implementation and testing of controls, risk-weighted scoring of controls, role-based access management and an in-place control action assignment workflow to track control implementation, testing status and evidence management.



SOURCE: https://docs.microsoft.com/en-us/microsoft-365/compliance/meet-data-protection-and-regulatory-reqs-using-microsoft-cloud

Compliance Manger combines the detailed information provided by Microsoft to auditors and regulators as part of various third-party audits of Microsoft 's cloud services against various standards (for example, ISO 27001, ISO 27018, and NIST) and information that Microsoft compiles internally for its compliance with regulations (such as HIPAA and the EU General Data Protection Regulation, or GDPR) with your own self-assessment of your organization's compliance with these standards and regulations.

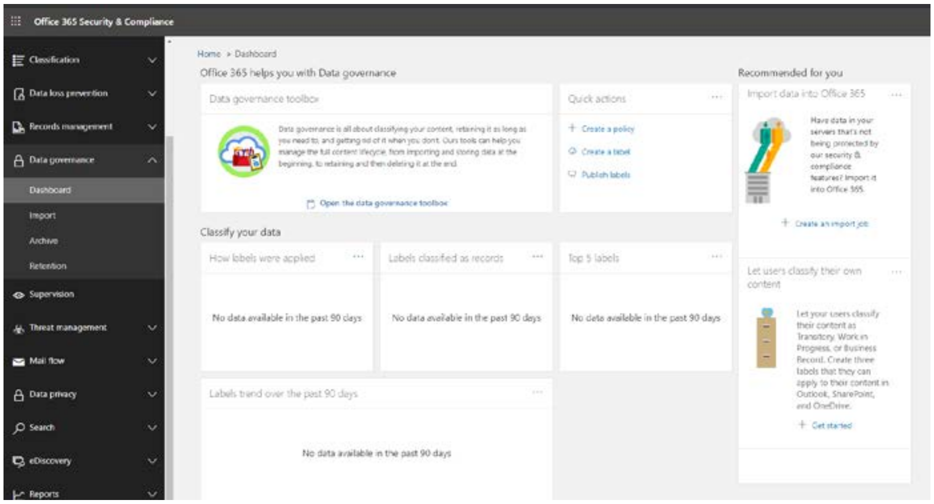
AUDIT & REPORT

O365 provides an excellent way to audit usage. You can use the View Reports page in the Security & Compliance Center to quickly access audit and usage reports for your SharePoint Online and Exchange Online organizations. Note of caution: Microsoft audit reporting scores against tools and controls within the Microsoft stack. So, for example, if you use a Mobile Device Management (MDM) tool such as MobileIron rather than Microsoft's InTune, your score will reflect a gap in the MDM space that you will need to notate or explain.

DATA LOSS PREVENTION REPORTS

Data loss prevention (DLP) reports contain information about the DLP policies and rules that have been applied to content contain sensitive data in your O365 organization. You can also configure the report to display information about DLP actions that were based on your DLP policy and rules. For more information, see view the report for data loss prevention.

You now have, possibly an overwhelming, sense of the large number of O365 tools and the many ways they can be combined to address the IG needs of your firm. Next, let's focus some attention on other governance issues you should consider.



OFFICE 365 AND CORE GOVERNANCE ITEMS

PROVISIONING

There are several features that users can enjoy while using O365 and Teams. Determining the features you want to provide in the context of your particular regulatory and control environment should drive many of the decisions you need to make regarding how to control O365. Be agile and live where your customer lives to understand how they will use the tools. In addition to the questions listed in the Agile IG section of the paper, ask:

- What is the intended purpose of the functions you wish to enable in O365? OneDrive provides basic file storage and exchange. SharePoint Online can provide a more feature-rich file storage and exchange, as well as other capabilities. Teams brings chat, conferencing, collaboration, apps, and SharePoint Online and OneDrive into one interface.
- Who are the intended participants in these functions?
  - Are there some functions you want to make available to the entire firm, such as Teams for internal chat and conferencing (replacing Skype)?
  - Do you want to have Teams deployed for departments, or practice groups or client engagement teams?
  - Do you want to have a Team for each client, and do you want to provide a Team for every client and/or matter automatically or just for those that warrant it, perhaps based upon request of the client or because of the nature of the matter?
  - Do you require approval of the General Counsel or the client's General Counsel or review of the client's outside counsel agreements prior to implementation?

Once you have determined the intended functions, remember our 'iterate rapidly and fail fast' approach. Determine the appropriate controls that support your desired level of security and IG for each function. Do you want people to be able to access the environment outside of the firm network? If so, will you utilize multi-factor authentication (MFA)? If your established IG controls dictate MFA for external access, O365 should not cause you to stray from there. What Conditional Access Policies[4] will you put in place? Will you allow remote users or guests to download materials or just access materials within the O365 experience? Will you apply Rights Management to documents, either in O365 or upon download, and if so, how will you deal with the DMS impacts for the Guest and internal to the firm?

Office 365 allows for the distribution of privilege to setup certain resources (e.g. you could allow Marketing to setup Teams or a practice group team to create their own Teams space). Focus on simplicity, combining the perspective of your customer and managing your IG needs. Depending on the complexity of your configuration, you may consider controlling the deployment process centrally to ensure that all approved access, security, and control is implemented as planned. As you experiment with different IG controls, fully involve your security professional. As an Agile IG practitioner, you want to provide your customer as much flexibility as they need to make the tool useful while keeping the firm's risk low. Because security control configuration is vital to protect client information, firms may want to consider, for example, having the IT group create Teams, while the security team reviews Teams for security hardening compliance, prior to deployment.

ACCESS CONTROLS, INCLUDING ETHICAL WALLS

The administration of Teams can be delegated to users, relieving the burden on IT. However, factor in the need to ensure that access to the Team needs to respect firm ethical walls/screens. Firms may want to consider administering Teams through IT where appropriate authorizations and eligibility checks can be performed. Wall-builder automation may be available for applying screens in Teams, so check with your vendor. Or, consider the simplicity of using Information Barriers [5] , an ethical wall tool built into O365.

INTERNAL VS EXTERNAL SHARING

One of the great capabilities of Teams is information sharing. This can be sharing among your internal teams (not to be confused with the big 'T', Teams application), or with guest Teams' members. For a law firm, this implies co-counsel or clients outside of the firm. While law firms often collaborate and share information with parties outside of their firm, there are common controls and restrictions on this sharing that should be considered when deciding how your firm is going to use Teams.

WHERE SHOULD THE RECORD LIVE?

Traditionally, firms use a document management system (DMS) as the repository that represents the file of record. If lawyers put content in Teams, and are potentially collaborating with others in the firm and with the client, where should this content live? One option could be to have the user manually move content to the DMS in order to maintain the integrity of the client representation file. But this additional step may not happen and may break the very features that made Teams useful in the first place. Another option, one that focuses on simplicity, is to allow the content to live in Teams and use Teams as an additional repository of record. We discussed this idea in more depth earlier in the paper.

For those that long to avoid the multiple repositories of record dilemma, there is reason to believe that at least some DMS vendors are working on more elegant ways to achieve integration. Talk to your vendor (and maybe their competition) to determine where in your Agile focus they may provide additional tools for you to consider.

MAINTAINING A RECORD OF COMMUNICATIONS WITH CLIENTS

Today you retain records of communication with clients via email. If you need to perform discovery of client interactions related to litigation, you search email and capture all of that. If clients are picking up documents containing substantive legal advice via Teams, you need to consider how to reproduce that interaction if needed in the future. Additionally, think about:

- Controlling the distribution of metadata.
    - Law firms are often concerned that metadata, such as edit marks, may make their way to the client and therefore use metadata scrubbing tools to clean attachments. If clients are access documents via Teams, metadata could be a

concern. For example, documents edited using Word online in Teams won't display track changes that may exist in the document and are visible if the same document is edited with the desktop version of Word

- Maintaining copies of substantive drafts (i.e., versioning).
  - Teams can be configured to save versions of documents edited in Teams files. This functionality saves each editing session as a new draft. There is not a way to designate a particular editing session as substantive and a new version, so there may be more versions saved than are necessary. How to manage these versions requires consideration and perhaps some experimentation.

Another great feature of Teams is the ability to apply, in an automated fashion, advanced rights management to documents. This feature allows a document to be encrypted and an access control list applied that limits who can access the content. Other features include the ability to restrict printing, cut and paste and access past an expiration date. These controls allow you to share a document with, for example, opposing counsel and set rights to it so they cannot extract the content or access the document after a designated period. Before making the decision to utilize rights management, consider the impact this has on the usefulness of documents outside of Teams. If you apply rights management to a document in Teams, that same document won't be indexed and users won't be able to find it if you place a copy in your DMS. This presents challenges to ongoing work for the client as well as spoliation of preservation if you can't produce that document down the road. Clients who download documents with rights management from Teams may have similar challenges on their side. Rights management can be removed from a document so that the document can be useful in the DMS, but that is a manual process. Firms should consider if they are willing to accept the risk of a user not removing rights management and documents being lost in the DMS. If rights management is a useful control, that is another reason to manage content in Teams using native O365 tools instead of using your records system or your DMS.

BLIND SUBPOENAS

A key component to making the jump to any cloud provider involves your comfort level with outsiders having some level of control over your data. How that data is stored, secured, encrypted, retained and disposed of are some of the more prominent discussions for an organization. However, one slightly less prevalent point is how your data can be subpoenaed and even more complex is how you'll manage expectations and outcomes of cloud providers giving your data to those issuing silent or blind subpoenas.

In 2011, ZDNet explored this issue with Microsoft (https://www.zdnet.com/article/usa-patriot-act-and-the-controversy-of-canada/). Microsoft stated that, in a limited number of circumstances, they may disclose data without your prior consent. Microsoft indicated that they first try to redirect the requestor to the owner of the data. They also notify you when legally allowed to do so. However, there are circumstances where cloud providers are legally restricted from notifying you of their release of your data. This is difficult enough to swallow when it is your firm's data. Now consider the idea of Microsoft or any cloud provider, releasing your client's data, not only without your consent or knowledge, but likely not narrowed in scope with the same level of scrutiny you would have applied. And what happens with a subpoena related to one client that ends up including data of other clients?

Layer on top of these concerns the complexities of:

- The Patriot Act, which requires data outside the US to be able to be requested by the US (from US-owned entity), if the investigation involves suspected terrorist activities. This brings in the concerns of both citizen right's infringement as well as impact on foreign nationals by relinquishing data without requesting a court order.
- The CLOUD Act (March 2018) which states that US providers must supply US info stored outside the country.

For organizations with locations outside the US, these acts add numerous cross-border data complexities. But, does this really happen often enough to impact your decisions to move to the cloud? Well, it seems that we only have part of the picture to help answer that question. Microsoft, for example, is quite public about their disclosure governance https://blogs.microsoft.com/datalaw/our-practices/. They are also publishing twice a year the number of requests they receive and some key disclosure stats: https://www.microsoft.com/en-us/corporate-responsibility/lerr & https://www.microsoft.com/en-us/corporate-responsibility/fisa. So this should help your decision, except, Microsoft only discloses the stats related to standard subpoenas. They do not share information, not even aggregated stats, related to the frequency with which they have provided data for blind subpoenas. So it leaves room for concern as to how often this occurs. A recent NY Time article attempts to shed a bit more light on the topic: https://www.nytimes.com/2019/09/20/us/data-privacy-fbi.html

But there must be some protections we can reply upon? In June of 2019, Law.com highlighted guidance from the US Attorney Manual and how subpoenas for law firms can impact attorney/client privilege. https://www.law.com/americanlawyer/2019/06/28/can-cloud-providers-calm-the-legal-industrys-apprehensions/?slreturn=20190802150107. "When determining whether to issue a subpoena to an attorney for information relating to the attorney's representation of a client, department personnel must strike a balance between an individual's right to the effective assistance of counsel and the public's interest in the fair administration of justice and effective law enforcement." How much murkier does this get when data is being requested via a cloud provider vs directly from the law firm?

And finally, firms need to consider what they agree(d) to in outside counsel guidelines. Some clients require firms to either refrain from using cloud storage for their data or may require the firm to get express consent before doing so. This is not very practical or feasible, as firms often don't have the time or resources to manage multiple exceptions from various clients.

Microsoft (and other tech giants) continue to fight the issue in court to help alleviate privacy concerns that both they and their clients have on this topic: https://www.law360.com/cybersecurity-privacy/articles/1203043/microsoft-fighting-gov-t-secrecy-order-for-user-data So we'll need to watch this space for continued updates and outcomes. Ultimately, in sorting through these complex issues, each firm needs to assess the types of clients they represent as well as the types of data they store and have some detailed discussions on where their risk tolerance lies in this space. These discussions should not be isolated to the IT team; General Counsel and/or lawyers with expertise in this space should be brought in to collaborate and help make these decisions.

ENCRYPTION KEY MANAGEMENT

Like the rest of O365, understanding encryption key management depends on what applications you are going to use and your firm's risk tolerance. There is, however, one definitive fact that you need to know from the onset. Choosing to manage your own encryption keys DOES NOT prevent Microsoft from accessing the keys, nor does it mean that this approach can be used to maneuver around the subpoena issue. Microsoft clearly states "Customer Key (tool to help BYOK see below) was not designed to respond to law enforcement subpoenas. It was designed for regulated customers to meet their internal or external compliance obligations" https://docs.microsoft.com/en-us/office365/securitycompliance/service-encryption-with-customer-key-faq

How does Microsoft comfort customers that they are not looking at customer data? There is a feature called Customer Lock Box, which is a policy feature whereby Microsoft employees are not allowed to access the Key Vault without gaining customer permission first. This is a prohibition by policy and not a prevention by technology. To bolster this control, customers can review the access logs on the Key Vault, establishing a detective control to close the loop on the risk of Microsoft accessing the Key Vault.

O365 provides several options for the use of encryption and the management of encryption keys. You will need to determine how much encryption key protection your organization requires.

Out of the box, O365 encrypts data at rest, and O365 encrypts and decrypts with keys that they manage. If that is enough to satisfy your organization's risk posture, then you can rely on Microsoft.

O365 also allows for a customer to provide their own key that is created and managed by the customer. This key will still need to be put into the Key Vault so that Microsoft can use it to apply to the appropriate encryption routines, however the customer owns the key and can revoke the key if needed, ensuring that Microsoft no longer has access to their data. This process involves establishing a Key Vault server in Azure, which has a setup and ongoing operational expense associated with it. It also requires the customer to have their own Hardware Security Module (HSM), actually two, including DR, for creating and protecting the keys appropriately. After all this expense, Microsoft still can access your keys in the Key Store, so the benefit is solely that when you leave, you can ensure your clients that Microsoft no longer has access to the data.

CONCLUSION

This paper certainly didn't provide all the answers to IG within O365, but we hope it presented an approach and basic information to allow your organization to meet O365 challenges head-on. Utilizing the knowledge you gain from deep learning, and with the thoughtful application of Agile IG, O365 could be the collaborative platform we've all been striving for—and may even get your lawyers cheering "IG for everyone!"

ENDNOTES

1This is a better sounding misquote of an article from 1946 where Einstein said "a new type of thinking is essential if mankind is to survive and move toward higher levels."

2For those software developers reading this, we realize it is a massive oversimplification of Agile techniques, but our goal is to lay out a new process for IG professionals, not examine Agile programming techniques. If you are interested in more about Agile, we recommend The Lean Startup by Eric Ries, for a great macro view of how Agile can work and Extreme Programming Explained by Kent Beck and Cynthia Andres for details on an Agile software development methodology.

3Want to know more - https://support.office.com/en-us/article/create-a-records-center-6bf1488b-62a8-486c-90dd-54b6bcce4b3a

4To learn more, try https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

5https://docs.microsoft.com/en-us/microsoftteams/information-barriers-in-teams

WE PROTECT WHAT YOU VALUE MOST®

800.899.IRON | IRONMOUNTAIN.COM

ABOUT IRON MOUNTAIN

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

USLGL-RPT-101619A