Retention & Disposition
In a Cloud Environment

Final Report
prepared for:
InterPARES Trust
by the members of the
R&D in a Cloud Environment
Project Committee
May 17, 2016

This research project was conducted under the research agenda of InterPARES Trust (ITrust 2013-2018), a multi-national, interdisciplinary research project exploring issues concerning digital records and data entrusted to the Internet. Its goal is to generate theoretical and methodological frameworks to develop local, national and international policies, procedures, regulations, standards and legislation, in order to ensure public trust grounded on evidence of good governance, a strong digital economy, and a persistent digital memory.

InterPARES Trust, directed by Dr. Luciana Duranti, is based at the Centre for the International Study of Contemporary Records and Archives of the School of Library, Archival and Information Studies at the University of British Columbia, in Vancouver, British Columbia, Canada. Major funding for The InterPARES Trust Project is provided by a Social Sciences and Humanities Research Council of Canada Partnership Grant.

Sixteen individuals were members of this team since the inception of the project:

Lead Researcher: Dr. Patricia C. Franks

Project Researchers:

Alan Doyle	Linda Nobrega
Jane Morrison	Lara Wilson

Graduate Research Assistants:

Fall 2013	Mark Driscoll (SJSU), Katie Ferrante (UBC)
Spring 2014	Mark Driscoll (SJSU), Karla Harriott (SJSU), Anousheh Shabani (UBC)
Fall 2014	Ryan Banks (SJSU), Anousheh Shabani (UBC)
Spring 2015	Ryan Banks (SJSU), Vicki Casteel (SJSU), Kelsey Poloney (UBC), Alison Weck (UBC)
Fall 2015	Hoan-Vu Do (SJSU, Kelsey Poloney (UBC), Alison Weck (UBC)
Spring 2016	Tara Haghighi (SJSU), Kelsey Poloney (UBC), Connie Redic (SJSU)

Table of Contents

Retention and Disposition in A Cloud Environment

1. Introduction

Effective Information Governance is increasingly recognized as an imperative for corporate compliance and risk mitigation. Defensible records retention and disposition programs cut costs for discovery and storage, reduce risk, and increase compliance. Ninety-five percent of the 1,060 IT professionals responding to a 2016 survey indicated their organizations employ cloud services, with 71% using hybrid cloud environments (RightScale, 2016). Although a greater portion of the organization's records are in the "possession" or "custody" of a cloud service provider, the organization maintains ultimate responsibility to preserve and produce those records for as long as necessary. It is, therefore, essential that organizations can "trust" that records residing in the cloud can be retained and disposed of in accordance with the same requirements that govern the retention and disposition of records stored within the enterprise.

2. Purpose and Scope

This study was designed to contribute to a better understanding of the difficulties encountered when managing records in a cloud environment by answering two questions:

- How does the use of cloud services affect an organization's ability to retain and dispose of records in accordance with the law and other guidelines?
- What can be done to mitigate the risks that arise from the gaps between the ability to apply retention and disposition actions to records residing within the enterprise and those residing in the cloud?

Answers to these questions can be used to to develop a deeper understanding of the risks associated with retention and disposition in the cloud environment and to design a framework for best practices in choosing cloud service providers based on records management functionalities present in cloud solutions. This study identifies requirements for service providers and systems that store records in the cloud that, if present, would engender trust in the client organization that the records can be retained and disposed of in accordance with the same requirements that govern the retention and disposition of records stored within the organization. It also provides guidance for identifying records retention and disposition functionalities in cloud-based systems and services under review and suggestions on how to mitigate risks posed by gaps between what is provided and what is required.

3. Methodology

This study addressed two main topics: the functional requirements needed for retention and disposition in the cloud (along with users' knowledge of cloud usage), and the functions existing in services provided by a limited number of cloud vendors. This research was conducted using a twofold approach. First, information was collected on a selection of major cloud services, and second, users of cloud products and services belonging to a records and information management professional association were surveyed.

The literature review was completed during the first phase in order to identify the necessary functional requirements for retention and disposition in the cloud. The standards and guidelines examined include:

- ISO 15489, parts 1 and 2: *Records management*
- ISO 23081, parts 1, 2, and 3: *Metadata for Records management*
- ISO 16175, parts 1, 2, and 3: *Electronic office environments*
- DoD 5015.2: *Records Management Applications Design Criteria*
- MoReq 2010: *Modular Requirements for Records Systems*
- ARMA International's *The Generally Accepted Recordkeeping Principles*

Using the functional requirements extracted, a checklist was created to examine the level of records retention and disposition capabilities included in various cloud services (see Appendix A).

A list of specific major cloud offerings was compiled through the literature review. The user checklist served as a guide to investigate the capabilities of those cloud providers. Information was gathered through a combination of publicly available product information, white papers, and interviews with company representatives. The resultant vendor profiles compare the functionalities provided against those needed to comply with records management standards and guidelines.

During the second phase of the study, information was gathered from a user perspective. This was accomplished through a questionnaire on cloud use distribute to ARMA International members. A complete executive summary of the survey results, which included a discussion of each question, was published in 2015. The answers revealed the level of involvement of Records and Information Management professionals in cloud decisions made by their organizations, their understanding of retention and disposition functionalities in the cloud services used, and the types of cloud services that were being used by their organizations. The Executive Summary (InterPARES Trust, 2015) can be downloaded from the InterPARES Trust website.

4. Terminology

The InterPARES Trust Terminology Database (http://arstweb.clayton.edu/interlex/) is the source of definitions of terms used in this research project.

5. Literature Review

A review of the literature revealed five themes central to discussions of retention and disposition in the cloud. These include: risk analysis and risk management, legal regimes and standards, information governance, emerging approaches to retention and disposition, and trust. An in-depth literature review for this study was previously released through InterPARES trust in July 2014, and a second version was released in June 2015.

In the area of risk analysis and management, the literature emphasized the need for organizations to fully understand all possible risk factors and then manage those factors in the cloud environment. Legal and eDiscovery risks are discussed in articles by A. Dutta et al (2013) and A. Grounds et al (2013), both of whom emphasize that any cloud system must be compliant with legal needs. Practical security risks are cited by J. Gold (2012), including the problems associated with contractual agreements with vendors.

Legal standards were a significant part of this study's focus, and the existing literature includes a discussion of the legal environment as related to cloud computing. Changes to legal systems are recommended by E. Goh (2014) in order to better protect information in the cloud. Other sources suggest possible legal solutions for addressing cloud systems through legislation or regulations. The literature in this area reveals that many information professionals have identified a need for change in legal standards pertaining to the cloud.

Discussions of information governance related to this study are concerned with retention and disposition practices that comply with ISO 15489 and the involvement of cloud providers in educating users on information governance needs. Cloud vendors are encouraged to become involved in the records programs of an organization by providing consulting services rather than acting merely as a third-party system provider.

The emergence of new approaches to enforcing retention and disposition in the cloud were discussed more often by IT professionals than by Records and Information Managers. This literature focused mainly on retention and disposition functionality available in various cloud offerings and the adoption of new technological developments in cloud storage.

Trust is an important area to consider for cloud systems, as they are a relatively new technology. The literature shows a tension between the perceived benefit of cloud services and the potential security or legal risks. While a number of articles recount positive experiences with cloud storage, others show some skepticism about the cloud and lack trust in its reliability. Publications by S. Pearson (2011) and Burda and Teutenerg (2014) specifically discuss how better accountability from cloud providers can build trust for consumers, and the best way to improve trust is to make the risks of cloud use obvious to users.

Both versions of the completed literature review can be downloaded from the InterPARES Trust website (https://interparestrust.org/).

6. Findings

6.1 Phase 1: Cloud Services

6.1.1 Aggregated Responses to Cloud Service Questionnaire

The questionnaire included in Appendix A is comprised of 25 items grouped into seven categories: privacy and security considerations, establishing disposition authorities, applying disposition authorities, executing disposition authorities, documenting disposal actions, reviewing disposition, and integration.

One questionnaire was completed for each of the cloud services under review (see Table 1) by gathering information from websites, published white papers, and vendor presentations, as well as interviews with company representatives when possible.

Table 1: Cloud Services Explored as Part of the Study

Amazon Web Services http://aws.amazon.com/	Microsoft One Drive for Business https://onedrive.live.com/about/en-us/
Archivematica https://ww.archivematica.org/en/	MS SP Add-on Gimmal http://www.gimmal.com/
ArchiveSocial http://archivesocial.com/	MS SP Add-on Collabware http://www.collabware.com/
CenturyLink Cloud/Tier 3 http://www.centurylink.com/business/cloud/	NextPoint http://www.nextpoint.com/
Cloud 9 Discovery http://www.cloudninediscovery.com/	Office 365 https://products.office.com/en-us/business/office-365-business
Crashplan http://www.code42.com/products/crashplan/	Preservica http://preservica.com/
Dropbox for Business https://www.dropbox.com/	Rackspace http://www.rackspace.com/
Egnyte https://www-avl.egnyte.com/	SharePoint Online https://products.office.com/en-us/SharePoint/collaboration
GoGrid (a DATAPIPE Company) https://www.datapipe.com/gogrid/	Smarsh http://www.smarsh.com/
Google Apps for Business/include Google Vault https://www.google.com/work/apps/business/	Symantec Enterprise Vault http://www.symantec.com/enterprise-vault-cloud/
HP Digital Safe http://www8.hp.com/us/en/software-solutions/digital-safe-cloud-archiving/	

During the course of the investigation, some cloud providers added new services (e.g., Amazon Web Services added Glacier for low-cost data archiving and backup) while others partnered with other vendors to create new offerings (e.g., Archivematica partnered with DuraCloud to launch a cloud-based, long-term, digital preservation service called *ArchivesDirect)*.

A profile of *ArchivesDirect* was added to this study after the final report was in draft form; however, statistics in this section were not updated to reflect the addition. The answers to the questions regarding ArchivesDirect were included in the gap analysis (see Appendix B).

While it is difficult to categorize cloud services with complete certainty due to acquisitions and expansion of offerings, the cloud services reviewed fell into several broad categorizes as shown in Table 2.

Table 2: Cloud services under review.

File Sharing and Cloud Storage	Records Management Extender	Infrastructure/Platform/ Managed Services	Litigation Support & eDiscovery
Dropbox Egnyte One Drive for Business	Collabware Gimmal	Amazon Web Services Century Link (Tier 3) GoGrid/DATAPIPE Rackspace	Cloud Nine Next Point
Archiving Solution	**Enterprise Content Management**	**Long-term Digital Preservation**	**Backup & Data Protection**
ArchiveSocial Google Vault (Email & chats) Smarsh Symantec Enterprise Vault	Office 365 and SharePoint Online	Archivematica Preservica ArchivesDirect (profile added late, not included in statistics)	CrashPlan HP Digital Safe

Questions 1-5 relate to vendor services: More cloud vendors provide encryption for content while in transit (75%) than for content residing in the cloud (55%). Approximately 50% allow independent audits of systems. Only 40% store content on physical servers located within a jurisdiction approved for the client, and still fewer, 35%, store backup copies on servers located within an approved jurisdiction.

Questions 6-8 relate to establishing disposition authorities. The cloud services explored did not refer to *disposition authorities*, as archival and records management terms are not often used by cloud vendors. However, 70% allow retention periods to be applied to content, and indexing capability is present in 60% of the systems. Destruction can be automated in 45% of the services.

Questions 9-13 relate to applying disposition authorities and locking down records for view only. One half of the cloud services reviewed allow records that are not in an aggregation (individual records) to be destroyed (50%); forty percent allow records not in an aggregation to be (40%) at a future date. Less than half (45%) allow a disposition authority (retention and disposition specifications) to be applied to aggregations of records.

Questions 14-17 relate to executing disposition authorities. A large majority, 75%, allow records to be deleted according to a retention/disposition schedule, but only 60% allow backups to be deleted according to the retention and disposition schedule. Multiple retention requirements can be tracked in 30% of the cloud systems to allow the manual or automatic lock or freeze on the disposition process when more than one disposal authority is associated with an aggregation of records, but only 10% of the services alert users to conflicts related to links from records to be deleted to other records aggregations with different retention requirements.

Questions 18-19 relate to documenting disposal actions. The same percentage of cloud services 60%, document disposal actions in process metadata as automatically record disposal actions and report them to the administrator. However, in some cases, the metadata exported is descriptive and does not include operational metadata added while in the custody of the cloud provider.

Questions 20-24 relate to reviewing disposition. More than half, 65%, provide system generated reports on the disposition process, and 40% provide the ability to interface with a workflow facility to support scheduling, review, and export transfer processes. Fewer services provide additional disposition review functionality: 30% allow records to be marked for destruction, 25% store all decisions made during the review in metadata; and 20% present electronic aggregations, their metadata, and disposal authority for review.

Question 25 is related to integration**.** Only 35% of the services indicated they use a metadata scheme compatible with other systems, such as Enterprise Content Management Systems or Records Management Systems. In some instances, third party providers develop connectors that allow integration of cloud services with other products. For example, Preservica includes multiple connectors to allow content to be ingested from ContentDM, DSpace, Outlook, Lotus Notes, and SharePoint.

6.1.2 Cloud Services

Information on the type of service model was gleaned from vendor information found online and directly from some of the vendors who made themselves available to discuss our initial findings for their checklist. For our assessment purposes, the vendors we reviewed were subsequently grouped into the following categories related to their primary functional service:

- Archiving Solution: ArchiveSocial, Google Vault (email and chat), Smarsh, and Symantec Enterprise Vault.
- Backup and Data Protection: Crash Plan and HP Autonomy Cloud Services
- Enterprise Content Management: Office 365/SharePoint Online.
- File Sharing and Storage: Dropbox for Business, Egnyte, and One Drive for Business.
- Infrastructure/Platform/Managed Services: Amazon Web Services, Century Link (Tier 3), DataPipe (GoGrid), and Rackspace.
- Litigation Support and eDiscovery: Cloud Nine and NextPoint
- Long-term Digital Preservation: Archivematica, ArchivesDirect (late add), and Preservica.
- Records Management Extender: Collabware and Gimmal.

The ability to gather information from vendors was mixed. Of the vendors who were actively engaged in our data gathering, some completed our checklist in detail and gave us extra information as well. Of the vendor information that was gathered from online or other available resources, the information reviewed did not provide the level of granularity that we sought through our checklist tool. Vendors completed or verified completed questionnaires for 7 of the 20 cloud services in the GAP analysis in Appendix B (7 or the 21 cloud services profiled): Archivematica, ArchivesDirect, ArchiveSocial, Collabware, Gimmal, Preservica, and Smarsh.

6.1.3 Cloud Service Profiles

The checklist categories consisted of the following:

- Privacy & security considerations
- Establishing & applying disposition authorities
- Executing disposition authorities
- Documenting disposal actions
- Reviewing disposition
- Integration with other systems

The primary weaknesses revealed by vendor responses were in the executing, documenting, and reviewing disposition sections—retention and disposition functionalities. Profiles of the 20 original and 1 additional cloud service (ArchivesDirect) are included in this section. Each profile is listed on a separate page. They are included in alphabetical order of category of service and not cloud service name. For example, ArchiveSocial, Google Vault (email and chat), Smarsh, and Symantec Enterprise Vault are listed first under the category of Archiving Solution followed by CrashPlan and HP Digital Safe services listed under the category of Backup and Data Protection.

ArchiveSocial (Archiving Solution) – Verified

Introduction:
ArchiveSocial is a social media archiving solution for records management, regulatory compliance, and eDiscovery. ArchiveSocial captures and preserves records from social networks including Facebook, Twitter, LinkedIn, and YouTube.

R&D Functionality Present	R&D Functionality Lacking/Unverified
Privacy and Security Consideration: (Questions 2-5) Content is encrypted when in transit and at rest in the cloud, and the physical and backup servers are located within a jurisdiction.	**Privacy and Security Consideration:** (Question 1) Unsure if vendor allow independent audits of systems and processes as audits are carried out through Amazon
Establishing Disposition Authorities: (Question 1) Indexing capability is supported; they use custom tagging. Retention periods are applied.	**Establishing Disposition Authorities:** (Question 8) Destruction can't be automated (automatic notification for destruction, but not destruction itself)
Applying Disposition Authorities: (Questions 9-13) Disposition authority can be applied to aggregations of records. Records can be locked down for viewing only, be retained indefinitely, and not in an aggregation can be transferred or destroyed at a future date.	**Executing Disposition Authorities:** (Question 15) Backups can't be deleted according to the retention/disposition schedule
Executing Disposition Authorities: (Questions 14, 16-17) Records can be deleted according to retention and disposition schedule and users are alerted to conflicts related to links from records to be deleted to other records aggregations that have different records disposition requirements (only for native conversations). Multiple retention requirements can be tracked to allow the manual/ automatic lock or freeze on the process.	**Reviewing Disposition:** (Question 24) There isn't an interface with workflow facility to support scheduling, review, and export transfer processes either provided nor supported
Documenting Disposal Actions: (Questions 18-19) Disposal actions are documented in process metadata and can be automatically recorded and reported to the administrator.	**Integration:** (Question 25). Unsure if metadata scheme is compatible with other systems such as ECM or RMS (content can be exported to HTML or Excel formats; retention periods not transferrable to other systems)
Reviewing Disposition: (Question 20-23) Electronic aggregations are presented for review along with their records management metadata and disposal authority information so both content and records management metadata can be reviewed. Records can be marked for destruction, transfer, further review and all decisions are made during review stored in metadata (use of tagging indicates decisions made). The system can generate reports on the disposition process	

Assessment:
ArchiveSocial provides some level of records management functionalities through their services. The system "communicates directly with each social network to capture complete records in their raw, native format with complete metadata" (http://archivesocial.com/our-approach-social-media-archiving). They fulfill most of their privacy and security needs with the exception of allowing independent audits of systems and process. They also fulfill most of the requirements for establishing, applying, and executing disposition authorities. In addition, ArchiveSocial allows for the review and documentation of disposition actions.

Google Vault (Archiving Solution)

Introduction:
Google Vault is an add-on for Google Apps to allow users to retain, archive, search, and export their organization's email and chat messages for eDiscovery and compliance needs. You can also search and export files stored in Google Drive. Vault is entirely web-based, so there is no need to install or maintain any software. It provides the following eDiscovery services: Email and chat archiving, legal holds, drive file search, email and chat search, export, and audio reports.

R&D Functionality present	R&D Functionality lacking/unverified
Privacy and Security Considerations: (Questions 1-3) Vendor allows independent audits of systems and processes. Content is encrypted when in transit and when at rest in the cloud.	**Privacy and Security Considerations:** (Questions 4-5) The physical and backup servers are not located within an approved jurisdiction
Establishing Disposition Authorities: (Questions 6-8). It can accommodate customers' taxonomy for indexing. Retention periods can be applied and be automated	**Applying Disposition Authorities:** (Question 10, 13) Unsure if records can be locked down for viewing only or if records can be transferred at a future date
Applying Disposition Authorities: (Question 9, 11-12) Disposition authority can be applied to aggregations of records. Records can be retained indefinitely, and be destroyed at a future date	**Reviewing Disposition:** (Question 22) Unsure if all decisions are made during review stored in metadata
Executing Disposition Authorities: (Question 14-17) Records and backup can be deleted according to the retention/disposition schedule. Users are alerted to conflicts related of links from records to be deleted to other records aggregations that have different records disposition requirements. If more than one disposal authority is associated with an aggregation of records, all retention requirements can be tracked to allow the manual or automatic lock or freeze on the process	**Integration:** (Question 25) Unsure if the metadata schema is compatible with other systems such as ECM or RMS
Documenting Disposal Actions: (Question 18-19) Disposal actions are documented in process metadata. All disposal actions can be automatically recorded and reported to the administrator (reporting requires audit action by admin?)	
Reviewing Disposition: (Question 20-21, 23-24) Electronic aggregations are presented for review along with their records management metadata and disposal authority information so both content and records management metadata can be reviewed (admin view retention rules & their creators). Records can be marked for destruction, transfer, and further review. System can generate reports (audit reports, various fields). Has the ability to interface with workflow facility to support scheduling, review, and export transfer process provided or supported (emails and chat)	

Assessment:
Google Vault provides a firm foundation for Retention and Disposition functionality and offers most of the services on the checklist. It is fully integrated with Gmail, which means that when searching for email with Vault, it includes the organization's Gmail Archive. This means that messages are available in Vault as soon as they are received by Gmail and the first 1 MB of each message and its attachments are immediately searchable in Vault, the equivalent of about 250 pages. Google Vault supports hangout chats and Google Talk chats. Google Vault can also accommodate indexing, which includes .pdf, .xslx, and .docx files.

Smarsh (Archiving Solution) - Verified

Introduction:
Smarsh delivers cloud-based archiving solutions for the information-driven enterprise. The Smarsh platform provides a unified compliance and eDiscovery workflow across the entire range of digital communications, including email, social media, websites, instant messaging and mobile messaging.

R&D Functionality Present	R&D Functionality Lacking/Unverified
Privacy and Security Considerations: (Question 2) Content is encrypted when in transit to the cloud	**Privacy and Security Considerations:** (Questions 1, 3-5) Unsure if Smarsh allows independent to audit its systems and processes. Unsure if the content is encrypted when at rest in the cloud. Unsure if the physical and backup servers are located within an approved jurisdiction
Establishing Disposition Authorities: (Question 7) Retention periods can be applied	**Establishing Disposition Authorities:** (Question 6, 8) Unsure what index is supported and if destruction is automated
Applying Disposition Authorities: (Question 10-11) Records can be locked down for viewing only and be retained indefinitely	**Applying Disposition Authorities:** (Question 9, 12, 13) Unsure if disposition authority can be applied to aggregations of records. Or if records not in an aggregation be transferred/destroyed at a future date
Executing Disposition Authorities: (Question 14) Records can be deleted according to the retention/disposition schedule	**Executing Disposition Authorities:** (Question 15-17) Unsure if backups can be deleted according to the retention/disposition schedule. Users are not alerted to conflicts related to links from records that are to be deleted to other records aggregations that have difference records disposition requirements. Multiple retention requirements can't be tracked to allow the manual or automatic lock or freeze on the process.
Documenting Disposal Actions: (Question 19) All disposal actions can be automatically be recorded and reported to the administrator	**Documenting Disposal Actions:** (Question 18) Unsure if the disposal actions are documents in the process metadata
Reviewing Disposition: (Question 23) The system can generate reports on the disposition process	**Reviewing Disposition:** (Question 20-24) Unsure if the electronic aggregations presented for review along with their records management metadata and disposal authority information so both content and records management metadata can be reviewed. Unsure if records can be marked for destruction, transfer, further review and if all decisions are made during review stored in metadata. Unsure if the ability to interact with workflow facility to support scheduling, review, and export transfer processes provided or supported
	Integration: (Question 25) Unsure if the metadata schema is compatible with other systems such as ECM or RMS

Assessment:

Smarsh includes functions for the capture, control, and supervision of information. Smarsh provides government records management services including application of retention periods and FOIA, and litigation preparedness. Some enterprise services include risk and governance related to records retention, litigation preparedness through policy enforcement. However, there is a lack of privacy and security capabilities and few services for establishing, applying, and executing disposition authorities.

Symantec Enterprise Vault (Archiving Solution)

Introduction:
Symantec Enterprise Vault introduces innovative new technology that expands the archiving platform to support end-user archiving for email platforms such as Google Mail, Office 365 or any IMAP enabled mail system and enhances the productivity of both IT staff and enterprise end-user customers.

R&D Functionality present	R&D Functionality lacking/unverified
Privacy and Security Considerations: (Questions 1-3) Vendor allows independent audits of systems and processes	**Privacy and Security Considerations:** (Questions 4-5) Unsure if physical and backup servers are located within an approved jurisdiction
Establishing Disposition Authorities: (Questions 6-8) Content is encrypted when in transit and when at rest in the cloud. Indexing capability is supported and it can accommodate customers' taxonomy for indexing. Retention periods can be applied and destruction can be automated.	**Executing Disposition Authorities:** (Question 16) Unsure if users are alerted to conflicts related to links from records to be deleted to other records aggregations that have different records disposition requirements
Applying Disposition Authorities: (Questions 9-13) Disposition can authority be applied to aggregations of records. Records can be locked down for viewing only and it can be retained indefinitely. Records not in an aggregation can be transferred or destroyed at a future date	**Documenting Disposal Actions:** (Questions 18-19) Unsure if disposal actions are documented in process metadata (assumed). Unsure if all disposal actions can be automatically recorded and reported to the administrator (assumed)
Executing Disposition Authorities: (Questions 14-15, 17) Records and backups can be deleted according to the retention/disposition schedule. If more than one disposal authority is associated with an aggregation of records, these multiple retention requirements can be tracked to allow the manual or automatic lock or freeze on the process	**Reviewing Disposition:** (Questions 20-24) Unsure if electronic aggregations are presented for review along with their records management metadata and disposal authority information so both content and records management metadata can be reviewed (assumed). Unsure if records can be marked for destruction transfer, further review (assumed). Unsure if all decisions are made during the review stored in metadata (assumed). Unsure if the system generates reports on the disposition process (assumed). Unsure if the ability to interface with workflow facility to support scheduling, review, and export transfer processes provided or supported (assumed)
	Integration: (Question 25) Unsure if the metadata schema is compatible with other systems such as ECM or RMS (assumed).

Assessment:
Symantec Enterprise Vault provides storage predictability, helping organizations keep applications at predictable storage levels by reclaiming primary storage on-premises or leveraging unlimited storage in a cloud archiving service. It can also help reduce the volume of data to be migrated to Office 365 and shrink the project timeline while minimizing the risk of permanent data loss.

CrashPlan (Backup and Data Protection)

Introduction:
CrashPlan is a backup software and services suite provided by Code42. It is an enterprise SaaS solution that backs up all distributed end-user data such as Apple OS X®, Windows and Linux laptops and desktops. The platform enables IT, security and business teams to limit risk, meet data privacy regulations and recover from data loss, no matter the cause.

R&D Functionality present	R&D Functionality lacking/unverified
Privacy and Security Consideration: (Questions 1-4) Vendor allows independent audits of systems and processes. Content is encrypted when in transit and rest in the cloud. The physical servers located within an approved jurisdiction	**Privacy and Security Consideration:** (Question 5) Unsure if backup servers are located within an approved jurisdiction
Establishing Disposition Authorities: (Question 7) Retention periods can be applied	**Establishing Disposition Authorities:** (Questions 6, 8) Unsure what indexing capability is supported and if destruction can be automated
Applying Disposition Authorities: (Questions 9-11) Disposition authority can be applied to aggregations of records. Records can be locked down for viewing only and can be retained indefinitely,	**Applying Disposition Authorities:** (Questions 12-13) Unsure if records not in an aggregation be transferred or destroyed at a future date
Executing Disposition Authorities: (Questions 14, 17) Records can be deleted according to the retention/disposition schedule. If more than one disposal authority is associated with an aggregation of records, the multiple retention requirements can be tracked to allow the manual or automatic lock or freeze on the process	**Executing Disposition Authorities:** (Questions 15, 16) Unsure if backups be deleted according to the retention/disposition schedule, and if users are alerted to conflicts related to links from records to be deleted to other records aggregations that have different records disposition requirements
Reviewing Disposal Actions: (Question 21, 24) Records can be marked for destruction, transfer, and further review. Has the ability to interface with workflow facility to support scheduling, review, and export transfer processes provided or supported	**Documenting Disposal Actions:** (Question 18-19) Unsure if disposal actions are documented in process metadata or if all disposal actions can be automatically recorded and reported to the administrator.
	Reviewing Disposal Actions: (Questions 20, 22-23) Unsure if electronic aggregations are presented for review along with their records management metadata and disposal authority information so both content and records management metadata can be reviewed. Unsure if all decisions are made during review stored in metadata. Unsure if the system can generate reports on the disposition process
	Integration: (Question 25) Unsure if the metadata schema is compatible with other systems such as ECM or RMS

Assessment:
CrashPlan fulfills most of the privacy and security services with the exception of having backup servers located within an approved jurisdiction. It lacks some of the services in establishing, applying, and executing disposition authorities.

HP Digital Safe (Backup and Data Protection)

Introduction: HP Digital Safe is an intelligent, hosted archiving solution that can help businesses meet their data management needs, with increased business agility and cost savings in the cloud. Leveraging the world's largest, private hosted cloud, Digital Safe is a market-proven solution that can help businesses support their unique information and business objectives.

R & D Functionality Present	R & D Functionality Lacking/Unverified
Privacy and security considerations supported are content encrypted when in transit and while at rest in the cloud, physical and backup servers located within an approved jurisdiction (questions 2-5).	**Privacy and security** considerations not supported: the vendor allowed independent audits of systems and processes (question 1).
Disposition authorities are supported by applied retention periods, records locked down for viewing only, records retained indefinitely, records and backups deleted according to retention/disposition schedule (questions 7,10-11, 14-15).	**Disposition authorities** not supported: indexing capabilities, automated destruction, disposition authority be applied to aggregations of records, records not in aggregation be destroyed or transferred at a future date, users alerted to conflicts related to links from records to be deleted, multiple retention requirements be tracked to allow the manual or automatic lock on the process (questions 6, 8-9, 12-13, 16-17).
	There are no **disposal actions or reports** that are supported: disposal actions documented in process metadata, all disposal actions be automatically recorded and reported to an administrator, electronic aggregations presented for review, records marked for destruction, transfer or further review, all decisions made during review stored in metadata, system generate reports on the disposition process, the ability to interface with workflow facility to support scheduling, review and export transfer process (questions 18-24).
	Metadata schema is not compatible with other systems, such as Enterprise Content Management or Records Management systems to enable **integration** (question 25).

Assessment:
Digital Safe's benefits include secure, private hosted archiving: Identify, manage, and control most data types across enterprise repositories in a hosted archive to support policy management, litigation preparedness, ensure compliance and mitigate risk. Datacenter security: Data within the largest, private cloud is secured and protected across multiple geographically separated SOC2 data centers utilizing split-cell WORM technology to prevent data loss. eDiscovery responsiveness: Robust identification, legal hold, processing, and export capabilities are integrated with Digital Safe to accurately and efficiently identify potentially responsive data.

Microsoft Office 365/SharePoint Online (ECM)

Introduction:
Office 365 is a cloud-based office productivity suite offered in several different plans that can include office applications (Word, Excel, PowerPoint, Outlook, Publisher, and OneNote) in the cloud as well as on premise, storage through OneDrive for Business, and video conferencing through Skype. Profiles can be created and communication facilitated through email, newsfeeds, and Yammer (additional steps necessary for Yammer). SharePoint Online can be used as a standalone offering or as part of the Office 365 suite. Records management features are included in all options, but compliance features are built into only the Enterprise plans.

R&D Functionality present	R&D Functionality lacking
Privacy and security considerations (questions 1, 2, 4, and 5) allow for independent audits of systems and processes, encryption of content in transit, and physical servers and backups located within an organization approved jurisdiction.	**Privacy and security considerations** (question 3). Content is not encrypted while at rest in the cloud.
Disposition authorities (questions 6-8,10-14, and 17) are supported, including indexing, applying retention periods, automatic destruction, lockdown of records for viewing, indefinite retention, destroying or transferring records not in an aggregation, and tracking multiple retention requirements to allow manual or automatic lock or freeze on the disposition process.	The following issues with **disposition authorities** (questions 9, 15-16) exist: A disposition authority cannot be applied to aggregations of records, backups cannot be deleted according to a retention/disposition schedule, and users are not alerted to conflicts related to links from records to be deleted to other record aggregations that have different records disposition requirements.
Disposal actions and reports (questions 18, 21, 23-24) are supported in that disposal actions are documented in process metadata, records can be marked for destruction, transfer and further review, the system generates reports on the disposition process, and there is an ability to interface with workflow facility to support scheduling, review, and export transfer processes.	The following **disposal actions and reports** (questions 19-20, and 22) features are lacking: Disposal actions cannot automatically be recorded and reported to the administrator, electronic aggregations are not presented for review along with their records management metadata and disposal authority information, and not all decisions made during the review process are stored in metadata.
Metadata schema is compatible with other systems, such as Enterprise Content Management or Records Management systems to enable **integration**.	

Assessment:
Retention functionality is built into Office 365/SharePoint Online. Retention periods can be applied to individual documents or aggregations of documents in libraries. Connectors allow automatic ingest of content from source systems, such as from legacy systems. Integration is provided on the back end for objects that need to be moved to a long-term digital repository (such as Preservica). Several solutions are available to enable more robust retention and disposition capabilities (such as Collabware and Gimmal). One cloud solution, Records 365, was designed specifically for Office 365. Office 365/SharePoint online has limited retention and disposition features that may be sufficient for smaller organizations or for initial installations to better understand its capabilities. However, those who demand more robust records management functionality would be wise to look at the integration of third-party solutions.

Dropbox (File Sharing & Storage)

Introduction:
Dropbox is a Software as a Service (SaaS) provider for cloud storage. In addition to a free desktop app with some free storage, Dropbox has other services with more capabilities. The three options for services include: Pro (for individuals), Business (for teams), and Enterprise (for large organizations). These offer varying levels of storage space admin controls, and security functions for different prices. Dropbox allows files to be accessed from any device, and emphasizes the ability to keep backups of files and allows for easy sharing and collaboration.

R&D Functionality present	R&D Functionality lacking or unverified
Privacy and Security Considerations (Questions 1-5) Independent audits and encryption in transit and at rest are supported. Users are informed of the Jurisdictions of servers, and there are many locations to choose from.	**Establishing Disposition Authorities** (Questions 7-8) Retention periods and destruction cannot be automated.
Establishing Disposition Authorities (Questions 6-7) User indexing is supported. Retention periods can be applied manually.	**Applying Disposition Authorities** (Question 9) Disposition authorities cannot be applied to aggregates automatically.
Applying Disposition Authorities (Questions 9-13) Disposition can be applied to aggregates only if done manually. Records can be locked down for viewing only and retained indefinitely. Records not in aggregations can be destroyed or transferred at future dates.	**Executing Disposition Authorities** (Questions 16-17) Users are not alerted to conflicts between disposition requirements of individual records and aggregates. Multiple retention periods cannot be tracked or locked down.
Executing Disposition Authorities (Questions 14-15) Records and their backups can be deleted according to a retention and disposition schedule if done manually.	**Reviewing Disposition** (Question 20) Only audits are presented for review, not electronic aggregations with records management metadata and content.
Documenting Disposal Actions (Questions 18-19) Disposal actions are documented in process metadata, automatically recorded, and reported to the administrator.	**Integration** (Question 25) Unsure if metadata schema is compatible with other systems.
Reviewing Disposition (Questions 20-24) Audits of records can be reviewed and records can manually be marked for review, destruction, or transfer. Decisions made during review are recorded in metadata. System-generated reports are produced. Able to interface with workflow for scheduling, transfer, and export.	

Assessment:
The records management capabilities of Dropbox are sufficient only if an organization is willing to apply retention and disposition schedules manually. The easy to use cloud storage is appealing in its collaborative capabilities, backups, and encryption, but the service does not provide extensive aggregate-level retention planning functions. This would most likely not be an adequate service for larger organizations or government agencies which would need greater control for legal compliance, Freedom of Information requests, and litigation or eDiscovery.

Egnyte (File Sharing & Storage)

Introduction:
Egnyte is a hybrid cloud service for enterprise storage and sharing. Egnyte offers secure storage for a business to share files within an enterprise and collaborate on those files from different devices. The hybrid environment means that both on-site and cloud storage can be managed centrally and records can be progressively added to the cloud. Egnyte complies with a number of data security and privacy standards, including HIPPA and ISO/IEC 27001:2013.

R&D Functionality present	R&D Functionality lacking or unverified
Privacy and Security Considerations (Questions 1-3) Servers are audited annually; content is encrypted in transit and at rest.	**Privacy and Security Considerations** (Questions 1, 4-5) Independent audits are not supported. No information is given on the jurisdiction of physical and backup servers.
Applying Disposition Authorities (Questions 10-11) Records can be locked down for viewing only and can be retained indefinitely.	**Establishing Disposition Authorities** (Questions 6-8) Unclear if these functionalities are offered. Includes: indexing capabilities, application of retention periods, automatic destruction.
Executing Disposition Authorities (Questions 14-15) Records and their backups can be deleted according to a schedule through a user dashboard.	**Applying Disposition Authorities** (Questions 9, 12-13) Unsure if disposition can be applied to aggregates or if records not in an aggregate can be destroyed or transferred at a future date.
Documenting Disposal Actions (Questions 18-19) Disposal actions are documented in process metadata and are automatically recorded and reported to administrator.	**Executing Disposition Authorities** (Questions 16-17) Unsure if users are alerted to conflicts related to links from records to be deleted to other records aggregations that have different records disposition requirements. Multiple retention periods cannot be tracked for freeze or lock.
Reviewing Disposition (Question 23) The system can generate reports on the disposition process	**Reviewing Disposition** (Questions 20-22, 24) Unsure if aggregations can be presented for review with records management metadata, if records can be marked for review/transfer/destruction, if decisions in review are recorded in metadata, or if system is able to interface with workflow.
Integration (Question 25) Metadata schema is compatible with other systems.	

Assessment:
Egnyte is an appropriate service to use for integrating workflows and sharing in a collaborative enterprise. However, for records management functionalities, it falls short of providing adequate retention and disposition capabilities in the cloud. Without the ability to mark records for destruction, automatically apply retention schedules, or apply disposition to aggregates, organizations using Egnyte would have difficulties implementing sound management practices to their records in the cloud. Manual destruction could be carried out, but this is not the most efficient method for large organizations. The inability to mark aggregates for disposition means that a separate service or process would be required to monitor records under a particular schedule, making RIM workflows more convoluted and prone to errors.

OneDrive (File Sharing & Storage)

Introduction:
Microsoft's OneDrive is a file hosting and sharing service. Users can upload files to the cloud and then sync between devices, allowing for cross-platform access. Users can also share their files with specific persons, or share them publicly. Persons with access to hosted content can download them as a zip file. The file hosting can be accomplished through a web browser or a desktop application. Increased storage space is available for purchase, up to 1 TB.

R&D Functionality present	R&D Functionality lacking or unverified
Privacy and Security Considerations (Questions 1-2, 4-5) The vendor allows independent audits of systems and processes. Content is encrypted in transit to the cloud. Physical and backup servers are located in multiple jurisdictions.	**Privacy and Security Considerations** (Question 3) Content is not encrypted at rest in the cloud
Establishing Disposition Authorities (Question 7) Retention periods can be applied manually	**Establishing Disposition Authorities** (Questions 6, 8) User taxonomy for indexing is not offered. Destruction cannot be automated.
Applying Disposition Authorities (Questions 10-13) Records can be locked down for viewing only and retained indefinitely. Records not in an aggregation can be destroyed or transferred at a future date.	**Applying Disposition Authorities** (Question 9) Disposition cannot be applied to aggregations of records.
Executing Disposition Authorities (Questions 14-15) Records and their backups can be deleted according to their retention schedule if done manually.	**Executing Disposition Authorities** (Questions 16-17) Users are not alerted to conflicts related to links between records with different retention periods. Multiple retention periods cannot be tracked to freeze/lock for legal purposes.
	Documenting Disposal Actions (Questions 18-19)Disposal actions are not documented in metadata nor are they automatically recorded and sent to the administrator as a report.
	Reviewing disposition (Questions 20-24), Aggregations are not presented for review with metadata, and actions during review are not recorded. System-generated reports on disposition are not offered. Records cannot be marked for future action. Interfacing with existing workflows is not offered
	Integration (Question 25) metadata schemas are not compatible with other systems

Assessment:
Microsoft OneDrive is best suited for personal file organization and sharing. Users with multiple devices will find the service useful in its sync functions and ability to use contacts in the Windows account to share files. Individuals can also know that information stored in OneDrive is secure and encrypted, and deleted records can be easily recovered. However, the lack of automated records management functionalities or compatible metadata schemas means that this service is not ideal for larger organizations or public agencies needing to comply with legal demands. Institutions with a large volume of records would have difficulty manually carrying out retention schedules without the ability to mark aggregates or even individual files as having a particular retention period. Without these capabilities, OneDrive should not be adopted by government or other large organizations.

Amazon Web Services (IaaS/PaaS/Managed Services)

Introduction:
Amazon Web Services (AWS) is a secure cloud services platform that offers compute power, database storage, content delivery and other functionalities to help organizations scale and grow.

R & D Functionality Present	R & D Functionality Lacking/Unverified
Privacy and Security considerations (questions 2 & 3) allow for content encrypted while in transit and at rest in the cloud.	**Privacy and Security** considerations (questions 1, 4 & 5) do not allow for independent audits of systems and processes, physical servers and back up servers located in approved jurisdictions.
Disposition authorities (questions 7-11 & 14) are supported in larger part, retention periods can be applied, destruction can be automated, disposition authority may be applied to aggregations of records, records may be locked down for viewing only and retained indefinitely, records can be deleted according to a retention/disposition schedule.	The following issues with **disposition authorities** are not supported (question 6, 12, 13 & 15-17): Indexing capability, records not in an aggregation be destroyed or transferred at a future date, backups be deleted according to a retention/disposition schedule, users alerted to conflicts related to links from records and if more than one disposal authority is associated with aggregation can these multiple retention requirements be tracked down to allow manual or automatic lock or freeze.
	The following **disposal actions and reports** features are not supported (questions 18-24): disposal actions documented in process metadata, disposal actions are automatically recorded and reported to administrator, electronic aggregations presented for review so both content and records management metadata can be reviewed, records marked for destruction, transfer or further review, decisions made during review stored in metadata, system generate reports on the disposition process, ability to interface with workflow facility to support scheduling, review, and export transfer processes provided or supported
	Metadata schema is compatible with other systems, such as Enterprise Content Management or Records Management systems to enable **integration** (question 25).

Assessment:
Amazon Web Services offers basic storage and data archiving options with strong encryption. However, when it comes to retention and disposition, the primary focus is on disposition authorities such as applied retention periods, automated destruction of records and indefinite retention, without allowing for review, integration, or retention and disposition of aggregations.

Century Link (Tier3) (IaaS/PaaS/Managed Services)

Introduction:
CenturyLink is the third largest telecommunications company in the United States and is recognized as a leader in the network services market by technology industry analyst firms. The company is a global leader in cloud infrastructure and hosted IT solutions for enterprise customers. CenturyLink provides data, voice and managed services in local, national and select international markets through its high quality advanced fiber optic network and multiple data centers for businesses and consumers.

R & D Functionality Present	R & D Functionality Lacking/Unverified
Privacy and security considerations (questions 1-5) allow for: independent audits of systems and processes, encrypted content when in transit and rest in the cloud, physical and back up servers are located within approved jurisdictions.	The following issues with **disposition authorities** are not supported (questions 16-17): users alerted to conflicts related to links from records to be deleted to other records aggregations, multiple retention requirements can be tracked to allow the manual or automatic lock/freeze on the process.
Disposition authorities (questions 6-15) are supported in larger part, accommodate customers taxonomy for indexing, applied retention periods, automated destruction of records, records can be locked for viewing, disposition authority are applied to aggregations of records, records may be retained indefinitely, non aggregated records may be destroyed or transferred at a future date, records and back up records may be deleted according to retention schedule.	**Disposal actions and reports** (questions 20-22, 24) are not supported: electronic aggregations are presented for review along with their records management metadata, records may be marked for destruction, transfer or further review, the ability to interface with workflow facility to support scheduling, review and export transfer processes provided or support.
Disposal actions and reports (questions 18, 19 & 23) are supported: disposal actions are documented in process metadata , disposal actions may be automatically recorded and reported, system may generate reports on the disposition process.	Metadata schema is not compatible with other systems, such as Enterprise Content Management or Records Management systems to enable **integration** (question 25).

Assessment:
CenturyLink provides most services for retention and disposition actions and should be a strong contender when investigating vendors. They fulfill all the services in privacy and security and all but two disposition authorities.

GoGrid/Datapipe (IaaS/PaaS/Managed Services)

Introduction:
GoGrid is the world's first multi-cloud-server control panel that enables customers to deploy and manage on-demand server hosting. Datapipe, a global leader in managed hybrid IT solutions for the enterprise, has recently acquired GoGrid. GoGrid's proprietary orchestration and automation technologies are unique in the market, providing 1-Button deployment for Big Data solutions that speed creation and results of new cloud projects.

R & D Functionality Present	R & D Functionality Lacking/Unverified
The only **privacy and security** consideration present is independent audits of systems and processes (question 1).	**Privacy and security** considerations not supported: content encrypted when in transit and at rest in the cloud, physical and back up servers located in approved jurisdictions (questions 2-5).
Disposition authorities are supported by indexing capability, applied retention periods, records that can be locked down for viewing only and backups can be deleted according to retention/disposition schedule (questions 6, 7, 10 & 15).	**Disposition authorities** not supported are automated destruction of records, disposition authority be applied to aggregation of records, record retained indefinitely, records not in aggregation be destroyed or transferred at a future date, records be deleted according to retention/disposition schedule, users alerted to conflicts related to links from records to be deleted to other records aggregation that have different disposition requirements, multiple disposal authorities are associated with an aggregation of records (Questions 8, 9, 11-14, 16 & 17).
	There are no **disposal actions or reports** that are supported: disposal actions documented in process metadata, all disposal actions be automatically recorded and reported to an administrator, electronic aggregations presented for review, records marked for destruction, transfer or further review, all decisions made during review stored in metadata, system generate reports on the disposition process, the ability to interface with workflow facility to support scheduling, review and export transfer process (questions 18-24).
	Metadata schema is not compatible with other systems, such as Enterprise Content Management or Records Management systems to enable **integration** (questions 25).

Assessment:
GoGrid/DataPipe offers very few retention and disposition functions. They specialize in basic data storage and provide a scalable and reliable file-level back up service. The following is the responsibility of the customer: encryption in transit, encryption at rest, secure data deletion, data backup, security audits, managing and monitoring the firewall service, and more.

Rackspace (IaaS/PaaS/Managed Services)

Introduction:
Rackspace Inc. is a managed cloud computing company based in Windcrest, TX. They have two primary lines of business: Cloud Servers and Dedicated Servers. Rackspace helps design, build, and operate workloads across both environments depending on the individual needs of the customer.

R & D Functionality Present	R & D Functionality Lacking/Unverified
Privacy and security considerations supported are independent audits of systems and processes, content is encrypted when in transit and at rest in the cloud (questions 1-3).	**Privacy and security** considerations not supported: physical and backup servers located within an approved jurisdiction (questions 4-5).
Disposition authorities supported are indexing capabilities, applied retention periods, automated destruction, disposition authority applied to aggregations of records, locked down records for viewing only, records retained indefinitely, records not in aggregation can be destroyed at a future date, records and backups can be deleted according to the retention schedule (questions 6-12, 14-15).	**Disposition authorities** not supported: records not in an aggregation be transferred at a future date, users alerted to conflicts related to links from records to be deleted to others records aggregations that have different records disposition requirements , multiple retention requirements be tracked to allow manual or automatic lock (questions 13, 16-17).
Disposal actions & reports supported: disposal actions documented in process metadata, disposal actions are automatically recorded and reported to the administrator, records marked for destruction, transfer and further review, decisions made during review stored in metadata, system can generate reports on the disposition process, ability to interface with workflow facility to support scheduling, review and export transfer processes (questions, 18-19, 21-24).	
Metadata schema is compatible with other systems, such as Enterprise Content Management or Records Management systems to enable **integration** (question 25).	

Assessment:
Rackspace is an application specific archive vendor. The service offers solutions tailored to application data, specifically email archiving. Using Rackspace would require some setup work to integrate with the customer's email software, but no additional software or hardware is needed. Rackspace uses its existing infrastructure as a repository for data storage. Additionally, a private cloud can be hosted at the client's own data center, in a partner data center, or at Rackspace. Archived email can be accessed from any web browser. Redundant storage is used for email retention, and nine copies of each message are held across multiple data centers. Users can locate and recover deleted emails. Their security management model is based on the 'Plan, Do, Check, Act' model as recommended by ISO 27001.

CloudNine (Litigation Support and eDiscovery)

Introduction:
CloudNine is a Software as a Service (SaaS) online eDiscovery tool. Marketed towards law firms and large corporations, the service lets users upload data, automatically convert and process, and then review their discovery data. CloudNine is meant to reduce the duration of eDiscovery reviews and outsourcing for processing.

R&D Functionality present	R&D Functionality lacking or unverified
Privacy and Security Considerations (Questions 2-3) Content is encrypted at rest and in transit to the cloud	**Privacy and Security Considerations** (Questions 1, 4-5) It is unverified whether the vendor allows independent audits. Jurisdiction for physical and backup servers may or may not be in approved locations.
Applying Disposition Authorities (Question 10) Records can be locked down for view only	**Establishing Disposition Authorities** (Questions 6-8) Unsure if vendor allows for indexing, application of retention periods, or automated destruction.
	Applying Disposition Authorities (Questions 9, 11-13) Most of this is out of scope for an eDiscovery tool. The following functionalities are unverified or not offered: dispositions applied to aggregates, indefinite retention, records not in an aggregation can be destroyed or transferred in the future.
	Executing Disposition Authorities (Questions 14-17) Questions 14 and 15 (can records and backups be deleted according to the retention schedule) are both outside of the scope of Cloud Nine's purpose. Users are not alerted to conflicts related to different retention periods, and retention periods cannot be tracked to freeze or lock the process.
	Documenting Disposal Actions (Questions 18-19) Unclear if actions are documented in metadata or if actions are automatically recorded and sent to administrator
	Reviewing Disposition (Questions 20-24) These functionalities are out of scope for the service.
	Integration (Question 25) Unsure if metadata schema is compatible with other systems

Assessment:
CloudNine is a specialized tool for litigation and discovery purposes, and therefore has less of a focus on retention and disposition or long-term storage. For organizations such as law firms or corporations at a risk for litigation, this is an effective tool for facilitating eDiscovery in an organized way. However, for organizations seeking to store the entirety of their institutional records in the cloud, this service should only be supplementary.

NextPoint (Litigation Support and eDiscovery)

Introduction:
NextPoint is litigation support software for eDiscovery. It is focused on collecting email, social media, and websites for use in litigation. The data is collected, then imaged and indexed for users to review for litigation. NextPoint provides collaboration functionalities and a variety of tagging, indexing, and search capabilities. The modules of NextPoint are: Collect, Analyze, Review, Exchange, and Preparation. Each of these is aimed at a specific step of eDiscovery and litigation processes.

R&D Functionality present	R&D Functionality lacking or unverified
Privacy and Security Considerations (Questions 2-3) Content is encrypted in transit and at rest in the cloud.	**Privacy and Security Considerations** (Questions 1, 4-5) Unsure if independent audits are permitted. Backup and physical servers are provided through Amazon Web Services, which has data centers in multiple jurisdictions.
Establishing Disposition Authorities (Question 6) Some indexing capabilities are supported. User tagging and searches for eDiscovery are offered.	**Establishing Disposition Authorities** (Questions 7-8) Unclear if retention periods can be applied. Destruction cannot be automated.
Applying Disposition Authorities (Question 10) Records can be locked down for viewing only.	**Applying Disposition Authorities** (Questions 9, 11-13) Most disposition functions are out of scope for Nextpoint as an eDiscovery software. Application of disposition authorities to aggregates, indefinite retention, and destruction or transfers of records not in an aggregate are all functionalities which are either not offered or not verified.
	Executing Disposition Authorities (Questions 14-17) These functionalities are all out of scope for Nextpoint: deletion of records and backups according to a retention schedule, user alerts for conflicts between different retention periods, and tracking or locking multiple retention periods.
	Documenting Disposal Actions (Questions 18-19) Disposal actions are not documented in process metadata. Actions are not automatically recorded and sent to administrator
	Reviewing Disposition (Questions 20-24) These capabilities are out of scope for Nextpoint: Presenting content and metadata of aggregates for review, mark records for future review/transfer/destruction, review decisions stored in metadata, system-generated reports on disposition, ability to interface with workflow.
	Integration (Question 25) The metadata schema is not compatible with other systems.

Assessment:
As a litigation software solution, NextPoint should not be used as the sole cloud provider of an institution. NextPoint has functionalities specific to eDiscovery needs which makes it useful for law firms and organizations that are at risk for litigation. However, when it comes to storing and applying retention and disposition schedules to an organization's records, a different type of cloud provider should be used. NextPoint does not provide significant storage or records management functionalities due to the nature of its services.

Archivematica (Long-Term Digital Preservation) – Verified

Introduction:
Archivematica is a standards-based, open-source preservation system for long-term access to trustworthy, authentic, and reliable digital content. It complies with the ISO-OAIS functional model, and all of its functions take place within a web-based dashboard accessed through a web browser. Archivematica interacts with other software (e.g., Archivist Toolkit). Access to Memory (AtoM) is its archives catalog and de facto dissemination platform. It runs on Linux and can use a local or a cloud service provider such as Microsoft Azure to host data.

R&D Functionality present	R&D Functionality Lacking or Not Applicable
Archivematica does support Questions 1, 4-5 in the **Privacy & Security Considerations** category. Archivematica allows independent audits of systems and processes. Physical servers and backup servers can be located in a jurisdiction approved for the organization, since AIPs are stored in the client's preferred repository.	Archivematica does not provide encryption for content in transit to or at rest in the cloud (Questions 2-3, **Privacy & Security Considerations**).
Archivematica does allow records to be retained indefinitely, **Disposition Authorities** (Question 11).	**Disposition authorities**, questions 6 through 17, with the exception of 11, are not supported by Archivematica—this includes indexing capabilities, applying retention and destruction rules, and locking down content for viewing only, retaining records indefinitely, and destroying or transferring records at a future date. Records and backups cannot be deleted according to the retention/disposition schedule, users are not alerted to conflicts related to links from records to be deleted to other records aggregations with different retention requirements, and multiple retention requirements cannot be tracked to allow manual or automatic lock or freeze on the disposition process.
Question 20, **Disposal Actions & Reports**, asks if electronic aggregations are presented for review along with their records management metadata and disposal authority information. The response is "partial."	Question 18-19, 21-24, **Disposal Actions & Reports** are not supported. Disposal actions are not documented in process metadata or automatically recorded and reported to the administrators. Records cannot be marked for destruction, transfer, or further review. Decisions made during review are not stored in metadata. The system does not generate reports on the disposition process. The ability to interface with workflow facility to support scheduling, review, and export transfer processes are not provided or supported.
The metadata schema is compatible with other systems, such as Enterprise Content Management or Records Management systems to allow **integration** (Question 25).	

Assessment:
Archivematica is designed for long-term preservation and therefore does not support disposition authorities or most disposition actions. Records managed through this OAIS-compliant preservation system would have to be retrieved through a Dissemination Information Package for production in response to eDiscovery. This is a very good solution for organizations with the technical expertise to install Archivematica and associated software. But it focuses on only one segment of the records lifecycle: disposition through preservation.

ArchivesDirect (Long-Term Digital Preservation) - Verified

Introduction:
ArchivesDirect is an open-standards, hosted solution that combines the Archivematica preservation workflow tool with archival cloud storage and preservation service from DuraSpace. Users access the suite of digital preservation functions via an online dashboard. Archivematica produces standardized, interoperable Archival Information Packages, automatically transfers AIP packages to DuraCloud for long-term secure archival storage. Some key features available in ArchivesDirect include assigning permanent identifiers and checksums, virus checking, identifying and validating file formats, extracting technical metadata, normalizing files upon ingest to preservation-friendly formats, and generating detailed PREMIS and METS metadata to facilitate inter-repository data exchange.

R&D Functionality present	R&D Functionality lacking
Only one **Disposition Authority** feature is supported (Question 11). Records can be retained indefinitely.	**Privacy and security** features are either unknown (audits and storage location dependent upon the user) or lacking (encryption when in transit to the cloud and when at rest in the cloud).
Disposal actions are documented in process metadata (Question 18). .	**Disposition authorities** (questions 6-17) are not supported except for question 11. Indexing capability is not present, retention periods can not be applied, destruction cannot be automated, retention and disposition specifications cannot be applied to aggregations of records, records cannot be locked down for viewing, and records and backups cannot be deleted according to retention and disposition requirements. Users are not alerted to conflicts related to links from records to be deleted to other aggregations that have different records disposition requirements. If more than one disposal authority is associated with an aggregation of records, multiple retention requirements cannot be tracked to allow automatic or manual lock or freeze on the process.
The metadata schemas (METS and PREMIS) are compatible with other systems, such as Enterprise Content Management or Records Management Systems, making **Integration** possible.	Except for Question 18 (disposal actions documented in process metadata), none of the **disposal actions and reports** functionalities are present, including automatic recording of disposal actions and reporting to the administrator and marking records for destruction, transfer, or further review. Decisions made during review are not stored in metadata, the system does not generate reports on the disposition process, and the system does not interface with workflow to support scheduling, review, and export transfer processes provided or supported.

Assessment:
This solution is limited in scope. Records management features are not addressed with the exception of the fact the records can be ingested and retained indefinitely, a goal of long-term storage. Objects can be accessed or removed from the repository. Disposal actions are documented in process metadata, and integration is possible based on the metadata standards used. This open-source solution is suited for long-term preservation based on the archival storage and access features available. However, it does not include retention and disposition functionality. Other solutions should be investigated to enable retention and defensible deletion of records.

Note: Late entry; not included in the gap analysis in Appendix B.

Preservica – (Long-Term Digital Preservation) - Verified

Introduction:
Preservica provides digital preservation technology, consulting services, and research products. Preservica is also the name of the the company's digital preservation and access software based on the trusted digital repository standard ISO 14721- Open Archival Information System (OAIS) – Reference Model. In addition to providing compliant workflows for ingest, data management, storage, access, administration, and preservation, it provides a Universal Access module that allows content to be shared with the public. The company has offices in both the United Kingdom and the United States.

R&D Functionality present	R&D Functionality either not applicable or lacking
Privacy & Security Considerations (Questions 1-3) reveal that Preservica allows independent audits and encrypts content in transit and at rest.	**Privacy & Security Considerations** (Questions 4-5). Physical servers for the OAIS-compliant software are located in regions in both the US and UK. However, physical servers may be located outside of a jurisdiction approved for your organization.
Disposition Authorities (Questions 6-14). Indexing of custom metadata is available on all editions (CE, SE, EE) from Preservica v5.6 as of February 2016. Retention periods can be applied to content, and destruction can be automated. A disposition authority (retention and disposition specifications) can be applied to aggregations of records. Records can be locked down for viewing only and can be retained indefinitely. Records not in an aggregation can be destroyed or transferred at a future date. Records can be deleted according to a retention/disposition schedule.	**Disposition Authorities** (Questions 15-17). Preservica Cloud Edition stores metadata in Amazon RDS and digital content in either Amazon S3 or lower-cost Amazon Glacier. Preservica Standard and Enterprise Editions can store content on a customer's local storage array as well. All editions include a "Copy Home" feature to save collections to an external FTP server. Backups cannot be deleted according to a retention/disposition schedule. Users are not alerted to conflicts related to links from records to be deleted to other records aggregations that have different records disposition requirements. If more than one disposal authority is associated with an aggregation of records, multiple retention requirements cannot be tracked to allow the manual or automatic lock or freeze on the process (ex., Freeze for litigation or freedom of information request).
Disposal Actions & Reports (Questions 18-24) are supported. This includes documenting disposal actions in process metadata and automatically recording and reporting disposal actions to the administrator. Electronic aggregations, their records management metadata, and disposal authority are presented for review. Records can be marked for destruction, transfer, and further review. All decisions are stored in metadata, and the system can generate a report on the disposition process. Workflow facility is present to support scheduling, review, and export transfer processes.	
Integration (Question 25). Preservica supports CMIS interface for interoperability. Preservica is also schema agnostic making it easy to interoperate with other systems, such as SharePoint, Outlook, ContentDM, PastPerfect, Lotus Notes, Gmail.	

Assessment:
Designed for long-term digital preservation based on the OAIS reference model, Preservica recognizes that long-term may be as brief a 10 years due to technology refresh cycle acceleration. This demands the ability to set retention schedules, a recently added feature in Preservica. Preservica Cloud Edition supports almost all of the functionality identified for retention and disposition in a cloud environment within a long-term trusted digital repository.

Collabware CLM (RM Extender) – Verified

Introduction:

Collabware CLM is designed specifically to extend the Records Management functionality of Microsoft's SharePoint. Collabware CLM allows full records management capability, including auto-declaration and auto-classification. Unfortunately, SharePoint Online is not supported with this product. However, this product is included here for SharePoint Online users so they can monitor the further development of a new offering, *Collabspace*, which at the time of this writing, can integrate with SharePoint on premise and SharePoint Online. Currently it enables real-time chat, collaboration and file sharing with internal and external team members without leaving Microsoft Outlook. According to the vendor, their "target is to have complete feature parity between Collabware CLM for SharePoint 2010/2013/2016 and Collabspace for SharePoint Online by the end of the 2016 calendar year" (Sibley, email 2016, February 23). View the assessment below the Collabware CLM Functionality Table, which should be mirrored in Collabspace when it is released.

R&D Functionality present	R&D Functionality lacking
Disposition Authorities (Questions 6-15 and 17) are supported in Collabware. This includes indexing capabilities, application of retention periods, automation of destruction, application of disposition authority to aggregations of records, lock down for viewing, retaining records indefinitely, and destroying and transferring records in an aggregation at a future date. Records and backups can be deleted according to the retention/disposition schedule. In addition, if ore than one disposal authority is associated with an aggregation of records, multiple retention requirements can be tracked to allow the manual or automatic lock or freeze on the process.	**Disposition Authorities** (Question 16). Users are not alerted to conflicts related to links from records to be deleted to other records aggregations that have different records disposition requirements. (Note: This will be possible in Collabspace)
Disposal Actions & Reports (Questions 18-19 and 21-24) are supported. This includes documenting disposal actions in process metadata; recording and reporting disposal actions to the administrator; marking records for destruction, transfer, and further review; storing all decisions in metadata; generation reports on the disposition process; and interfacing with workflow facilities to support scheduling, review, and export transfer processes.	**Disposal Actions & Reports** (Question 20). Electronic aggregations are not presented for review along with their records management metadata and disposal authority information so both content and records management metadata can be reviewed. (Note: This will be possible in Collabspace)
Integration (Question 25). Metadata schema is compatible with other systems, such as Enterprise Content Management or Records Management systems.	

Assessment:

Organizations that seek to demonstrate compliance with their own organization's records management policy should consider an extension such as Collabware CLM to add functionality not present in SharePoint. Privacy and security issues are not addressed for this product, since the decisions related to encryption, jurisdiction of primary and backup servers, and auditing of the system—in this case SharePoint—are related to the implementation of the ECM and not the Collabware third-party extension. Since the start of this project and the initial review of Collabware CLM, a new product has emerged, Collabspace.

Gimmal Compliance Suite for Microsoft SharePoint (RM Extender) – Verified

Introduction:
The *Gimmal Compliance Suite for Microsoft SharePoint*. This suite is Department of Defense 5015.2 Certified for SharePoint 2010 and 2013 to ensure compliance with regulations or best practices. The Functionality listed below relates to the functions that can be added to On-premise SharePoint installations. A second product, *Gimmal Records-as-a-Services for Microsoft® Office 365*, provides similar functionality for Microsoft Office 365 (the cloud version of MS Office).

R&D Functionality present	R&D Functionality lacking
Disposition Authorities (Questions 6-15 and 17) are supported in Collabware. This includes indexing capabilities, application of retention periods, automation of destruction, application of disposition authority to aggregations of records, lock down for viewing, retaining records indefinitely, and destroying and transferring records in an aggregation at a future date. Records and backups can be deleted according to the retention/disposition schedule. In addition, if ore than one disposal authority is associated with an aggregation of records, multiple retention requirements can be tracked to allow the manual or automatic lock or freeze on the process.	**Disposition Authorities** (Question 16). Users are not alerted to conflicts related to links from records to be deleted to other records aggregations that have different records disposition requirements.
Disposal Actions & Reports (Questions 18-19 and 21-24) are supported. This includes documenting disposal actions in process metadata; recording and reporting disposal actions to the administrator; marking records for destruction, transfer, and further review; storing all decisions in metadata; generation reports on the disposition process; and interfacing with workflow facilities to support scheduling, review, and export transfer processes.	**Disposal Actions & Reports** (Question 20). Electronic aggregations are not presented for review along with their records management metadata and disposal authority information so both content and records management metadata can be reviewed.
Integration (Question 25). Metadata schema is compatible with other systems, such as Enterprise Content Management or Records Management systems.	

Assessment:
Encryption, jurisdiction of primary and backup servers, and auditing of the system—in this case Office 365/SharePoint—are related to the implementation of the ECM and not the third-party extension. *Gimmal Advanced Content Retention Rules* allow organizations to implement a manage-in-place records strategy with centralized, robust, and highly granular retention policies for O365 content. The product provides search, discovery, and legal holds to enable litigation preparedness and enforce compliance. Gimmal enhances the records management features of SharePoint on premise and Office 365/SharePoint Online.

6.2 Phase 2: User Feedback

To understand the records retention and disposition challenges for the organization, it is necessary to view the issue of cloud computing from the perspective of the user. The research team conducted an online survey of records and information management professionals to determine their involvement with records in the cloud and their understanding of retention and disposition functionality available or lacking within the cloud services and products employed by the enterprise.

6.2.1 Participant information and experience with cloud services

Members of ARMA International were invited to participate in an online survey through email announcements sent to members as well as posts in social media accounts. The first invitation to participate was sent to all ARMA members on February 5, 2015. The survey was closed on March 15, and a total of 168 useable responses were received. The majority of respondents (60.84%) were identified as records managers, followed by information governance professionals (10.24%). The majority of respondents worked in the government sector (37.13%), those who work in professional and technical services and finance and industry followed at 8.98% and 8.38%. Organizations with less than 1,000 employees made were represented by 49.09% of the respondents. Organizations with more than 5,000 employees made up 26.67% followed closely by those with 1,000 to 5,000 at 24.24%.

Of the 168 respondents, ninety-seven (57.74%) indicated their organization employed cloud services, forty (23.81%) indicated their organizations did not, and twelve (7.14%) did not know if cloud services were in use by their organization. The use of cloud computing was a relatively new phenomenon as reported by respondents. Of the ninety-seven that answered yes, only 25 percent had used it for more than three years; 56.82 percent stated they used it between one and three years, and 13.64 percent used it less than one year. The remaining respondents indicated they did not know the answer to this question or did not respond.

6.2.2 Retention and disposition policies and practices

A number of questions were asked related to retention and disposition policies and practices, as summarized in Figure 1. Although ninety-seven respondents indicated their organization employed cloud services, not all felt they were in a position to respond to questions on this topic. The three “decline to respond” selections were included with the “no response” selections.

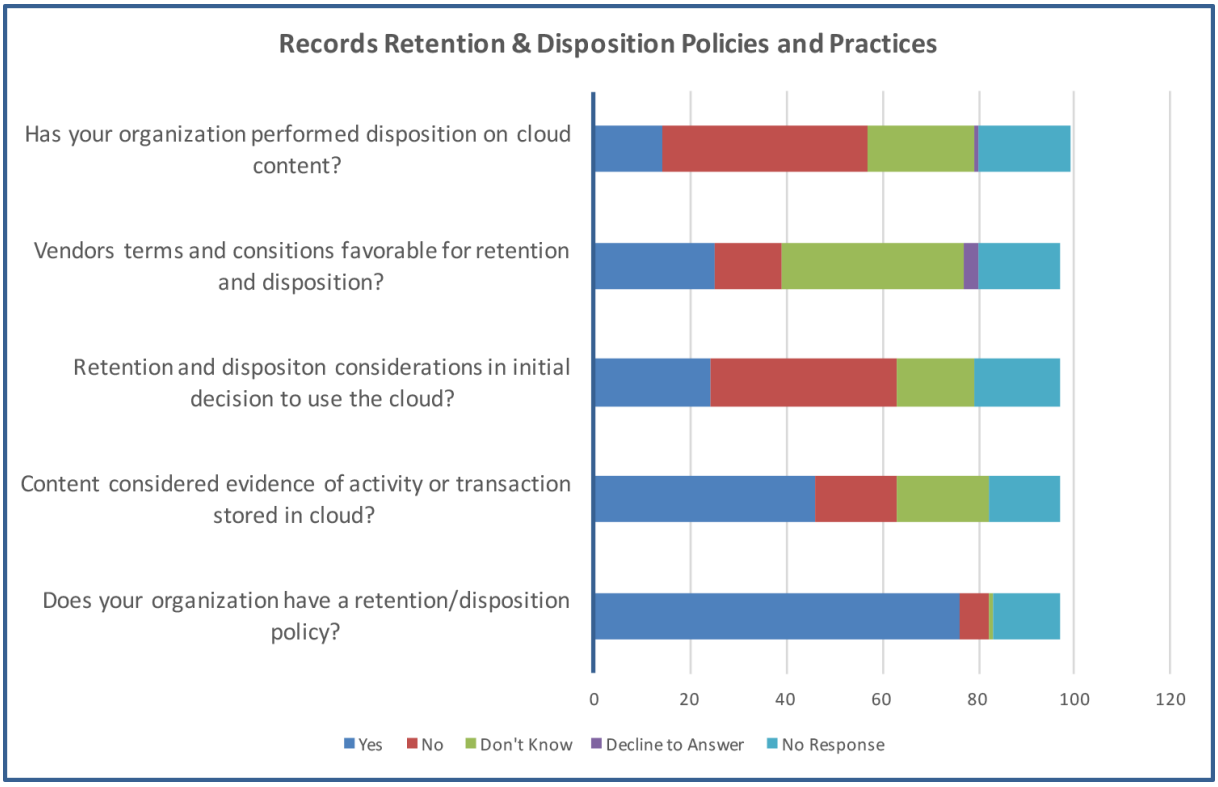

Figure 1: Retention and Disposition responses to survey of records and information management professionals.

The findings indicated that although an overwhelming majority of respondents stated their organizations have retention and disposition policies in place, and almost half have content considered as evidence of activities or transactions stored in the cloud, only approximately one-quarter believe the vendor terms and conditions are consistent with their organization's goals and objectives for retention and disposition.

Under one-quarter of survey respondents indicated retention and dispositions considerations were included when selecting cloud services. In addition, only approximately 14 percent of the respondents indicated that their organization performed disposition of content stored in the cloud, with some remarking that the retention period for content residing in the cloud had not yet been met.

6.2.3 Basic cloud security requirements

Although not an indicator of retention and disposition functionality, organizations must consider basic cloud security requirements before entering into agreements with cloud service providers. Users were asked five questions related to data encryption, auditing of vendor systems and services, and jurisdiction within which content is stored (see Figure 2).

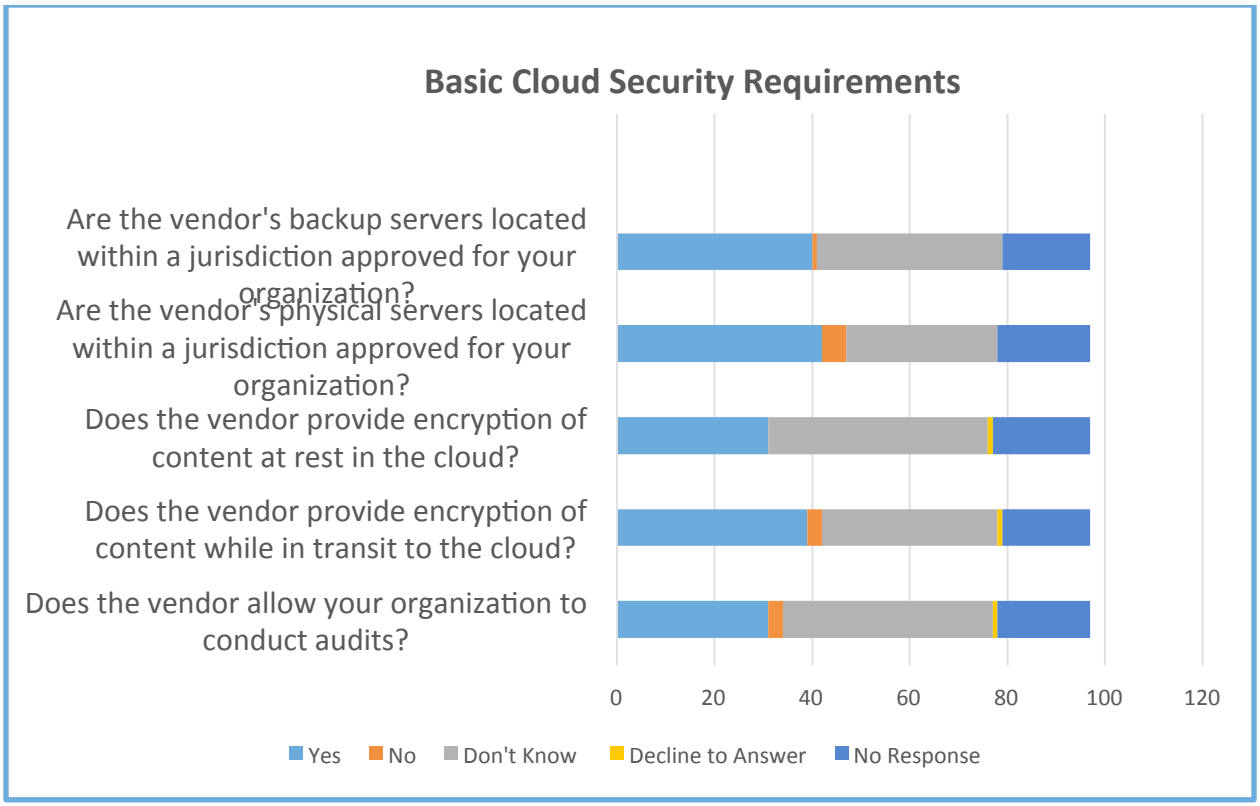

Figure 2: Basic Cloud Security Requirements Met by Cloud Vendors.

The responses revealed that more physical servers are located within an organization-approved jurisdiction than are backup servers. In addition, more respondents indicated that content is encrypted while in transit to the cloud than when at rest in the cloud. Only 32% of respondents stated that their cloud vendor allows the company to conduct audits, and a much smaller percentage, 3%, indicated they were not allowed to conduct audits. Notably, a large number of responses to questions about basic cloud security requirements were "don't know." Because cloud computing has become part of an organization's strategic planning fairly recently, records and information managers must become better informed about and more involved in the cloud decisions in the future.

6.2.4 Retention and disposition functionality offered by services in use

A number of questions were directly related to retention and disposition functionality. The responses for each question can be found in the Executive Summary prepared for ARMA International and posted to the InterPARES Trust website. Responses to select questions are provided here as an indicator of the functional requirements necessary for retention and disposition and the perceptions of the respondents related to the availability of those features. Figure 3 illustrates the responses to four questions related to deletion from the system. In this survey, the terms "disposition" and "destruction" are synonymous.

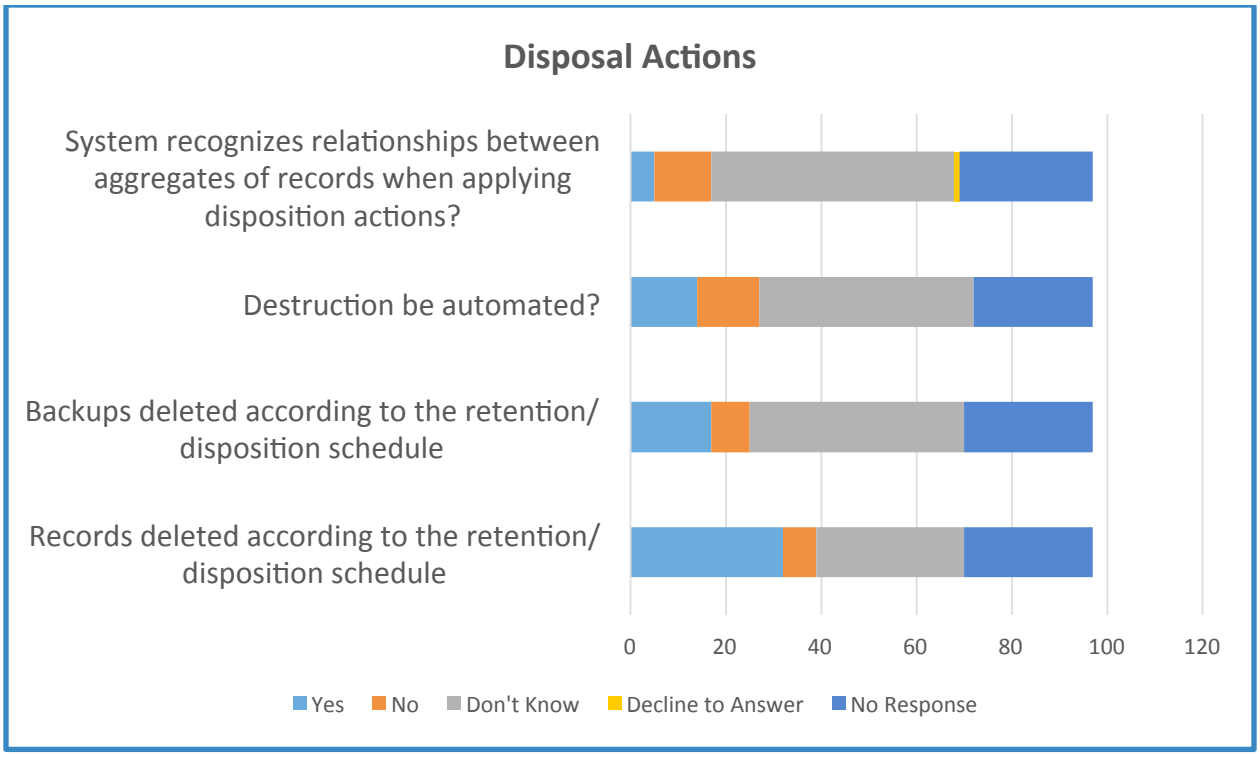

Figure 3: Responses to questions related to disposition of records.

A number of respondents did not answer the technical questions related to disposal actions, and most of those that did respond, did so by indicating "don't know." The question that resulted in the largest number of "yes" responses was a basic one, "Can records be deleted according to the retention/disposition schedule?" Fewer respondents replied yes to a similar question about copies of records on backup servers. Even fewer indicated that destruction could be automated. The lowest number of yes responses was to the question about the system recognizing relationships between aggregates of records when applying disposition actions.

Defensible disposition requires that records of decisions made and actions taken are documented. Several questions were posed related to documentation of those decisions and actions, including the possibility of suspending disposition in the case of an eDiscovery request. Figure 4 provides a summary of the responses to several questions related to overriding the disposition action and providing reports of the actions taken.

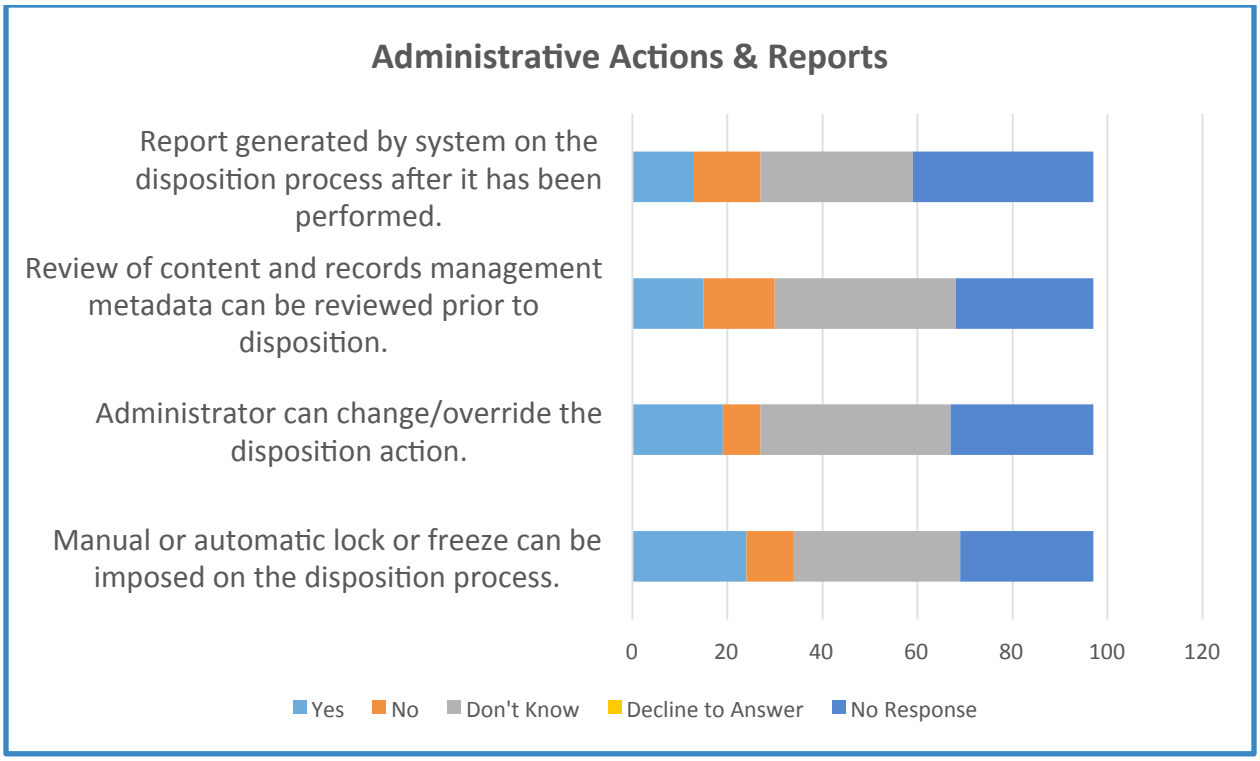

Figure 4: Administrative Actions & Reports

Again, most of the respondents who stated their organization employs cloud services either indicate they don't know the answer to these questions or refrain from responding to the question. Of those that did respond, the largest number state a lock or freeze can be imposed on the disposition process. The functional requirements evaluated through these questions are necessary to complying with eDiscovery requests. When the organization learns that records are likely to be requested for litigation or Freedom of Information requests, there must be a process in place to freeze the disposition process. And if records have been destroyed according to the organization's polices and normal practices, proof of that process must be produced.

The questions summarized in this section are only a selection from the full survey. For additional questions and responses, the reader is directed to the "Retention and Disposition in the Cloud, Executive Summary of Survey Distributed to Members of ARMA International."

7. Discussion

Gartner's hype-cycle model of the evolution of cloud computing characterizes the progression of the technology from user and media enthusiasm through disappointment and eventual understanding and acceptance into productive use. After reaching the peak of inflated expectations in 2009 on Gartner's Hype Curve for Cloud Computing, cloud computing began a long descent into the Trough of Disillusionment. This study was conducted in 2014 and early 2015, when Cloud Computing was at the lowest points on the hype curve (shown in Figure 5).

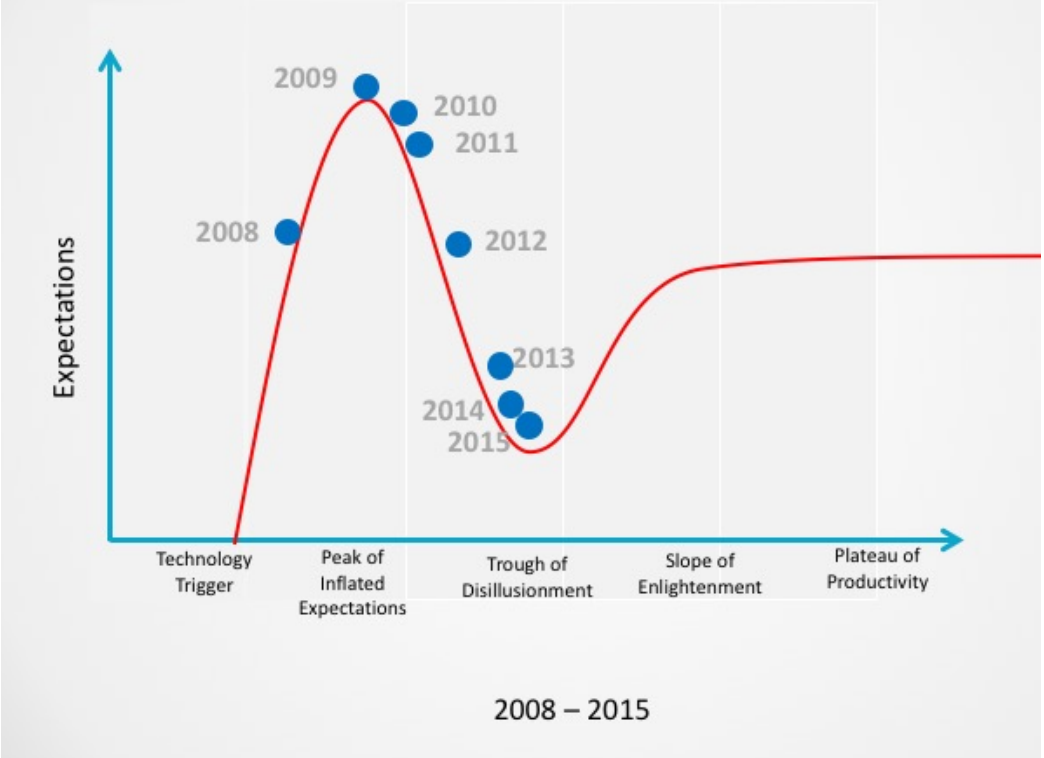

Figure 5: Gartner Hype Curve for Cloud Computing compiled from annual hype cycle reports.

In addition to tracking the term "cloud computing," specific cloud deployment models and service models are also charted, and Gartner's 2015 report placed both Software as a Service and Infrastructure as a Service on an upward trajectory on the Slope of Enlightenment. One SaaS offering, Sales Force Automation, has already entered the Plateau of Productivity. Experts predict that examples of success with cloud initiatives by early adopters will encourage the late majority and laggards to enter the cloud computing market (McCoy, 2015).

7.1 Retention and disposition features included across 20 original services

Further analysis can be conducted by reviewing the two charts in Appendix B. A quick review of the data reveals that least 70 percent of the cloud services offer the following six features. Records can be locked down for viewing only in 85 percent; records could be retained indefinitely in 80 percent of the services; indefinite retention is possible with 80 percent of the services: 75 percent of the services allow records to be deleted according to a records retention and disposition schedule; seventy-five percent provide encryption while data is in transit; and seventy percent allow retention periods to be applied.

Twenty-five percent or fewer of the cloud services investigated possess the following features: storing records management decisions in metadata (25%), presenting electronic aggregations for review along with their records management metadata and disposal authority information so both content and records management metadata can be reviewed (20%), and alerting users to conflicts related to links from records to be deleted to other records aggregations that have different records disposition requirements (10%).

These findings do not imply a failing on the part of the vendors but a difference in purpose that users must understand. Archivematica, for example, is a digital preservation system that stores records indefinitely, so records retention schedules are not considered necessary; however, this functionality can be added by the user through third-party software.

7.2 Similarities and differences among 8 categories of cloud services

It is also important to understand the similarities and differences among cloud services based on category of service provided. For example, two of the three file sharing and storage services (Dropbox for Business and One Drive for Business) allow independent audits of systems and processes; Egnyte does not. Gimmal and Collabware, two records management extenders do not allow vendor audits of systems, but that is because they extend the records management features in Microsoft Office 365/SharePoint Online, which does allow such audits.

Two services in the Litigation Support and eDiscovery category ranked the lowest, with Cloud Nine satisfying only three of the requirements (encryption of data in transit and at rest and locking down records for viewing) and NextPoint satisfying the same three and one additional requirement (support of customer's taxonomy for indexing).

These examples indicate a need to examine each cloud service in depth. There can be vast differences between what seem like similar offerings.

8. Research Limitations

Data gathering from vendors was challenging due to lack of direct responses from the majority contacted and the fact that retention and disposition information was lacking from the materials made publicly available. It is clear that more detailed information on aspects of cloud-based records disposition and its documentation by cloud service vendors is needed. This may also reflect the general role of records management within organizations, where compliance and eDiscovery are driving the need for cloud services. Records management features to support general accountability, overall workflow efficiency, and organizational memory as a component of an archival program framework are considered a part of a niche market. However, movement in the cloud space toward integration of products and services—such as through 'connectors' and Integration Platform as a Service cloud models—makes the implementation of retention and disposition strategies increasingly possible.

The user survey was disseminated to members of a records and information management professional association with approximately 10,000 members, but a disappointingly low response rate (1.68%) resulted. The study reveals user knowledge of cloud-based services employed within their organization, but a majority of response to questions were "don't know." It could be that records and information management professionals are behind their colleagues in understanding the implications of cloud computing on their work. A longitudinal study would be needed to determine if this is the case.

9. Conclusions

The lack of participation by potential survey respondents may reflect skepticism around the promises made for cloud computing and the inability to understand the ramifications for records management programs. The lack of involvement by the majority of survey respondents in cloud computing initiatives may also be reflected in the failure by cloud vendors to address records retention and disposition functionality when describing their products.

A better understanding the retention and disposition functionality needed for compliance and presented in cloud services on the part of both records and information management professionals and vendors will facilitate discussions that can help both parties. Vendors will be able to explain clearly the retention and disposition functionality present in their cloud offerings, and organizations will be able to identify gaps between what is needed and what is offered in order to create defensible retention and disposition programs for content residing in the cloud.

9.1 Best Practices for Retention and Disposition in a cloud environment

A defensible retention and disposition policy must include records and information stored in a cloud environment. Gaps between functionality available in the cloud and the requirements for compliance must be understood. Steps must be taken to mitigate risks related to those gaps. A checklist such as the one used in this study can assist in the evaluation process. Those retention and disposition features offered will vary depending on the type of cloud service model employed.

The decision to move to employ a cloud service should include communication among the potential service provider, upper level management with decision-making authority, IT, and RIM professionals. Planning and preparation is an essential but sometimes ignored step in moving to the cloud. Organizations need to balance needs for RIM functions, IT capacity, and cost in deciding on a cloud provider.

9.2 Recommendations for Vendors

Vendors should be more open and transparent about the exact offerings of their products. Most include terms such as “security” or “flexibility” to describe functionality, without giving more specific capabilities. Descriptions of functionality are particularly lacking for records management features. Vendors should be more aware of records management requirements and promote informed clientele by making existing functions more apparent. Website design is an important part of this as well; it is not always clear where one can find information about specific functionalities, and it may mean that a downloadable pdf that resides behind many nested links is the only way to find that information.

Vendor awareness of records management concerns is essential when providing records services. Providing information to clients about features available to address these concerns can give users confidence in vendor services and avoid possible legal fallout if compliance or privacy protection requirements are neglected. If vendors make records management

functionalities more obvious, then it will also be more obvious to organizations that records managers should be consulted about cloud decisions.

Vendors should consider how they can provide a degree of control over retention and disposition to their clients. The form which this takes may vary between vendors; however, all information stored in the cloud should be connected in a clear and substantial way to the client's tools such as classification schemes and retention schedules, and disposition should be complete, guaranteed, and documented.

Most of the vendors gave generalized descriptions of their overall capability and little detail concerning retention and disposition. Lack of detail may reflect information created for a target audience that is comprised of executive managers as opposed to records managers and archivists. In addition, whether retention and disposition functionality Is integrated into a cloud service depends upon the service model selected. Users should not expect all cloud services to meet all retention and disposition needs, but they should expect cloud vendors to be able to engage records managers in a discussion of retention and disposition capabilities available. A clear, concise statement of how retention and disposition concerns are or are not met by the service is essential for users to identify gaps between what is provide and what is needed and develop a plan to bridge the gaps.

9.3 Recommendations for RIM Professionals

Records managers should be more confident regarding cloud computing. Building knowledge and skills around the cloud can ensure that upper-level management and IT will consult records professionals about cloud storage decisions, which can then guarantee that records management functionalities are considered. If records managers ask records-related questions of cloud vendors, then those providers may be more likely to incorporate those features into their products and, at a minimum, the terminology into their product descriptions.

The lack of retention and disposition functionality does not imply the service should not be used, but it does indicate that the organization will have to develop a plan to govern the records in accordance with retention and disposition requirements regardless. Records managers need to be more aware of the ways in which the cloud affects their work. If RIM professionals consistently do not know the difference between different storage models and the functionality of services currently used by their organization, then it is unlikely that they will be involved in future decisions regarding cloud services.

Corporate culture should be challenged if records managers are consistently left out of decisions which affect their ability to do their job. At the same time, the records manager must make a concerted effort to keep abreast of emerging technology, understand the goals of their organization and how cloud technology can contribute to reaching those goals, and take proactive measures to become involved in information governance programs.

9.3.1 Corporate culture: RIM involvement in cloud decisions

The ARMA survey results demonstrate that RIM professionals are mostly excluded from the

selection of cloud services. This is analogous in general to RIM being excluded from non-cloud based enterprise system selection, and while not surprising, is equally unfortunate.

When asked, "Were you involved in the selection of a cloud provider?" only 18 of the 86 respondents said yes. There were 54 comments, 20 indicating the respondent was excluded from the decision-making process, 11 were substantially involved in the process, and 9 joined the firm after the decision had been made.

In addition, the survey asked if retention and disposition considerations were included in the initial decision to use specific cloud services. The minority of respondents (24 of 79 answering this question) indicated yes; this indicates that some organizations allowed indirect input on records management issues, even if the respondents were not directly involved.

If RIM professionals are not given the opportunity to be engaged in the process and R&D functionalities are not included as requirements, we cannot expect that more Cloud Service Providers will add those features to their offerings.

9.3.2 Better understanding of cloud

Cloud services, like many enterprise systems, do not tend to have retention and disposition functionality built in.

We have amassed a set of data on the state of the industry/cloud services in 2014-15; the industry is still in its early years and provides a wide variety of services are available. Unless the vendor specifically targets records management needs, it is likely their services will not provide the level of retention and disposition functionality needed to ensure a defensible retention and disposition program.

10. Related Research Documents and Publications

10.1 Work Products

Several related documents were referred to in this report, such as the complete Literature Review and the Executive Summary of the Retention and Disposition survey.

A complete list of the documents and articles published related to this research project are provided here in chronological order. All but the annotated bibliographies are available at https://interparestrust.org/trust/research_dissemination

- Retention and Disposition in a Cloud Environment – Annotated Bibliography, ver. 1. May 22, 2014.
- Retention and Disposition in a Cloud Environment – Literature Review, ver. 1. July 20, 2014.
- Retention and Disposition in a Cloud Environment – Functional Requirements. March 2015.
- Retention and Disposition in a Cloud Environment – Annotated Bibliography, ver. 2. May 7, 2015.

- Retention and Disposition in a Cloud Environment – Literature Review, ver. 2. June 2, 2015.
- Retention and Disposition in a Cloud Environment – Executive Summary of User Survey. July 18, 2015.

10.2 Dissemination

The following is a complete list to date of articles published and presentations made to disseminate information (in reverse chronological order):

- Franks, P. C. Perceived & Actual Cloud Records Retention & Disposition Challenges Facing Organizations Today, ICCSM 2015, Tacoma, Washington, October 22-23, 2015 (paper & presentation)
- Franks, P. C. Digital Preservation in the Cloud, CNYARMA October Training Event, October 15, 2015 (presentation)
- Franks, P. C. Evaluating Cloud Services Using Retention and Disposition Requirements, ARMA LIVE! 2015 Conference & Expo in Washington, D.C, October 5-7, 2015 (presentation)
- Franks, P. C. Government Use of Cloud-based Long Term Digital Preservation as a: An Exploratory Study, Digital Heritage (Conference), Granada Spain, September 28-October 2, 2015 (paper & presentation)
- Franks, P. C. (panelist). Recordkeeping in the Cloud and the Advent of Big/Open Data: Mission Critical, or Mission Impossible? ARCHIVES 2015 (SAA), August 22, 2015 (I-trust panel presentation)
- Franks, P. C. New Technologies, New Challenges: Records Retention and Disposition in a Cloud Environment, Canadian Journal of Information and Library Science, June 2015. (paper)
- Doyle, A. and Franks, P. C. "Retention and Disposition in the Cloud—Do You Really Have Control?" Included in the Conference Proceedings of ICCSM 2014 International Conference on Cloud Security Management, Reading, UK, 23-24 October 2014. (paper & presentation)
- Franks, P. C. Records Retention and Disposition in a Cloud Environment: Are You in Control? Invited speaker at InfoGovCon2014, Hartford, CT. (paper & presentation)
- Franks, P. C. Retention and Disposition in a Cloud Environment: Issues and Challenges. Paper presented at the NIRMA - Nuclear Information Management Conference 2014, Summerlin, NV. (presentation)

Dissemination will continue. Two presentations are scheduled (see below); others in the planning stages.

- Franks, P. C. *Capitalizing on the Cloud* (Invited Speaker), 2016 NYALGRO School, Villa Roma Resort, Callicoon, NY, June 7, 2016.
- Franks, P. C. *We've figured out our SIPs and AIPs and now it's time to deal with our DIPs* (Panel presentation), SAA's Archives*Records 2016, Atlanta, GA, July 31-Aug. 6, 2016.

10.3 Related Research

Almost 100 individual projects have been launched under the larger research agenda of InterPARES Trust. Several related directly to cloud computing are in progress or have been completed. Final reports are available through the InterPARES Trust website for the following related research:

- Checklist for Cloud Service Contracts
- Contract Terms with Cloud Service Providers
- Historical Study of Cloud-based Services

11. Further Research

This project team has completed its work. These recommendations are provided for consideration by future researchers.

Further research on trends in cloud functionality could reveal directions of service providers and their offerings, such as whether or not records management needs are addressed in publicly available information.

Research on organizational culture and the role of records managers in decision making could be effective in showing how RIM professionals could become more involved in evaluating cloud computing technology. This could be argued to be a professional duty of records managers.

Case studies describing how records managers conduct their tasks in the cloud environment may assist uses in understanding how the work is affected by the new environment.

Further research into specific sub-technologies of cloud computing—such as Disaster Recovery as a Service (DRaaS), Business Process as a Service (BPaaS), Hybrid Cloud Computing, and Data Warehousing and Advanced Analytics—could assist records and information managers to better understand the retention and disposition functionalities present, to identify the gaps between those that are offered and those necessary, and to develop a strategy for a defensible retention and disposition policy that will include content residing in those cloud offerings.

References

Burda, D. & Teuteberg, F. "The Role of Trust and Risk Perceptions in Cloud Archiving – Results from an Empirical Study." *The Journal of High Technology Management Research, 25,* no. 2 (2014): 172-187. DOI: 10.1016/j.hitech.2014.07.008.

Dutta, A., G. Peng, and A. Choudhary. "Risks in enterprise cloud computing: The perspective of it experts." *The Journal of Computer Information Systems* 53, no. 4 (2013): 39-48.

Gartner Research. [Online}. Available: http://www.gartner.com/technology/research.jsp

Goh, E. "Clear skies or cloudy forecast?: Legal challenges in the management and acquisition of audiovisual materials in the cloud." *Records Management Journal, 24*, no. 1 (2014): 56-73. DOI: 10.1108/RMJ-01-2014-0001.

Gold, J. "Protection in the cloud: Risk management and insurance for cloud computing." *Journal of Internet Law* 15, no. 12 (2012): 1-28.

Grounds, Alison and Ben Cheesbro. "Cloud Control: eDiscovery and Litigation Concerns with Cloud Computing." *The Computer and Internet Lawyer* 30, no. 9 (2013): 23-31.

Pearson, Siani. "Towards Accountability in the Cloud." *IEEE Internet Computing* 15, no. 4 (2011): 64-69.

InterPARES Trust. (2016, February 26). Checklist for Cloud Service Contracts. [Online]. Available: https://interparestrust.org/assets/public/dissemination/NA14_20160226_CloudServiceProviderContracts_Checklist_Final.pdf

InterPARES Trust. (2016, January 30). Contract Terms with Cloud Service Providers. [Online]. Available https://interparestrust.org/assets/public/dissemination/NA10_20160130_ContractTerms_InternationalPlenary3_FinalReport_Final.pdf

InterPARES Trust. (2015, January 8). Historical Study of Cloud-based Services. [Online]. Available: https://interparestrust.org/assets/public/dissemination/NA11_20150109_HistoricalStudyCloudServices_InternationalPlenary2_Report_Final.pdf

InterPARES Trust. (2014, July 20). Literature Review for Retention & Disposition in a Cloud Environment. [Online]. Available: https://interparestrust.org/assets/public/dissemination/NA06_20150602_RetentionDispositionClouds_LiteratureReview_v1.pdf

InterPARES Trust. (2015, June 2). Literature Review for Retention & Disposition in a Cloud Environment, Version 2. [Online]. Available: https://interparestrust.org/assets/public/dissemination/NA06_20150602_RetentionDispositionClouds_LiteratureReview_v2.pdf

InterPARES Trust. (2015). Retention and Disposition in the Cloud: Executive Summary of Survey Distributed to Members of ARMA International. [Online]. Available: https://interparestrust.org/assets/public/dissemination/NA06_20150331_RetentionDispositionClouds_ExecutiveSummary_Report_Final.pdf

McCoy, Mary. (2015, December 21). Top 2016 Cloud Computing Predictions Straight from IT Experts. MSP Blog [Online]. Available: https://blog.continuum.net/top-2016-cloud-computing-predictions-straight-from-it-experts

Weins, Kim. (2016, February 9). Cloud Computing Trends: 2016 State of the Cloud Survey. [Online]. Available: http://www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2016-state-cloud-survey#hybridcloudadoption

Appendix A

Retention & Disposition Functional Requirements

Questionnaire for use when evaluating specific cloud products/services

No.	Questions	Yes	No	Don't Know
Privacy and Security Considerations				
1	Does the vendor allow independent audits of systems and processes?			
2	Is the content encrypted when in transit to the cloud?			
3	Is the content encrypted when at rest in the cloud?			
4	Are the physical servers located within a jurisdiction approved for your organization?			
5	Are the backup servers located within a jurisdiction approved for your organization?			
Establishing disposition authorities				
6	What indexing capability is supported (can it accommodate customers' taxonomy for indexing)?			
7	Can retention periods be applied?			
8	Can destruction be automated?			
Applying disposition authorities				
9	Can a disposition authority (retention and disposition specifications) be applied to aggregations of records?			
10	Can records be locked down for viewing only?			
11	Can records be retained indefinitely?			
12	Can records not in an aggregation be destroyed at a future date?			
13	Can records not in an aggregation be transferred at a future date?			
Executing disposition authorities				
14	Can records be deleted according to the retention/disposition schedule?			
15	Can backups be deleted according to the retention/disposition schedule?			
16	Are users alerted to conflicts related to links from records to be deleted to other records aggregations that have different records disposition requirements?			
17	If more than one disposal authority is associated with an aggregation of records, can these multiple retention requirements be tracked to allow the manual or automatic lock or freeze on the process (ex. Freeze for litigation or freedom of information request)?			
Documenting disposal actions				
18	Are disposal actions documented in process metadata?			
19	Can all disposal actions be automatically recorded and reported to the administrator?			
Reviewing disposition				
20	Are electronic aggregations presented for review along with their records management metadata and disposal authority information so both content and records management metadata can be reviewed?			
21	Can records be marked for destruction, transfer, further review?			
22	Are all decisions made during review stored in metadata?			
23	Can the system generate reports on the disposition process?			
24	Is the ability to interface with workflow facility to support scheduling, review, and export transfer processes provided or supported?			
Integration				
25	Is the metadata schema compatible with other systems, such as Enterprise Content Management or Records Management Systems?			

Appendix B

Gap Analysis – page 1

Category based on business model	File sharing & storage			Records Management Extender		IaaS/PaaS/Managed Services				Litigation Support & e-discovery	
Cloud Vendors	Dropbox for Business	Egnyte	One Drive for Business	Collabware	Gimmal	Amazon Web Services	Century Link (Tier 3)	DataPipe (GoGrid)	Rackspace	Cloud Nine	Next Point
Functional Requirements											
Privacy & Security Considerations (1-5)											
Does the vendor allow independent audits of systems and processes?	Y	P	Y	0	0	0	Y	Y	Y	0	0
Is the content encrypted when in transit to the cloud?	Y	Y	Y	0	0	Y	Y	N	Y	Y	Y
Is the content encrypted when at rest in the cloud?	Y	Y	N	0	0	Y	Y	N	Y	Y	Y
Are the physical servers located within a jurisdiction approved for your organization?	Y	N	Y	0	0	N	Y	0	N	N	N
Are the backup servers located within a jurisdiction approved for your organization?	Y	N	Y	0	0	N	Y	0	N	N	N
Disposition Authorities (6-17)											
indexing)?	Y	0	N	Y	Y	0	Y	Y	Y	0	Y
Can retention periods be applied?	N	0	Y	Y	Y	Y	Y	Y	Y	N	0
Can destruction be automated?	N	0	N	Y	Y	Y	Y	0	Y	0	0
Can a disposition authority (retention and disposition specifications) be applied to aggregations of records?	N	0	N	Y	Y	Y	Y	0	Y	0	0
Can records be locked down for viewing only?	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Can records be retained indefinitely?	Y	Y	Y	Y	Y	Y	Y	N	Y	0	0
Can records not in an aggregation be destroyed at a future date?	Y	0	Y	Y	Y	0	Y	0	Y	0	0
Can records not in an aggregation be transferred at a future date?	Y	0	Y	Y	Y	0	Y	0	0	0	0
Can records be deleted according to the retention/disposition schedule?	Y	Y	Y	Y	Y	Y	Y	0	Y	0	0
Can backups be deleted according to the retention/disposition schedule?	Y	Y	Y	Y	Y	0	Y	Y	Y	0	0
Are users alerted to conflicts related to links from records to be deleted to other records aggregations that have different records disposition requirements?	N	0	N	0	0	0	N	0	0	N	0
If more than one disposal authority is associated with an aggregation of records, can these multiple retention requirements be tracked to allow the manual or automatic lock or freeze on the process (ex. Freeze for litigation or freedom of information request)?	N	0	N	Y	Y	0	N	N	0	N	0
Disposal Actions & Reports (18-24)											
Are disposal actions documented in process metadata?	Y	Y	N	Y	Y	0	Y	N	Y	0	0
Can all disposal actions be automatically recorded and reported to the administrator?	Y	Y	N	Y	Y	0	Y	N	Y	0	0
Are electronic aggregations presented for review along with their records management metadata and disposal authority information so both content and records management metadata can be reviewed?	0	0	N	0	0	0	N	N	Y	0	0
Can records be marked for destruction, transfer, further review?	Y	0	0	Y	Y	0	N	N	0	0	0
Are all decisions made during review stored in metadata?	Y	0	N	Y	0	0	0	N	Y	0	0
Can the system generate reports on the disposition process?	Y	Y	N	Y	Y	0	Y	N	Y	0	0
Is the ability to interface with workflow facility to support scheduling, review, and export transfer processes provided or supported?	Y	0	N	Y	Y	0	0	N	Y	0	0
Integration (25)											
Is the metadata schema compatible with other systems, such as Enterprise Content Management or Records Management Systems?	O	Y	N	Y	Y	0	0	0	Y	0	0
	18	10	11	18	17	8	18	5	19	3	4

Appendix B

Gap Analysis – page 2

Category based on business model	Archiving Solution				ECM	Long-term Digital Preservation		Backup & Data Protection	
Cloud Vendors	Smarsh	Archives Social	Google Vault (email & chats)	Symantec Enterprise Vault	Office 365/SharePoint Online	Archivematics	Preservica	CrashPlan	HP Autonomy Cloud Services
Functional Requirements									
Privacy & Security Considerations (1-5)									
Does the vendor allow independent audits of systems and processes?	0	0	Y	Y	Y	Y	0	Y	0
Is the content encrypted when in transit to the cloud?	Y	Y	Y	Y	Y	0	0	Y	Y
Is the content encrypted when at rest in the cloud?	0	N	Y	Y	N	0	0	Y	Y
Are the physical servers located within a jurisdiction approved for your organization?	0	Y	N	0	Y	Y	N	Y	Y
Are the backup servers located within a jurisdiction approved for your organization?	0	Y	N	0	Y	Y	N	0	Y
Disposition Authorities (6-17)									
indexing)?	0	Y	Y	Y	Y	0	Y	0	N
Can retention periods be applied?	Y	Y	Y	Y	Y	0	0	Y	Y
Can destruction be automated?	0	N	Y	Y	Y	0	0	Y	0
Can a disposition authority (retention and disposition specifications) be applied to aggregations of records?	0	Y	Y	Y	0	0	0	Y	0
Can records be locked down for viewing only?	Y	Y	0	Y	Y	0	0	Y	Y
Can records be retained indefinitely?	Y	Y	Y	Y	Y	0	Y	Y	Y
Can records not in an aggregation be destroyed at a future date?	0	Y	Y	Y	Y	0	0	0	0
Can records not in an aggregation be transferred at a future date?	0	Y	0	Y	Y	0	0	0	0
Can records be deleted according to the retention/disposition schedule?	Y	Y	Y	Y	Y	0	0	Y	Y
Can backups be deleted according to the retention/disposition schedule?	0	N	Y	Y	0	0	0	Y	Y
Are users alerted to conflicts related to links from records to be deleted to other records aggregations that have different records disposition requirements?	N	Y	Y	0	0	0	0	0	0
If more than one disposal authority is associated with an aggregation of records, can these multiple retention requirements be tracked to allow the manual or automatic lock or freeze on the process (ex. Freeze for litigation or freedom of information request)?	N	0	Y	Y	Y	0	0	Y	0
Disposal Actions & Reports (18-24)									
Are disposal actions documented in process metadata?	0	Y	Y	0	Y	Y	Y	Y	0
Can all disposal actions be automatically recorded and reported to the administrator?	Y	Y	Y	0	0	Y	Y	Y	0
Are electronic aggregations presented for review along with their records management metadata and disposal authority information so both content and records management metadata can be reviewed?	0	0	Y	0	0	Y	Y	0	0
Can records be marked for destruction, transfer, further review?	0	N	Y	0	Y	0	0	Y	0
Are all decisions made during review stored in metadata?	0	N	0	0	0	Y	Y	0	0
Can the system generate reports on the disposition process?	Y	Y	Y	0	Y	Y	Y	Y	0
Is the ability to interface with workflow facility to support scheduling, review, and export transfer processes provided or supported?	0	N	Y	0	Y	0	Y	Y	0
Integration (25)									
Is the metadata schema compatible with other systems, such as Enterprise Content Management or Records Management Systems?	0	0	0	0	Y	Y	Y	0	0
	7	15	19	14	18	9	9	17	9