InterPARES Trust Project

Final Report

Title:		10-Contract Terms with Cloud Service Providers
Status:		Draft (restricted)
Version:		2
Date submitted:		2014-05-18
Last reviewed:		
Author:		InterPARES Trust Project
Writer(s):		Robert McLelland and Grant Hurley with additional contributions from Daniel Collins
Research domain:		Infrastructure
URL:		
Project lead		Yvette Hackett

Document Control

Version history			
Version	Date	By	Version notes
1.0	Feb 12, 2014	YH, GH, RM	Drafted and submitted
1.0	Feb 15, 2014	CR	Formatted, minor copy edits
2.0	May 18, 2014	RM	Changed category group names, added discussion on European cloud service providers, added analysis of European contacts, enhanced conclusion paragraph.

Table of Contents

1. Introduction

The growing popularity of the cloud in business and personal life is difficult to dispute. Google alone claims on its cloud services webpage that over 5 million businesses are subscribers to Google Apps.[1] Additionally, in 2010, a study by the Poneman Institute found that 56% of IT practitioners surveyed worked for organizations that were actively utilizing the cloud in some capacity.[2] With increasing regularity individuals and organizations have begun to adopt the services that are universally referred to as the cloud. This generally involves client acceptance of a contract that establishes the terms and conditions by which the service provider will provide access to the cloud services. While agreement with these contracts is often as simple as clicking a mouse, the ramifications for the records that may be stored in this environment is not. Presently, the terms established and how they relate to the concerns of records management professionals is not well documented, limiting the ability to work effectively towards agreements that protect the trustworthiness of records.

2. Purpose and Scope of Study

This study was designed to identify the types of terms, as well as the gaps, that currently exist in contracts between cloud service providers and their clients across multiple jurisdictions. In addition, the research would identify an array of Records and Information Management (RIM) concerns that were specific enough to reflect the needs of records managers attempting to work in the cloud. See the original project proposal in Appendix A.

3. Methodology

A number of approaches were used to identify the needs that cloud service providers should address in their contracts. Information technology and recordkeeping issues were identified through a literature review. These included how cloud services were organized and offered for sale as well as the translation of recordkeeping requirements into the cloud. Sources included ARMA International, advice generated by the National Archives of Australia and the United States and ISO standards. See the annotated bibliography in Appendix B.

Once relevant concepts were identified, they were placed in a table designed to facilitate comparisons among the service providers. This section of the review shows that concerns expressed by records managers, as expected, tended to be more or less

[1] Google, "Over 5 million businesses have gone Google." Accessed January 17, 2014. http://www.google.com/enterprise/apps/business/customers.html.

[2] Ponemon Institute LLC, "Flying Blind in the Cloud: The State of Information Governance." Last modified 2010. Accessed November 17, 2012. http://eval.symantec.com/mktginfo/enterprise/white_papers/b-ponemon_institute_flying_blind_in_the_cloud_WP.en-us.pdf. This study was undertaken by the Poneman Institute on behalf of Symantec, Inc.

uniform.

A search for legal cases was also undertaken, to learn whether cloud contracting activities had already resulted in litigation. Issues which were identified as a result were matched to the comparison table to ensure that they were also represented.

Finally, service providers from the United States, Canada, and the European Union were chosen based on a combination of their high profile among consumers and the availability of contracts on their websites. These were reviewed to confirm the extent to which recordkeeping issues were addressed in the existing agreements. An overview of each company's services is provided in Section 8 of this report.

4. Overview of the Cloud

4.1 Types of Cloud

Although the term "the cloud" appears straightforward, the reality is that it is a single term used to describe a multitude of different services and technologies. A cloud may be implemented for a client in any of four different ways.[3]

The first possible implementation is a "public" cloud. Here the word "public" does not refer to government agencies but rather to an infrastructure that is shared by all clients of a service provider. In this public cloud, all clients' information is stored together, with only logical separations to distinguish one from the other. This form of cloud service is commonly accessed remotely.[4]

The next type of cloud service implementation is a "private" cloud. Again, this term describes the number of clients who access the infrastructure. In this model, only the client who is purchasing the service would have its information stored in the infrastructure, which would be physically isolated from that of other clients. This type of implementation can be provided remotely but it may also be provided at the client's site.[5] It may even be owned and administered by the client for its employees. This model, particularly if it is owned and maintained by the client itself, is more expensive than the public model, but can offer better guarantees of security and privacy.

The third type of cloud implementation that is available is a "hybrid" cloud. In this model, some of the infrastructure would be the shared space of the public model and some

[3] Hickling Arthurs Low Science & Technology Policy Research and Analysis Resource team, "Primer on Policy Implications of Cloud Computing," *Government of Canada* (2012), p. 2. Also Rackspace Inc., "Understanding The Cloud Computing Stack SaaS, Paas, IaaS," *CloudU* (2011), p. 3. And Frederick Barnes. ARMA International, "Putting a Lock on Cloud-Based Information." Last modified 2010. Accessed January 17, 2014. http://content.arma.org/imm/JulyAug10/IMM0710puttingalockoncloud-basedinformation.aspx.

[4] Hickling Arthurs Low, p. 5. Also Barnes.

[5] Ibid. Also Barnes

would be the isolated infrastructure of the private model.[6] This model is appropriate when some client information is more sensitive, requiring storage in higher cost private space while less sensitive information can be kept in less expensive but more public space.

The final type of cloud is referred to as a "community cloud," where a specified group of clients all share the same cloud service. [7] In this way, the clients can ensure that their information is not being stored with other unknown organizations but can still gain the purported benefits of sharing the burden of cost. This implementation could also enable information sharing between organizations with shared interests or data uses.

The cloud providers examined in this study tended to offer all of these forms of implementation. The most common, however, was that of the public model, most likely due to the cost savings it promises clients.

4.2 Types of Cloud Services

In general, the cloud service industry offers four types of services - Infrastructure as a Service, Software as a Service, Platform as a Service and, less commonly, Data as a Service.[8]

Infrastructure as a Service (IaaS) refers to the provision of access to hardware (e.g. hard disks, servers, etc.).[9] This service allows the client to rent, rather than purchase IT infrastructure on an as-needed basis, allowing it to easily and quickly increase infrastructure capacity when required. The most commonly promoted benefit of this service is the cost saving to the client who no longer needs to purchase and maintain infrastructure. This "rented" infrastructure can then be accessed remotely by members of the client organization.

Software as a Service (SaaS) refers to a service which allows the client to remotely access software that is hosted on infrastructure owned and maintained by the service provider.[10] This service enables a client organization to use software that might otherwise be too expensive to purchase, install, maintain, and update itself.

The third type of cloud computing is Platform-as-a-Service (PaaS). This service provides the client with an environment for creating and running its own software.[11] This has been done, for example, by Google in its Google Apps platform, which allows

---

[6] Ibid. Also Barnes

[7] Ibid. Also Barnes

[8] Hickling Arthurs Low Science & Technology Policy Research and Analysis Resource team, "Primer on Policy Implications of Cloud Computing," *Government of Canada* (2012), p. 2. Also Rackspace Inc., "Understanding The Cloud Computing Stack SaaS, Paas, IaaS," *CloudU* (2011), p. 3.

[9] Hickling Arthurs Low, p. 3. Also Barnes.

[10] Hickling Arthurs Low, p. 3 Also Barnes.

[11] Ibid. Also Barnes

developers to create software that can run on devices using Google operating systems such as Android.[12] This is again meant to save the client the cost of owning and running an environment that supports such activities.

A fourth type of cloud service has been dubbed Data as a Service (DaaS). This type "is typically implemented within a SaaS, PaaS or IaaS solution and provides (often spatial) data within applications that support more specialized data discovery, access, manipulation, and use."[13]

These four types of clouds and four different services can be implemented in any number of combinations, for example software being provided in cloud-based platforms through rented infrastructure.[14] This report focuses primarily on cloud infrastructure and the storage of records therein, which would form the central part of most recordkeeping initiatives.

4.3 Types of Contracts

There is lack of uniformity within cloud contracts themselves. Many providers use a tiered contract structure, with an overarching contract supplemented by several more specific agreements.

The "Terms and Conditions (TaC)," "Terms of Service (ToS)," or similarly named document TaC may contain more general clauses that would encompass all of the services that a provider offers, such as conditions for service termination, legal protections for the service provider in terms of content uploaded by the client, and copyright terms. In general, these contracts describe the client's obligations when using the service, and they are clearly meant to protect the service provider more than the client.

Service Level Agreements (SLA), on the other hand tend to contain more specific terms relating to particular services. A study by IBM Research on SLAs identified terms such as "service guarantee metrics" which quantify "availability (e.g., 99.9%), response time (e.g., less than 50ms), disaster recovery and fault resolution time (e.g., within one hour of detection) and how compensation will be calculated and reimbursed for a fault in service.[15] Availability or uptime can be offered based on a tiered payment structure. The SLAs also tend to offer service guarantees on a basis of time periods as well as at different granularities. For example, time periods may be measured in requests to the service per minute, hour, day, week, etc., and service interruption may be measured by

[12] Google Inc., "App Engine." Accessed February 3, 2014. https://cloud.google.com/products/app-engine/?utm_source=google&utm_medium=cpc&utm_campaign=appengine-search&gclid=CPHg26nVsbwCFY1FMgodjR8AKw.

[13] Hickling Arthurs Low, p. 3.

[14] Ibid.

[15] Salman Baset, "Cloud SLAs: Present and Future," *ACM SIGOPS Operating Systems Review*, 46, no. 2 (2012): 57-66, p. 57

service, data centre, etc.[16]

In addition to these, SLAs may contain exclusions for service outages,[17] the most common one being planned system maintenance. In all of the SLAs examined in this and the IBM report, the result of unavailable service was a credit applied to the clients' next bill.[18] Interestingly, all the SLAs placed the burden of reporting outages in order to claim a credit on the client.[19]

Finally, some services available at a provider's site may not be covered in any of the contract tiers. Clients use these services at their own peril.

Despite the prevalence of this tiered contract structure, there is little that is standardized about the contracts. Not every service provider has both a ToS/TaC and SLAs. Some providers have a ToS/TaC and only SLAs for particular services; some have only ToS/TaCs. It is not always immediately apparent how many contracts a service provider requires. When contracts are available on a service provider's website, they are often difficult to find, though presumably they would be presented to a client as a part of the "signup" process.

Contracts also can change quickly and the non-static nature of these contracts could cause problems. Most contracts require the provider to notify the client of any changes to the contract. While this could not be tested in the course of this project, clients should learn whether cloud service providers have adopted the same notification method as many large organizations, such as banks, credit card companies and social media sites. They notify the client that changes have occurred, but leave it to the client to discover the nature of the changes and their potential impact.

5. Literature Review

There was some overlap between the information technology literature and the records management literature, with a shared interest in:

- Storage specifications (primarily hardware)
- Security of the infrastructure (both physical and technological)
- Access authority
- Data segregation (physical)
- Regularity of access

[16] Ibid. p. 58

[17] Ibid.

[18] Ibid. Rackspace, for example, offers a higher percentage of its clients' last billed fee as a credit on the clients' next bill, 10% credit is offered for 99.89-99.5% availability on a scale up to 100% credit for less than 96.5% availability for some services. Rackspace US Inc, "Cloud Files SLA." Last modified January 21, 2011. Accessed January 24, 2014. http://www.rackspace.com/information/legal/cloud/sla.

[19] Ibid. p. 62

Articles aimed at RIM professionals suggested that, prior to entering into a cloud service, their organization would need also need to know:

- Disposal scheduling and proper disposal methods
- Jurisdiction of storage
- Records loss or premature destruction
- Loss of value as evidence
- Long-term viability
- Loss of confidentiality/protection of privacy.

These concerns mirror requirements set forth in many guidelines, principles, best practices, and standards within the profession. ISO 15489, for example, lays out what a recordkeeping system should contain, including elements such as the ability to retain and properly dispose of records at any time and in a way that permits audit trails, requirements for physical protection of records media, timely and efficient access, and capture and classification.[20] The ARMA International Generally Accepted Recordkeeping Principles, meanwhile, lays out eight principles that are necessary for a strong recordkeeping system: accountability, integrity, protection, compliance, availability, retention, disposition, and transparency.[21] All of these principles and requirements would still be necessary in a cloud storage system and would therefore need to be addressed in contract clauses.

Ultimately, fifteen contract term categories were identified. These term types were placed into four groups with other logically similar categories.

Group 1, for example, includes all contract term categories related to the ability to destroy records. This group could not be encompassed by just one category, as the literature tended to have different apprehensions related to destruction: RIM professionals were concerned with destruction as part of a retention and disposition policy, as well as ensuring no copies would remain with the service provider at the end of the contract.

Group 2, meanwhile, was used to encompass different situations that affect a client's ability to access records whenever necessary, and how such access will be ensured.

Group 3 encompasses term categories that deal with a client's ability to trust the records that are stored within the cloud service.

Finally, Group 4 covers a client's control over records and the information contained within them such as their legal rights over the information and their responsibilities to

[20] *ISO 15489 - Information and Documentation - Records Management*, (International Standards Organization, 2001), p. 10-16.

[21] ARMA International, "ARMA Generally Accepted Record Keeping Principles." Last modified 2014. Accessed January 20, 2014. http://www.arma.org/r2/generally-accepted-br-recordkeeping-principles.

protect personal information.

6. Legal Cases

Few cases were found which specifically addressed the recent “cloud service” developments. Seven legal cases, all from the United States, did identify recordkeeping concerns that could apply in a cloud environment. These were divided into three categories – Privacy, Storage and Copyright, and Jurisdiction. Detailed summaries of each case are available in Appendix C.

6.1 Privacy

In a 1976 Supreme Court ruling (United States v. Mitch Miller), a bank provided records requested by authorities conducting an investigation into tax evasion. The judged ruled that this was not an unreasonable search because the information had been provided to a third party and as such, was not protected.

A 2008 Oregon Court of Appeals case involved information stored on a computer which was handed over to a repairman. The repairman copied information to provide to the police, resulting in charges against the computer owner. In this case, the ruling said the owner of the information did have an expectation of privacy when the computer was in the hands of a third party.

In the third case, heard by the Georgia Court of Appeals in 2010, the court ruled that there was no expectation of privacy in the content of e-mails because they had been sent.

Two of these three rulings suggest that an individual’s right to privacy is lost if the information is turned over to a third party. The implications of this ruling are major for cloud computing if data sent voluntarily to the cloud is no longer protected in the United States, for example, by Acts such as the Electronic Communications Privacy Act (ECPA), the Privacy Protections Act (PPA), or the First or Fourth Amendments. Users would need to guard against this before entering into cloud services contracts.

6.2 Storage and Copyright

The first case in this category, heard in California District Court in 2007, dealt with whether the content of server logs containing information about website downloads had to be produced, even though they were in the hands of a third-party contractor. The Court found that the defendant had intentionally routed the data through the third party and therefore was still in “possession, custody and/or control” of the data.

The second case, from the United States Court of Appeal in 2008, concerned a copyright owner who objected to the distribution method used by a cable network provider because it allowed viewers to make a copy of the material and view it multiple

times, a potential copyright infringement. The Court ruled against the copyright owner because the transaction between the cable company and its client did not constitute "public" distribution. The Court also felt that the "copy" held by the cable company's client was not a genuine copy because of the way it came into existence, raising questions about the definition of "fixity" as it concerns digital files.

A 2009 case from the District Court of New York dealt with a bulletin board website which allowed the sharing of files, including material copyrighted by the complainant. Similar to earlier cases like Napster, the Court found the website had encouraged copyright infringement and was ordered to shut down operations.

All three cases touch on elements of service now offered in a cloud environment, including the sharing of a client's files with others, the creation of copies by various methods, and the possibility of copyright infringement.

6.3 Jurisdiction

A 2001 case in the Ontario Court of Appeal dealt with cross-border advertising and selling of computers. Advertising on an American website directed to American consumers caused Canadian shoppers to crash the website of the Canadian company that controlled the computers' trademark. The initial Court ruling ordered the American company to pay damages to the Canadian company, but was overturned on appeal because the American company was not targeting Canadian consumers.

This decision revolves around the target of the service provider's advertising and its impact on what jurisdiction might apply in the case of subsequent litigation, a scenario equally applicable to cloud service providers.

7. Public Sector Considerations

Public bodies in Canada and the U.S. are also moving to the cloud, driven in part by cuts to IT budgets. Public organizations may also be seeking to improve preservation practices and the storage and management of digital records; and to respond to increasing client demand for instantaneous, networked access to information. However, in the case of a public body, there may be stricter requirements for how their records can be stored, making the agreements offered by cloud services unacceptable for their use. Public sector cloud contract terms could differ from those used by the private sector due to three considerations:

- The freedom of information and privacy legislation of a particular jurisdiction
- A desire for greater standards for security
- The more common use of private or community cloud implementations.

The general situation with various levels of governments and universities was examined to identify current contracting trends, and to locate examples of specific contract terms.

7.1 Federal Governments

Federal governments are necessarily risk averse regarding cloud computing contracts, though potential cost benefits may be seen as outweighing the risks of cloud technology.

7.1.1 Shared Services Canada

Shared Services Canada is currently consolidating federal government storage and e-mail services. Created in 2011, its mandate is to update and centralize government data storage from over 485 outdated data centres located in departments across the country to 7 data centres and to consolidate multiple e-mail services into a single system.

The management of e-mail services was outsourced to Bell Canada and CGI Canada in June 2013. Among the requirements of the system, which is a large private cloud, are:

- Multiple, layered sets of security, including PKI support
- Data sovereignty/territory of storage terms (all systems and infrastructure must reside in Canada)
- A security clearance process for successful bidders completed by the Canadian Industrial Security Directorate
- Records management functions outlined as "dedicated e-mail archiving" and interface support for integration with an Electronic Document and Records Management Systems (EDRMS) solution.

Similarly, data centres will be internally controlled through a private cloud solution. The Canadian Government hosted an Industry Engagement Day in July 2013 to solicit suppliers of data centre technology and applications.[22] Though the tender process has not been initiated, the terms of the contracts will likely resemble those specified for e-mail services.

7.1.2 FedRAMP

The United States launched the Federal Risk and Authorization Management Program (FedRAMP) program as a method of certifying third-party cloud providers (among other IT providers), including providers such as Amazon Web Services and Microsoft Azure. FedRAMP requires a rigorous IT security assessment against the National Institute of Standards and Technology baseline requirements (NIST 8053)[23], the provision of information security documentation and plans, a third-party assessment of a cloud provider's security readiness, followed by testing and final approval. Contracts are then

[22] Industry Engagement Day - GCNet Wan – July 9, 2013. Shared Services Canada. http://www.ssc-spc.gc.ca/pages/telecomm_gcnet-eng.html. Accessed 2014-02-04.

[23] National Intitute of Standards and Technology. Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Revision 4, April 2013, 460 pp., http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf; and Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*, Revision 1, June 2010, 399 pp., http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf, Joint Task Force Transformation Initiative, U.S. Department of Commerce.

awarded on an individual basis between departments and approved providers.

The FedRAMP approval process restricts itself to IT security measures. It does not include records management concerns - these are to be negotiated between each department and their cloud service provider. The National Archives and Records Administration (NARA) served as a consulting body in the 2011 U.S. Federal cloud computing strategy document.[24] NARA had previously issued a Bulletin[25] and developed a Frequently Asked Questions (FAQ) website in 2010[26] on this subject. In 2013, NARA deployed an in-house cloud-based solution for its own operational use, using a combination of Google Apps, Exchange My Mail from Blackberry, and ZL Technologies United Archive.[27]

It is interesting to note the difference between American and Canadian federal government approaches to the implementation of cloud services. In Canada, cloud contract terms will be enforced through the tendering process designed to acquire a single government-wide solution, while the United States is operating a cloud services certification body (FedRAMP) to pre-approve providers with whom individual departments negotiate other specific contract terms depending on the services required.

This parallels the approaches used during the implementation of record and document management systems in the late 1990s. Both federal governments produced design criteria/functional specification documents but the Canadian government acquired a single government-wide solution (the Record, Document and Information Management System (RDIMS) application) through a tendering process, while the United States tested and certified applications against the 5015.2 standard (Design Criteria Standard for Electronic Records Management Software Applications) at the Joint Interoperability Test Command's software certification testing program.

7.2 Provincial/State and Local Governments

As the 2012 U.S. State and Local Government Cloud Commission report, *The Cloud Imperative* outlines state, provincial and local governments are adopting cloud solutions largely on a project or case basis, including e-mail hosting services offered by Google as well as data hosting and management for individual municipal and provincial services. The report identifies five “key contractual terms” that state and local governments should consider when choosing cloud providers:

---

[24] Vivek Kundra. *Federal Cloud Computing Strategy*. February 8, 2011. https://www.dhs.gov/sites/default/files/publications/digital-strategy/federal-cloud-computing-strategy.pdf. Accessed 2014-02-03.

[25] National Archives and Records Administration, Bulletin 2010-05, September 8, 2010. http://www.archives.gov/records-mgmt/bulletins/2010/2010-05.html. Accessed 2014-02-04

[26] National Archives and Records Administration. Frequently Asked Questions about Managing Federal Records in a Cloud Computing Environment. http://www.archives.gov/records-mgmt/faqs/cloud.html. Accessed 2014-02-04

[27] Ruttrell, Yasin. NARA moved email to the cloud at ‘lightning speed’, GCN, December 17, 2013. http://gcn.com/articles/2013/12/17/nara-cloud-email.aspx. Access 2014-01-06

- Asset location and ownership (territory of storage)
- Access to the data (availability and physical security)
- Terms of disentanglement (contract termination)
- Data and asset segregation (the option for private or hybrid clouds)
- Standard pricing models.[28]

While records management issues are not discussed in the report, these identified contract terms implicitly identify terms that relate to the destruction, availability, reliability and control terms previously identified. Of special note is the importance of territory of storage requirements: while U.S. legislation may not specifically require the location of data assets, many agencies require data to be located in the United States, in state, or locally.[29] As in federal deployments, provinces, states and local governments are still required to negotiate any contract terms on an individual basis with providers.

7.2.1 Ontario Geo Portal

The Ontario GeoPortal was developed by Infrastructure Ontario (IO) to consolidate provincial Geographic Information Systems (GIS) data and services. It works on the principle that much information of interest to individuals in government is geographically-based. Therefore, a map interface that allows users to navigate through information spatially is a functional way to organize this information. The portal integrates a variety of database services as well as ESRI GIS products and OpenText and presents it all through a central map interface.

The portal was a partnership between IO and a company called SKE Inc. Hosted in the cloud, the company calls their service "spatial cloud computing" and compares it to similar products such as ArcGIS and Google Maps.[30] The data is hosted in Toronto in data centres originally created for the Geo Portal initiative, with the option to create a hybrid solution using active internal firewalls to strengthen security protections for clients.[31] The portal is made available to government entities other than IO at a monthly subscription cost.

7.3 Universities

Universities have also been active in the United States and Canada implement university services in the cloud and collaborating with third-party industry members. These clouds provide:

---

[28] State & Local Government Cloud Commission (SLG-CC). *The Cloud Imperative: Better Collaboration, Better Service, Better Cost*. February 2012. http://www.techamerica.org/Docs/fileManager.cfm?f=taf_slg_cc.pdf. Accessed 2014-02-04.

[29] Ibid, p 25

[30] Hugh Williams. Spatial Cloud Computing (SC2). White Paper. August 2012. http://www.skeinc.com/pages/Downloads/SC2_White_Paper_August_2012.pdf Accessed 2014-04-02.

[31] "Ontario GeoPortal." http://www.skeinc.com/pages/casestudies/OntarioGeoPortal.html Accessed 2014-04-03.

- E-mail hosting for students, faculty and alumni
- Data centres for storage; and server space
- Specialized software infrastructure for advanced supercomputing.

In the Canadian cases examined, provincial Freedom of Information and Privacy Protection Legislation dictated the terms of the services offered by universities, and therefore, the contractual relationships with third-party providers. For example, Freedom of Information and Protection of Privacy Act legislation for British Columbia and Nova Scotia requires that personal information held by a public body be stored in Canada. Consequently, institutions in these provinces tend towards private/community clouds as detailed below. In provinces without territory of storage legislation, cloud providers need not store data in Canada, though they must remain compliant with other terms in provincial privacy legislation such as security provisions to ensure adequate protection of information.

Institutions in the United States share similar concerns, though territory of storage considerations are less a consequence of Freedom of Information and Privacy Protection legislation than institutional policy and practices.

7.3.1 University of Alberta

The University of Alberta signed a 4-year contract with Google to migrate their campus e-mail. A Privacy Impact Assessment (PIA) was prepared and submitted to the Alberta Office of the Information and Privacy Commissioner, who accepted the University's risk analysis of the situation. The program was implemented in 2011.

E-mails are stored in any one of Google's servers, and may be subject to the U.S. Patriot Act, as the university's Frequently Asked Questions (FAQ) page on the service makes clear.[32] Google agreed that it would not perform data mining on the e-mails or disclose to third parties except where required by law. The FAQ addresses further jurisdictional concerns such as "Does the U.S. Patriot Act allow the U.S. government to access my personal information?" to which the answer is: "Yes. The Patriot Act allows for the U.S. Government to access personal information that is held or accessible by anyone within the United States or any U.S. citizen." The page also confirms that from a "contract point of view, the University of Alberta owns the data. In reality, the University is acting as the custodian for it," but does not specify how Google uses e-mail metadata.

The University retains virtual custody enforced by contract over all of the data stored by Google.[33] Though concerned members of the university community requested to view the contract, Alberta privacy legislation requires that third parties give consent to disclose information; Google declined to give permission to release the contract.[34]

---

[32] "Privacy and Security." http://google.ualberta.ca/en/Privacy.aspx Accessed 2014-02-03.

[33] "Get to know Gmail." http://google.ualberta.ca/en/Get%20to%20Know%20GMail.aspx. Accessed 2014-02-04.

[34] "U of A goes Google." http://www.ualbertablog.ca/2011/03/u-of-goes-

7.3.2 University Consortia

In November 2013, a group of seven Nova Scotia universities opted for a shared community cloud being implemented with IBM for data storage and access, including the use of IBM analytics software through the cloud platform. Servers are to be hosted at Dalhousie University in Halifax.

Similarly, in April 2012, a consortium of seven Ontario universities also signed a contract with IBM for supercomputing and cloud computing purposes. Servers are to be located in Barrie, Ontario and Western University in London, Ontario and accessed solely by the consortium.

7.3.3 Council of Prairie and Pacific University Libraries

The Council of Prairie and Pacific University Libraries (COPPUL) will launch a cloud-based digital preservation service in the spring of 2014. It will be available in three tiers to members, each for a graduated fee subsidized by COPPUL. Service levels range from basic digital backlog management through to comprehensive Archival Information Package (AIP) packaging and Dissemination Information Package (DIP) upload to an access system. The cloud servers will be hosted in Canada and the service will use Archivematica from Artefactual Systemc, Inc., which will also store any data produced by Archivematica and provide support for the live systems.

7.3.4 Educloud

EduCloud is a suite of cloud services currently being developed by the University of British Columbia. The website describes it as a service designed with the higher education environment in mind, meeting all the provincial requirements under B.C. privacy legislation. The EduCloud Server Service, a component of EduCloud, allows resources pooling, server consolidation, regular backups and high availability redundancy, self-management and self-deployment. Other services in development include the Educloud WorkSpace - a Dropbox-like service hosted at UBC, EduCloud Web Hosting, EduCloud Virtual Desktop, and EduCloud Backup and Recovery.[35]

7.3.5 Educause

The organization Educause has produced the most documentation concerning cloud implementation for colleges and universities in the United States. A paper titled “If It’s in the Cloud, Get It on Paper: Cloud Computing Contract Issues” encourages post-secondary school administrators to assess the following contract terms when negotiating with providers:

- Availability (where upwards of 99.9 percent may be necessary for institutional needs);
- Data ownership terms;
- Disposition terms (particularly in the migration of services to other providers;

---

google.html?showComment=1306870544418#c1151421411440664595 Accessed 2014-02-04.

[35] “New Educloud Server Service Now Available.” http://www.it.ubc.ca/news/new-educloud-server-service-now-available Accessed 2014-02-04.

- Territory of storage considerations where foreign laws may apply.

As a cloud computing survey of research labs in the United States compiled by XSEDE reports, cloud services in universities are being negotiated at a highly granular level within institutions, with an emphasis towards computing power, software availability, and data management and analysis as supporting the choice of cloud services.[36] However, contract terms are not addressed in the document.

8. Companies Selected

In the next phase of the research, thirteen companies offering a variety of cloud services were selected for analysis - three American companies, five Canadian companies, and five European companies though several organizations operate in more than one jurisdiction.

When available online, company contracts and agreements were analyzed. In other cases, the promotional material available on the company's website was reviewed. Among the numerous services offered, emphasis was placed on those most likely to support recordkeeping activities, such as storage, access control, and disposition.

8.1 United States

8.1.1 Google

Google, best known for its search engine, also offers a suite of cloud services under the name Google Cloud Platform. They are organized into five categories: Compute, Storage, Big Data, Services, and Developer's Tools.[37] Compute offers the client the ability to utilize Google's infrastructure to run processes that require more computing power than the client possesses and to develop and run applications (apps). Storage allows the client to use Google's infrastructure to store large amounts of data and objects (including records). Big Data provides services to a user to more quickly analyze large amounts of data. Services offers support for clients in running their own apps. Finally, Developer's Tools allow clients to develop apps in various formats.

Google utilizes a two-tier structure for agreements related to its services. The primary document is the Google Cloud Platform Terms and Conditions, which is an overarching document that governs all of the services Google offers. Next, Google requires its clients to accept Service Level Agreements for each individual service they subscribe to. This project analyzed the Google Cloud Platform Terms and Conditions and the Google Cloud Storage Service Level Agreement.

8.1.2 Amazon

[36] David Lifka et. al. *XSEDE Cloud Survey Report*. September 2013. http://net.educause.edu/ir/library/pdf/CSD6239.pdf Accessed 2014-02-04.

[37] Google Inc., "Products." Accessed February 3, 2014. https://cloud.google.com/products/.

Amazon.com is a company based in the United States that sells merchandise to consumers as well as offering cloud services under the title Amazon Web Services (AWS). AWS is comprised of 14 different services, ranging from simple storage infrastructure to actual hirable workers.[38] Compute, for example, offers service similar to Google's Compute service, allowing the purchase of scalable infrastructure to handle the computing tasks of the client. Analytics, meanwhile, helps clients analyze massive quantities of data. Deployment and Management allows the client to create controls over who can access particular parts of the information that the client is storing in the cloud. This function could allow a client to better manage the records that are stored in the cloud.

AWS also uses a two-tiered structure for its Agreements. The Customer Agreement is the overarching contract for all of its cloud services. It then has SLAs for some, but not all, of its individual services. The S3 (Simple Storage Service) SLA deals with storage of any kind of data.

8.1.3 Rackspace

Rackspace offers services in three categories: public, managed, and private.[39] The "public" cloud option offered by Rackspace offers infrastructure support on demand for its clients. This service includes options for file storage, databases, servers, big data platforms, and so on. These services are given labels such as Compute, Storage, Databases, Network and Security, and Application and Platform.[40] The "managed" option includes full dedicated support from Rackspace. This service claims 100% network uptime and is advertised for clients with strict performance or compliance requirements.[41] Rackspace's "private" cloud offers "the agility and efficiency of a public cloud – built on infrastructure dedicated exclusively for [the client's] organization."[42] It also offers to assign "cloud specialists" to manage the client's cloud according to their specific requirements, so that the client can focus on running its business.

Rackspace offers these services using the two-tier contract structure. It provides the Cloud Terms of Service[43] which covers all the services it offers. The second tier offers SLAs which cover more specific services. This report focuses on the Rackspace Cloud Servers Service Level Agreement[44] which covers general access to cloud servers, though all of Rackspace's SLAs include similar terms (i.e. uptime guarantees and the credit provided for a lack of uptime).

---

[38] Amazon, "Products & Services." Accessed February 3, 2014. http://aws.amazon.com/products/.

[39] Rackspace, "Rackspace Private Cloud." Accessed January 26, 2014. http://www.rackspace.com/cloud/private/.

[40] Ibid.

[41] Ibid.

[42] Ibid.

[43] Rackspace US, Inc., "Cloud Terms of Service." Last modified October 22, 2013. Accessed January, 26 2014. http://www.rackspace.com/cloud/legal/tos.

[44] Rackspace US, Inc., "Cloud Terms of Service." Last modified June 6, 2013. Accessed January, 26 2014. http://www.rackspace.com/information/legal/cloud/sla#cloud_files_sla.

8.1.4 ProfitBricks

With offices in Massachusetts and Berlin, ProfitBricks is an international cloud IaaS and SaaS provider. The company promotes its services in six categories: Servers, Networks, Performance, Storage, Security and Data Centre Management. It advertises its services as an alternative to Amazon Cloud Services based on lower costs, faster performance, and more assured isolation of client data on shared servers.[45] The company operates 37 data centres in Europe and the United States.

Three documents govern relationships between ProfitBricks and clients: a General Terms and Conditions of Service[46] document; an Acceptable Use Policy[47]; and a Copyright Policy.[48]

8.2 Canada

8.2.1 Telus

As one of Canada's largest telecom providers, Telus has moved to strengthen its cloud services through the construction of a new data centre in British Columbia in February 2014, one of eight such Telus-owned data centres in Canada.[49] Telus offers scaled IaaS, SaaS and PaaS services in two forms for small to large businesses: its AgillT "virtual private cloud" solution for hosted services, and its StorageCloud for storage. A contract for Telus services was not available for viewing online, though certain contract terms can be surmised from promotional material available on the website.

Telus promotes StorageCloud using territory of storage terms ensuring its service is "Canadian from end to end, so your data never leaves the country."[50] The available services also guarantee maximum availability from 99.7 to 99.9% depending on the tier of services used[51] and guarantees that though customer data is stored on shared servers, security is addressed with "unique usernames, passwords and file-level metadata [which] separate your data from that of other clients."[52] No other terms were offered in materials available online.

8.2.2 Storagepipe

---

[45] "Amazon EC2 Cloud Alternatives," accessed on February 3, 2014, http://www.profitbricks.com/amazon-cloud-ec2-alternative.

[46] "General Terms & Conditions of Service." Last updated December 3, 2014. Accessed February 3, 2014, http://www.profitbricks.com/sites/default/files/pb_generaltermsandconditionsofservice_us.pdf

[47] "Profitbricks Acceptable Use Policy." Last updated September 6, 2012. Accessed February 3, 2014, http://www.profitbricks.com/sites/default/files/pb_acceptableusepolicy_us.pdf.

[48] "Copyright Policy." Last updated September 6, 2012. Accessed February 3, 2014, http://www.profitbricks.com/sites/default/files/pb_copyrightpolicy_us.pdf.

[49] Jonathan Brandon, "Telus $75m cloud datacentre in Canada," *Businesscloud News*, accessed on February 3, 2014, http://www.businesscloudnews.com/2014/02/03/telus-opens-75m-cloud-datacentre-in-canada/

[50] "Telus StorageCloud." Accessed on February 3, 2014, http://resources-business.telus.com/cms/files/files/000/000/060/original/TELUS_Storage_Cloud.pdf

[51] Ibid.

[52] Ibid.

Storagepipe is a medium-sized, Toronto-based data protection and backup company that advertises “e-mail archiving” and “electronic archives” services. Their core business is maintaining server backups for clients in the event of local server failure, including disaster recovery backups and business continuity services.

Electronic archiving services offer the ability to conduct “automated policy-based archiving” to “to create point-in-time archives that move older and inactive data off of production equipment and out of normal active backup cycles”.[53] Advertised services for “e-mail archiving” and “social media archiving” offer compliance and best practices for e-mail storage through “automatic identification and flagging of content that raises legal and compliance issues” and gives a “complete audit trail including logging and reporting capabilities”.[54]

The Storagepipe data centre is located in North America, though it is unclear whether it is in Canada or the United States. Storagepipe’s profile of the centre inplies that it is a public cloud as it “acts as a primary North American communications hub for telecommunications carriers and data centre firms from around the globe.”[55] Storagepipe does not detail its contract terms or services further on its website and does not offer Canada-only data storage options.

8.2.3 Titanfile

Based in Halifax, Nova Scotia, TitanFile is a smaller company that has built its business on secure document storage and access using a private cloud. Clients use TitanFile’s file sharing software to access documents from a central account. This account resembles some aspects of records management software in that it generates audit logs of document activity. Furthermore, TitanFile offers system, network and application-level security processes, including the use of 256-it encryption keys and the use of encryption on all files stored on their servers. Their servers reside solely in Canada and are subject to guaranteed facility-level protection. Aside from document transfer, TitanFile also operates a public-facing “deposit box” feature that allows clients to send and receive files through a web interface.

TitanFile provides a general Terms of Service agreement on its website that addresses the use of some of its services, while other contract-like guarantees are scattered throughout the promotional documentation. Concerning contract termination, the ToS notes that “If you cancel your account, shared files will remain available to the people you shared them with”, and “Files that have not been shared will be made inaccessible” and finally that “We may choose to retain your Content, Communications and Contact Info for a period of time after the Expiration of your Account (to allow for easier

[53] “Electronic Archiving Service.” Accessed on February 3, 2014, http://www.storagepipe.com/services/electronic-archiving-service.html.
[54] “E-mail Archiving Service.” Accessed on February 3, 2014, http://www.storagepipe.com/services/email-archiving-service.html.
[55] “Hosting Facilities.” Accessed on February 3 2014, http://www.storagepipe.com/about-us/hosting-facilities.html.

reinstatement of your Account)" with an option to opt-out of this feature.[56] Furthermore, the ToS absolves TitanFile from any responsibility regarding disaster recovery by stating that "You are responsible for backing up, to your own computer or other device, any important Content that you store or access via the Services" and elaborating that "NEITHER TITANFILE NOR ITS PROVIDERS MAKE ANY SPECIFIC PROMISES ABOUT THE SERVICES. FOR EXAMPLE, WE DON'T MAKE ANY COMMITMENTS ABOUT THE CONTENT WITHIN THE SERVICES, THE SPECIFIC FUNCTION OF THE SERVICES, OR THEIR RELIABILITY, AVAILABILITY, OR ABILITY TO MEET YOUR NEEDS. WE PROVIDE THE SERVICES "AS IS"."[57]

In a separate document titled "Security and Technology Overview," maximum outage times were suggested but not guaranteed: "As of the date this document was last updated, average server uptime over the last 12 months was 99.95%."[58]

8.2.4 Pathway Communications

Pathway Communications is an Ontario-based internet service provider. Its primary cloud product is CloudPath, a private cloud storage solution with small-to-large iterations for businesses. CloudPath may also be bundled with managed solutions. Advertising this service with the tagline "the cloud service designed for cautious businesses," ClouthPath offers National Institute of Standards and Technology-based security standards, private "virtual Local Area Networks (VLANs) for isolated access to data; the ability for clients to access all server and application logs for audit purposes; and guarantees that data remains stored in Canada.

Pathway Communications offers these services through four contract documents: CloudPath Terms and Conditions;[59] CloudPath Service Level Agreement[60], and an Acceptable Use Policy which govern the relationship between provider and client. Once the client opts to use and/or commits to the service, the company's Privacy Policy outlines standard protection for the information they collect from clients.

8.2.5 OpenText Corporation

OpenText is a Waterloo, Ontario-based software company and one of the largest enterprise information management software providers on the market. Widely used by businesses and governments, its software provides for content management; digital asset management and business process management, among other functions. Its cloud services are subdivided into three categories: Hosting Services for IT

---

[56] "Terms of Service." No updated date. Accessed February 3, 2014, https://www.titanfile.com/about-us/terms-of-service/.
[57] Ibid.
[58] "Security and Technology Overview." Accessed February 3, 2014, https://www.titanfile.com/wp-content/uploads/2013/05/TitanFile-Security-and-Technology-Overview.pdf
[59] "CloudPath Terms and Conditions." Last updated August 14, 2013. Accessed February 3, 2014, http://cloudpath.pathcom.com/terms/.
[60] "CloudPath Service Level Agreement." Last updated February 1, 2011. Accessed February 3, 2014, http://cloudpath.pathcom.com/sla/.

management and applications; Information Services for document and data transfer; and Social Collaboration Services to support collaboration and sharing. In the latter two categories, its Tempo Box product allows for document and data transfer, exchange and access but in combination with information governance principles such as auditing, retention periods and permissions.[61]

OpenText's Cloud Services Agreement[62] outlines the general terms by which OpenText cloud services are to be used by clients.

8.2.6 Other companies

Two other Canadian companies were considered but not included in the analysis due to a lack of information about their services. What little was learned about them is noted here:

Lexcom is an IT services management company operating out of Saskatchewan and the United States offering "hybrid cloud" solutions including SaaS. While their website indicates they serve government clients, the only information available about their cloud services were that they use a centralized storage facility (location unknown) with high-grade security.

Tenzing is a Canadian company operating out of Toronto, Ontario and Kelowna, B.C. (http://www.tenzing.com/tenzing/hosting-in-canada/). Its services include web-hosting with some pay-as-you-go cloud options geared towards SaaS hosting and storage through Canada Web Hosting, an arm of the company. Their services are all located in Canada.

8.3 Europe

8.3.1 CityNetwork

The Swedish internet services company CityNetwork provides, in addition to domain and hosting services, a cloud platform for cloud storage through a user-friendly API and easily scalable services depending on user needs. The company uses its own data centre and offers a 100% uptime guarantee in its promotional materials. Though the company shares cloud servers among its users, it advertises a "true cloud computing solution" where "each virtual server has its own kernel and cannot be in a same way affected by an execution [sic] of another customer's virtual server."

The company markets its SLA as "an SLA you can trust" in its General Conditions for My CityCloud document[63] and Service Level Agreement page[64] that contains the basic

[61] "OpenText Tempo Box." Accessed February 3, 2014, http://www.opentext.ca/file_source/OpenText/en_US/PDF/Tempo-Box-Product-Overview.pdf.
[62] "Open Text Cloud Services Agreement." No updated date. Accessed February 3, 2014, http://semanticnavigation.opentext.com/terms-and-conditions/.
[63] *General Conditions for My City Cloud*. Last updated 2011. Accessed February 3, 2014,

services offered by the company and the individual roles and responsibilities of the company and a contracted client.

8.3.2 CloudSigma

CloudSigma is a Switzerland-based IaaS public cloud services provider. The company promotes itself as a "pure IaaS that places little or no restrictions on how its users deploy their computing resources." Other than traditional service offerings of flexibility and stable, fast networking and SSID-based storage for greater speed, the service also allows for users to select the location of their cloud data (Zurich, Las Vegas or Washington, DC).

The company enforces the use of its services through six documents available on its website: an Acceptable Use Policy,[65] a Copyright Notice,[66] a Privacy Policy,[67] a Service Level Agreement[68] and a Terms of Service[69] and a Terms of Use[70] (applicable only in the United States). Where the SLA outlines CloudSigma's service guarantees to clients, the Acceptable Use Policy and the Copyright Notice enforce the behavior of users. The two ToS documents give greater granularity to these prior documents, including boilerplate clauses limiting liability and giving no warranty in addition to terms surrounding contract termination and data protection. The U.S. document alters these terms to fit U.S. juridical requirements.

8.3.3 GreenQloud

GreenQloud is an Iceland based company that offers IaaS (StorageQloud[71]), PaaS (ComputeQloud[72]), backup (QloudSync[73]), and SaaS (QStack[74]) in public, private, and

---

https://www.citycloud.com/wp-content/uploads/2011/09/SLA-City-Cloud-eng.pdf.

[64] "SLA (Service Level Agreement) – Dedicated servers, co-location and virtual servers." No updated date. Accessed February 4, 2014, https://www.citynetworkhosting.com/sla-service-level-agreement-dedicated-servers-co-location-and-virtual-servers. /.

[65] "Acceptable Use Policy." Last updated May 2, 2012. Accessed February 3, 2014, http://www.cloudsigma.com/legal/acceptable-use-policy/.

[66] "Copyright Notice." Last updated May 2, 2012. Accessed February 3, 2014, http://www.cloudsigma.com/legal/copyright-notice/.

[67] "Privacy Policy." No modified date. Accessed February 3, 2014, http://www.cloudsigma.com/legal/privacy-policy/

[68] "Service Level Agreement." Last updated November 11, 2013. Accessed February 3, 2014, http://www.cloudsigma.com/legal/service-level-agreement/.

[69] "Terms of Service." Last updated July 1, 2013. Accessed February 3, 2014, http://www.cloudsigma.com/legal/terms-of-service/.

[70] "Terms of Use." Last updated July 15, 2013. Accessed February 3, 2014, http://www.cloudsigma.com/legal/terms-of-use/.

[71] "StorageQloud." GreenQloud StorageQloud Comments. https://www.greenqloud.com/storageqloud/ (accessed May 17, 2014).

[72] "ComputeQloud." GreenQloud ComputeQloud Comments. https://www.greenqloud.com/computeqloud/ (accessed May 17, 2014).

[73] "QloudSync." GreenQloud QloudSync Comments. https://www.greenqloud.com/qloudsync/ (accessed May 17, 2014).

[74] "QStack." GreenQloud QStack Comments. https://www.greenqloud.com/qstack/ (accessed May 17, 2014).

hybrid models. In addition to this, GreenQloud's privacy policy states that "GreenQloud with headquarters in Iceland, abides by regulations set by Icelandic law [provides external link], which has adopted most of the European Economic Area (EEA) regulations [provides external link]."[75]

GreenQloud utilizes the two-tier contract model, employing an End-User License Agreement,[76] which provides more general terms as well as a Service Level Agreement,[77] which has service specific language.

8.3.4 T-Systems

T-Systems is a German company that specializes in providing information services on an enterprise level. One of the services that it offers is what it calls Zero Distance, which is a suite of cloud based services.[78] T-Systems also offers to help its clients customize their cloud services through what it calls Cloud Readiness and Management Services.[79]

9. Identified Categories of Contract Terms

Ultimately, fifteen contract term categories were identified. These are the areas that cloud service provider contracts should address. The articles advising RIM professionals about records management in the cloud, existing RIM standards, and the selected legal cases frequently referred to these term categories. All of the contracts that were read in the course of this research were evaluated to determine whether these were addressed within them. This section will introduce each term category with a definition and provide an explanation as to why each was included.

9.1 Group 1: General Destruction Guarantee

Requires language guaranteeing that records can be destroyed when the end of the client's retention period is reached and no copies whether backups or otherwise would remain.

This category is drawn from a combination of sources and is regularly mentioned by RIM professionals when writing about moving records into the cloud.[80] It is also a

[75] "Privacy Policy." GreenQloud Privacy Policy Comments. https://www.greenqloud.com/privacy-policy/ (accessed May 18, 2014).
[76] "End-User License Agreement (EULA)." GreenQloud EndUser License Agreement EULA Comments. https://www.greenqloud.com/eula/ (accessed May 18, 2014).
[77] "Service-Level Agreement (SLA)." GreenQloud ServiceLevel Agreement SLA Comments. https://www.greenqloud.com/sla/ (accessed May 18, 2014).
[78] "Cloud Computing." - New customer proximity thanks to dynamic IT. http://zero-distance.t-systems.de/zero-distance/int/en/technology/cloud-computing-dynamic-it-brings-us-even-closer-to-the-customer.html (accessed May 18, 2014).
[79] "T-Systems." Analyze your start in the cloud. http://www.t-systems.com/solutions/analyze-your-start-in-the-cloud-t-systems/760004 (accessed May 18, 2014).
[80] Katharine Stuart, and David Bromage. "Emerald Article: Current state of play: records management and the cloud." *Records Management Journal*. 20. no. 2 (2010): 217 - 225. http://dx.doi.org/10.1108/09565691011064340

requirement in all of the professional standards that were consulted during the course of this research.[81]

9.2 Group 1: Specific Destruction Method

Requires language specifying the method by which records will be destroyed to ensure that it is acceptable to the client and that it is in accordance with record keeping requirements.

This is drawn from requirements on how records will be destroyed in a digital environment. “Knowing” that a record is destroyed is paramount, as even records stored on backup could be subject to e-discovery. A client would need to know how copies of their records could be ensured destruction by the service provider when the time for their disposal arrives. Degaussing, physical destruction, and reformatting are examples of acceptable methods of digital record destruction.[82] ISO 15489 recommends that records be reformatted or overwritten,[83] and that records stored offsite from an organization require documentation as proof of destruction.[84]

9.3 Group 1: Destruction on Contract Termination

Requires language guaranteeing that any remaining records of the client can be retrieved by the client or will be destroyed by the service provider at the time the contract concludes.

(accessed January 17, 2014), p. 221.

[80]Also Ju, Jiehui, Jiyi Wu, Jianqing Fu, and Zhijie Lin. "A Survey on Cloud Storage." *Journal of Computers*. 6. no. 8 (2011): 1764-1771, p. 1768.

[80]Ferguson- Boucher, Kirsten. "Cloud Computing: A Records and Information Management Perspective." *Security & Privacy, IEEE*. 9. no. 6 (2011): 63 – 66, p. 64.

[80]National Archives of Australia, . Governmennnt of Australia, "Records management and the cloud." Last modified 2013. Accessed November 21, 2013. http://www.naa.gov.au/records-managnt/agency/secure-and-store/rm-and-the-cloud/.

[80]National Archives and Records Administration. Government of the United States of America, "Frequently Asked Questions about Managing Federal Rerordns In Cloud Computing Environments." Accessed Novembecaterses013. http://www.archives.gov/records-mgmt/faqs/cloud.html.

[80]Council of Australasian Archives and Records Authorities, "Advice on managing the recordkeeping risks associated with cloud computing," *ADRI* (2010), pp. 10-11.

[80]Blair, Barclay. "Governance for Protecting Information in the Cloud." Last modified 2010. Accessed January 17, 2014. http://www.arma.org/docs/hot-topic/makingthejump.pdf.

[81] *ISO 15489 - Information and Documentation - Records Management*, (International Standards Organization, 2001). Also, ARMA International. “Generally accepted record keeping principles.” (2013). Retrieved from http://www.arma.org/r2/generally-accepted-br-recordkeeping-principles, U.S. Department of Defense. “Electronic records management software applications design criteria standard.” [DoD 5015] (2007). Retrieved from http://www.dtic.mil/whs/directives/corres/pdf/501502std.pdf,

[81] Chapter 2, European Commission, "MoReq2 Specification" (2008), pp. 51- 53.

[82] Shepard, Yeo. p. 171.

[83] ISO 15489-2, p. 21.

[84] Ibid.

Any records remaining with the service provider after contract termination could still pose a security risk to the client.[85] RIM professionals and RIM bodies recommend receiving assurances that no information or records will remain with the service provider at the end of the contract.[86]

9.4 Group 2: Service Continuity

Requires language guaranteeing that service will not be ended without warning and that should the service no longer be offered by the service provider, the client will have adequate time to retrieve its records from the service prior to the cessation of access.

Some RIM professionals expressed concerns that records would be unavailable should service suddenly cease.[87] The inability to access records when needed can be disastrous to organizations. The Economist Intelligence Unit reports that 47% of businesses state that they could endure less than a day without access to their records.[88] The same study cites a National Archives and Records Administration's claim that 25% of businesses that experienced an IT outage of as few as 2 days went bankrupt.[89]

9.5 Group 2: Outages

Requires language guaranteeing the client that its records will be available for the vast majority of the time (i.e. 99.99% of the time).

This category also comes from the potential danger to a client if information is inaccessible for periods of time. A contract would need to guarantee a high level of uptime for the service and include a description of the compensation to the client that will result from less than maximum uptime.

9.6 Group 2: Disaster Recovery Plan

Requires **l**anguage describing the provisions of the provider's disaster recovery plan in the event that damage occurs to the servers or their ability to connect to the Internet.

Vital records need to be recovered quickly in the event of a disaster.[90] Records in the cloud are ultimately stored physically somewhere, and are therefore at risk of disaster

---

[85] Stuart and Bromage, p. 223.

[86] Ibid. Also Council of Australasian Archives and Records Authorities, pp. 12-13.

[87] Stuart Rennie, "Legal Implications of Working in the Cloud," *Hot Topic: Making the Jump to Cloud*: 11-16, http://www.arma.org/docs/hot-topic/makingthejump.pdf (accessed February 4, 2014), pp. 14-16.

[88] Economist Intelligence Unit, "Business resilience Ensuring continuity in a volatile environment." Last modified 2007: p. 4 Accessed January 31, 2014. http://graphics.eiu.com/files/ad_pdfs/eiu_Bus_Resilience_wp.pdf, p. 2.

[89] Ibid.

[90] European Commission, MoReq2, p. 48.

just as paper records or onsite digital records are.[91] Should a cloud service provider experience a disaster, a client would want reasonable knowledge of how its information would be recovered by the service provider prior to entering into the contract. Ideally, the extent to which a service provider would go to recover information would be contractually described.[92]

9.7 Group 3: General Security Provisions

Requires language that guarantees a level of security to the client for its records (i.e. at least the same level of security as the company provides for its own records).

This category is drawn from the need to protect the integrity of records. All standards that were reviewed discussed the importance of security and controlled access to records.[93] A client should be guaranteed that the service provider will provide security for information in its custody.

9.8 Group 3: Physical Security Specifications

Requires language that guarantees specific security for the physical servers and the physical location in which they reside.

This category is related to *Group 3: General Security Provisions*, but pertains specifically to information about physical security. Given that the records' physical location will be on servers controlled by the service provider, the client will need to know what precautions are in place to control physical access to the servers and their content pursuant to ISO 15489-2.[94] Additionally, a white paper published by the Cloud Security Alliance identifies threats to the physical location of records can emerge in the form of malicious insiders.[95]

9.9 Group 3: Technological Security Specifications

Requires language that guarantees specific security for the technology on which the records are stored (i.e. the use of firewalls).

This category also comes from the ISO 15489 requirement for controlled access.[96] Given that clients will not be able to monitor the traffic on the cloud service provider's infrastructure themselves, a contract would need to guarantee a certain level of security

---

[91] Council of Australasian Archives and Records Authorities, p. 10. Also Blair, p. 3.

[92] Blair, p. 3. Also Patrick Cunningham, "IT's Responsibility for Security, Compliance in the Cloud," *Hot Topic: Making the Jump to Cloud*: 6-10, p. 7.

[93] ISO 15489-2, pp. 12-13. Also, European Commission MoReq 2, pp. 41-45 and DoD 5015.02 49-53.

[94] ISO 15489-2, p. 12.

[95] Cloud Security Alliance, "Top Threats to Cloud Computing V1.0." Last modified March 2010. Accessed February 4, 2014, pp. ?

[96] Ibid.

to ensure records are not accessed without permission. Threats can come in forms such as hackers attacking the service by transmitting malicious software to a public IaaS and weaknesses to the interface software.[97]

9.10 Group 3: Tiered Security Provisions

Requires language that guarantees specific enhanced security which can be adjusted to match the identified sensitivity of record.

This category acknowledges that certain records are more sensitive than others. Should a client decide to take on the risk of storing these sensitive records in the cloud, terms should indicate what protections will be afforded to them. An example of this is records containing personal identifiable information. ISO requires that access controls be put in place for records of this nature,[98] as well as being required by governing bodies such as in the European Union's Privacy Directive.[99] In addition, RIM literature lists protection of privacy as a concern of moving into the cloud.[100]

9.11 Group 4: Territory of Storage

Requires language that guarantees the political territory where records will be stored and backed up throughout the entirety of their life within the cloud service (i.e. would the records be stored in the United States, the European Union, etc.).

This category was chosen largely due to the requirements found in legislation and directives, such as the European Union Privacy Directive[101] or the requirements for public bodies of British Columbia to store personal information within Canada.[102]

9.12 Group 4: Copyright/Ownership

Language that guarantees that the client will retain full copyright to the records and information and that ownership of any metadata that is applied to the records stored within the cloud service will also remain with the client.

This category was drawn from RIM professionals' concerns over assurances that information placed into storage in the cloud will remain under the copyright of the client. This idea has been expanded to include copyright over the metadata applied to the records by the cloud service provider as such metadata would be necessary to ensure its authenticity.

---

[97] Cloud Security Alliance, pp. 8-9.

[98] Ibid.

[99] European Union Privacy Directive Article 17, section 2.

[100] Blair p. 3.

[101] Article 25, transfer of information to a third country.

[102] Government of British Columbia Freedom of Information and Protection of Privacy Act, Section 30.1.

9.13 Group 4: General Privacy

Language that refers to general privacy provisions.

9.14 Group 4: Privacy Policy

Language that refers to a privacy policy.

9.15 Group 4: Privacy Legislation

Language that refers to privacy legislation.

The three last categories in group 4 were all drawn from organizations' obligations under various privacy and protection of personal information legislation. These three categories of terms would be necessary for a client to understand the full scope of a service providers' attitude and responsibilities towards personally identifiable information that is stored within the cloud infrastructure. Existing contracts often referred to privacy, a privacy policy, and privacy legislation in separate clauses, so the Terms were also separated in the table.

Privacy is a common concern among professionals and references to it are frequent in the literature.[103] A recent study at the Fordham University School of Law found that student data is often being placed in cloud computing services whose contract terms do not adequately protect student privacy. This study recommends contract terms that more directly address privacy.[104] Standards of practice such as ISO 15489 also advise that there are regulatory requirements related to privacy in information storage.[105] Additionally, court cases reviewed during this project indicated the need for specific references to privacy. *United States v. Mitch Miller*, for instance, found that it is the responsibility of the owner of information to trust that the party the information is revealed to will use it for the purposes intended. Strong contract language would enhance this trust.

10. Conclusion

The contract term categories identified in this report attempt to capture a wide range of recordkeeping needs and RIM concerns in regards to moving an organization's records into the cloud. The contracts that were reviewed in comparison to these term categories met some of the types and were absent in others. Unsurprisingly, the contracts tended to protect the service provider from risk, rather than meet client requirements.

---

[103] Ferguson- Boucher, p. 64. Also Stuart and Bromage, pp. 220 and 223,

[104] Reidenberg, Joel; Russell, N. Cameron; Kovnot, Jordan; Norton, Thomas B.; Cloutier, Ryan; and Alvarado, Daniela, "Privacy and Cloud Computing in Public Schools" (2013). *Center on Law and Information Policy.* Book 2.
[104]http://ir.lawnet.fordham.edu/clip/2

[105] ISO 15489-1, p. 14.

As can be seen in the three tables below, a number of the term categories were more commonly addressed in the contracts. "Group 2: Outages," for example, was addressed in a high number of contacts, being found in five of the eight. These categories, however, were not addressed in a uniform manner, providing similar guarantees with different language. Many of the contracts also provided general and technological security provisions, vague references to privacy, as well as language regarding copyright and ownership. Provided least often, meanwhile, were the categories related to the destruction of records as a recordkeeping function, an explanation of a disaster recovery plan, and security reliability for certain highly sensitive records.

It is hoped that this study will provide a starting point for other groups in InterPARES Trust project, particularly in the development of model terms, by showing some of the gaps that appear in contracts from a RIM perspective. One area in particular that requires significantly more research was pointed out during discussion of the first plenary meeting in February, 2014. Namely, the existence of any language in the contracts specifically related to the long-term preservation of the records stored with the cloud services.

11. Summary Tables and Specific Contract Term Language

The included tables are meant to provide an overview of the findings that resulted from the assessment of each selected contract using the 15 types of contract terms that were identified through the literature review. This section will provide an explanation for the actual terms that were found to address the related term categories. As the tables indicate, many of the term types that were identified were not addressed in the contracts reviewed. In an effort to save space, this section will not discuss term types that were not identified in each contact, only the terms that specifically included or, through directly contradictory language, specifically excluded an identified term type.

11.1 United States

Summary of Contract and Service Terms Offered by Cloud Service Providers - United States

Company Name	Google Cloud Platform	Amazon Web Services	Rackspace	ProfitBricks
Country	U.S.	U.S.	U.S.	U.S. and Europe (Germany)
Group 1: General Destruction Guarantee	not addressed	not addressed	not addressed	General Terms and Conditions of Service 3.9
Group 1: Specific Destruction Method	not addressed	not addressed	not addressed	not addressed
Group 1: Destruction on Contract Termination	Terms of Service - 9.5	not addressed	not addressed	General Terms and Conditions of Service 3.9
Group 2: Service Continuity	Terms of Service - 7.3	Customer Agreement - 2.1	Cloud Terms of Service - 12.1	General Terms and Conditions of Service 7.1-7.9

Group 2: Outages	Service Level Agreement	S3 Service Level Agreement	Cloud Terms of Service - 5	General Terms and Conditions of Service 7.1-7.3
Group 2: Disaster Recovery Plan	not addressed	not addressed	not addressed	not addressed
Group 3: General Security Provisions	Terms of Service - 2.2	Customer Agreement - 3.1	Cloud Terms of Service - 2	General Terms and Conditions of Service 7.1-7.9
Group 3: Physical Security Specifications	not addressed	not addressed	Cloud Terms of Service - 2	General Terms and Conditions of Service 7.4
Group 3: Technological Security Specifications	not addressed	not addressed	not addressed	General Terms and Conditions of Service 7.5
Group 3: Tiered Security Provisions	not addressed	not addressed	not addressed	not addressed
Group 4: Territory of Storage	not addressed	Customer Agreement 3.2	not addressed	not addressed
Group 4: Copyright/Ownership	Terms of Service - 6.1	Customer Agreement - 8.1	Terms of Service - 24	ProfitBricks - Copyright Policy
Group 4: General Privacy	Terms of Service - 2.4 and Google Privacy Policy	Customer Agreement - 3.2	Terms of Service - 14.1	Profit Bricks - General Terms and Conditions
Group 4: Privacy Policy	Terms of Service - 2.4 and Google Privacy Policy	Customer Agreement - 3.2	not addressed	ProfitBricks - Privacy Policy
Group 4: Privacy Legislation	Terms of Service - 2.4 and Google Privacy Policy	Customer Agreement - 3.2	Terms of Service - 14.3	not addressed

11.1.1 Google[106]

Group 1: Destruction on Contract Termination - Google Cloud Platform Terms of Service - 9.5

9.5 Effect of Termination. "… and (iv) upon request, each party will use commercially reasonable efforts to return or destroy all Confidential Information of the other party."

This language enables the client to request the destruction of its records upon the end of the contract. Although the term "commercially reasonable" may limit the extent Google must go through to destroy records upon the termination of the contract, it does leave the potential for the client to request a method that is compliant with record keeping needs. This language can been seen to meet the minimum needs of this requirement, however, better language would include specifications on how the information would be destroyed.

Group 2: Service Continuity - Google Cloud Platform Terms of Service - 7.3

"7.3 Deprecation Policy. Google will announce if it intends to discontinue or make backwards incompatible changes to the Services specified at the URL in the next sentence. Google will use commercially reasonable efforts to continue to operate those Services versions and features identified at

[106] Google Inc., " Google Cloud Platform Terms of Service." Last modified December 16, 2013. Accessed February 5, 2014. https://developers.google.com/cloud/terms/. Also, Google Inc., " Google Cloud Storage, Google Prediction API, and Google BigQuery SLA." Accessed February 5, 2014. https://developers.google.com/storage/sla.

https://developers.google.com/cloud/terms/deprecation without these changes for at least one year after that announcement…"

Under this language, a client has some assurance that if Google ever intents to no longer offer the service, the client will have a year in which to make arrangements for its records. However, the term "commercially reasonable" provide Google room in which to end a service earlier than a year after notice. Better language would provide this assurance in firmer language.

Group 2: Outages - Google Cloud Platform Service Level Agreement
Google's Cloud Storage SLA promises its clients 99.9% uptime for the service, with a percentage of the monthly bill offered as credit for lack of availability. This language providers some assurance to a client, however, given the potential financial and legal consequences for a client to be unable to access its records, this may be insufficient.

Group 3: General Security Provisions - Google Cloud Platform Terms of Service - 2.2
"2.2 Facilities and Data Transfer. All facilities used to store and process an Application and Customer Data will adhere to reasonable security standards no less protective than the security standards at facilities where Google processes and stores its own information of a similar type. Google has implemented at least industry standard systems and procedures to ensure the security and confidentiality of an Application and Customer Data, protect against anticipated threats or hazards to the security or integrity of an Application and Customer Data, and protect against unauthorized access to or use of an Application and Customer Data."

This language providers to the customer that its data will be protected to and less than the security Google would provide to its records and to industry standards. The language is not clear, however, how Google will determine "similar type" or "industry standards."

Group 4: Copyright/Ownership - Google Cloud Platform Terms of Service - 6.1
"6.1 Intellectual Property Rights. Except as expressly set forth herein, this Agreement does not grant either party any rights, implied or otherwise, to the other's content or any of the other's intellectual property. As between the parties, Customer owns all Intellectual Property Rights in Customer Data and the Application or Project (if applicable) and Google owns all Intellectual Property Rights in the Services and Software."

This language provides assurance to the client that the information it stores with Google will remain in its possession. However, it does not provide that metadata assigned to the records stored within Google's service will be under the copyright of the client.

Group 4: General Privacy – Group 4: Privacy Policy – Group 4: Privacy Legislation - Google Cloud Platform Terms of Service - 2.4 and Google Privacy

Policy
"2.4 Privacy Policies. The Services are subject to Google's Privacy Policy. Changes to the Privacy Policy will be made as stated in the applicable policy. In addition, Google is enrolled in the U.S. Department of Commerce Safe Harbor Program and will remain enrolled in this program or another replacement program (or will adopt a compliance solution which achieves compliance with the terms of Article 25 of Directive 95/46/EC) throughout the Term of the Agreement."

General privacy provisions are given here and in the privacy policy. The privacy policy explains what information is collected by Google and how it is used. It would be up to clients to determine how well this policy meets their needs, however the language is provided. Section 2.2 also takes that Google is enrolled in the U.S. Department of Commerce Safe Harbor Program, allowing Google to work with clients under the jurisdiction of European Union privacy legislation.

11.1.2 Amazon[107]

Group 2: Service Continuity – AWS Customer Agreement – 2.1
"2.1 To the Service Offerings. We may change, discontinue, or deprecate any of the Service Offerings (including the Service Offerings as a whole) or change or remove features or functionality of the Service Offerings from time to time. We will notify you of any material change to or discontinuation of the Service Offerings."

This language does provide that Amazon will notify its clients of the discontinuation of services, but not provide any period of time to allow the client to retrieve information stored with the services. This is indicated in red in the table.

Group 2: Outages – AWS S3 Service Level Agreement

Similar to Google, Amazon offers credits in return for its service being unavailable. This credit is 10-25% of the client's bill for availability less than 99.9% of the time. This language providers some assurance to a client, however, as with Google, given the potential financial and legal consequences for a client to be unable to access its records, this may be insufficient.

Group 3: General Security Provisions – AWS Customer Agreement 3.1
"3.1 AWS Security. Without limiting Section 10 or your obligations under Section 4.2, we will implement reasonable and appropriate measures designed to help you secure Your Content against accidental or unlawful loss, access or disclosure."

This section provides that security precautions will be in place, although the contract is far from specific, referring to "reasonable and appropriate," which the client may not

[107] Amazon.com, "AWS Customer Agreement." Last modified March 15, 2012. Accessed February 5, 2014. http://aws.amazon.com/agreement/. Also, Amazon.com, "Amazon S3 SLA." Last modified June 01, 2013. Accessed February 5, 2014. http://aws.amazon.com/s3/sla/.

believe to be the same level of security at the service provider.

Group 4: Territory of Storage – AWS Customer Agreement – 3.2
"3.2 Data Privacy. We participate in the safe harbor programs described in the Privacy Policy. You may specify the AWS regions in which Your Content will be stored and accessible by End Users. We will not move Your Content from your selected AWS regions without notifying you, unless required to comply with the law or requests of governmental entities."

This language implies that a client may select which region to store its records in, although the regions that are available are not specified.

Group 4: Copyright/Ownership - AWS Customer Agreement - 8.1
"8.1 Your Content. As between you and us, you or your licensors own all right, title, and interest in and to Your Content. Except as provided in this Section 8, we obtain no rights under this Agreement from you or your licensors to Your Content, including any related intellectual property rights. You consent to our use of Your Content to provide the Service Offerings to you and any End Users. We may disclose Your Content to provide the Service Offerings to you or any End Users or to comply with any request of a governmental or regulatory body (including subpoenas or court orders)."

This language provides that the client's information will be under its copyright, but does not provide that metadata assigned to records stored in the service will belong to the client.

Group 4: General Privacy – Group 4: Privacy Policy – Group 4: Privacy Legislation – AWS Customer Agreement – 3.2
"3.2 Data Privacy. We participate in the safe harbor programs described in the Privacy Policy. You may specify the AWS regions in which Your Content will be stored and accessible by End Users. We will not move Your Content from your selected AWS regions without notifying you, unless required to comply with the law or requests of governmental entities. You consent to our collection, use and disclosure of information associated with the Service Offerings in accordance with our Privacy Policy, and to the processing of Your Content in, and the transfer of Your Content into, the AWS regions you select."

This language provider some general privacy provisions, makes reference to the privacy policy, and references the service provider's adherence to the Safe Harbor Program. The language does not state that the contract adheres to the privacy policy, however.

11.1.3 Rackspace[108]

[108] Rackspace, "Cloud Terms of Service." Last modified October 22, 2013. Accessed February 5, 2014. http://www.rackspace.com/information/legal/cloud/tos. Also, Rackspace, "Cloud Files SLA." Last modified January 21, 2011. Accessed February 5, 2014. http://www.rackspace.com/information/legal/cloud/sla.

Group 2: Service Continuity – Rackspace Cloud Terms of Service – 12.1
"12.1 You will not have access to your data stored on the Services during a suspension or following termination."

The existing language appears to deny the RIM concern.

Group 2: Outages – Rackspace Cloud Terms of Service – 5
"5. Service Level Agreements. Cloud Service Level Agreements are located at http://www.rackspace.com/cloud/legal/sla. The terms there are incorporated herein by reference as to the applicable Services."

This section refers to an SLA which outlines guaranteed availability and compensation for lack of availability. The compensation model is similar to Google and Amazon's in that it offers a percentage of the client's bill as compensation should a service be unavailable for a percentage of time. As with the other two American Companies, given the potential financial and legal consequences for a client to be unable to access its records, this may be insufficient.

Group 3: General Security Provisions/Group 3: Physical Security Specifications - Rackspace Cloud Terms of Service – 2
"2. Rackspace's Obligations. Contingent on Rackspace's acceptance of your Order, and subject to these Cloud Terms of Service, Rackspace agrees to provide the Services and Support described in your Order. Rackspace agrees to follow security procedures at least as stringent, in Rackspace's reasonable judgment, as those described at http://www.rackspace.com/information/legal/securitypractices.php."

In this language, Rackspace makes references to both a general guarantee of security and links to a document[109] outlining more specific physical security including video surveillance and security authentication methods.

Group 4: Copyright/Ownership - Rackspace Terms of Service – 24
"24. Ownership of Intellectual Property. Each of us retains all right, title and interest in and to our respective trade secrets, inventions, copyrights, and other intellectual property. Any intellectual property developed by Rackspace during the performance of the Services shall belong to Rackspace unless we have agreed with you in advance in writing that you shall have an interest in the intellectual property."

This language provides to a client that it may keep the information that it stores with the service provider. The language "any intellectual property developed by Rackspace during the performance of the Services shall belong to Rackspace" would likely include any metadata applied to the records stored on the service. Rackspace, however, does allow that another agreement may be created allowing for the client to keep this generated property. This would likely be at Rackspace's discretion.

[109] http://www.rackspace.com/information/legal/securitypractices

Group 4: General Privacy/Group 4: Privacy Legislation - Rackspace Terms of Service - 14.1
"14.1 We do not promise that the Services will be uninterrupted, error-free, or completely secure. You acknowledge that there are risks inherent in Internet connectivity that could result in the loss of your privacy, Customer Data, Confidential Information, and property…. You are solely responsible for the suitability of the service chosen, including the suitability as it relates to your Customer Data."

Here, Rackspace removes itself from responsibility for the privacy of the client's information. It also states that the client is responsible for the suitability of the service, which would mean all legislation.

11.1.4 ProfitBricks

Group 1: General Destruction Guarantee – Group 1: Destruction on Contract Termination – ProfitBricks General Terms and Conditions of Service s. 3.9
"Notwithstanding the foregoing, after suspension or termination of your right to use the Services, and the expiration of any time periods set forth in Sections 3.7.1 or 3.7.2, you will no longer have access to your account, and your data, including but not limited to e-mails, log files, databases, or other data files associated with your account, will be deleted. Without limitation to Section 11.5, and notwithstanding the provisions of Sections 3.7.1 and 3.7.2, ProfitBricks accepts no liability for deleted data or content, and does not warrant or represent that you will be able to access, download, or recover such data or content after termination for any reason."

This section addresses deletion of data whether a contract has been terminated by the client as opposed to the suspension of accounts for such reasons as non-payment for services. In cases where the latter occurs, the company guarantees that "we will not take any action to intentionally erase any of your data stored on the Services" (s. 3.7.2[a]). Though the language does not specify the method of destruction, it can be assumed from the language that data is non-retrievable.

Group 2: Service Continuity - ProfitBricks General Terms and Conditions of Service s. 3.7
"In the event of any termination by us of any Service or any set of Services, or termination of this Agreement in its entirety, other than a for cause termination under Section 3.4.1, (a) we will not take any action to intentionally erase any of your data stored on the Services for a period of thirty (30) days after the effective date of termination"

This section refers to contract termination (as opposed to suspension detailed in s. 3.4.1) where ProfitBricks gives users 30 days to retrieve data if contracts are terminated "other than for cause." Contracts may be terminated "for cause" with stricter penalties (immediate termination with or without notice) for illegal or malicious use of the services.

Note that there are no terms that give positive availability guarantees: these terms only treat the termination of services, not their continuity.

Group 2: Outages - ProfitBricks General Terms and Conditions of Service s. 7.1-7.3

“ProfitBricks guarantees 99.95% uptime for internal network performance (“Network Guarantee”). The Network Guarantee only covers the network interfaces between the hypervisor and ProfitBricks network and other servers of the customer on the same VLAN. This Network Guarantee does not cover network connections to the Customer’s physical location or Internet access points”

This section and the following sections 7.2 (hardware guarantee) and 7.3 (storage guarantee) give similar language in guaranteeing 99.95% uptime for all three aspects of their cloud service. Section 7.7. in turn gives a reimbursement guarantee of “five percent of Customer’s monthly fee for each thirty minutes of downtime” for network, hardware and storage failure.

Group 2: Disaster Recovery Plan - Group 3: General Security Provisions - ProfitBricks General Terms and Conditions of Service s. 7.9

“[Y]ou acknowledge that you bear sole responsibility for adequate security, protection, and backup of Your Content, Applications, passwords, and user names. We strongly encourage you, where available and appropriate, to (a) use encryption technology to protect Your Content from unauthorized access, (b) routinely archive Your Content, and (c) keep your Applications or any software that you use or run with our Services current with the latest security patches or updates.”

In the concluding section of the terms on security, ProfitBricks absolves itself of security guarantees and places the burden of security on the client, including the encryption of content and regular archiving of content. As a result, the contract also absolves the company of providing for a disaster recovery plan in the event of a third party-sourced security breach or other disaster event except in the maintenance of the performance standards set in the above section (ss. 7.1-7.3).

Regarding data loss on ProfitBricks storage devices, Section 7.3 also absolves ProfitBricks of responsibility for data loss: “Under no circumstances will ProfitBricks be responsible for the restoration of any data or any data loss in the ProfitBricks storage services.”

Group 3: Physical Security Specifications - ProfitBricks General Terms and Conditions of Service s. 7.4

“ProfitBricks guarantees that the infrastructure providing the services is located in a physically secure environment protected from outside malicious activity 24 hours a day, 365 days per year (“Security Guarantee”). “Physically secure environment” means that all physical access to the ProfitBricks data centre requires a valid US driver’s license, passport and 12-hours’ notice. The Security Guarantee also includes 24/7 presence of

an on-site security officer and data-centre operations personnel at the facility, security cameras, and monitoring devices."

Group 4: Copyright/Ownership - ProfitBricks General Terms and Conditions of Service s. 10.2

"Other than the rights and interests expressly set forth in this Agreement, and excluding ProfitBricks Works and works derived from ProfitBricks Works, you reserve all right, title, and interest (including all intellectual property and proprietary rights) in and to Your Content."

"ProfitBricks Works" are defined in s. 6 as "a variety of software, data, and other content and printed and electronic documentation" produced by ProfitBricks. In contrast" your content" is defined in s. 4.1.2 as "any Application, data, or other content that you may (a) provide to us pursuant to this Agreement, (b) make available to any end users in conjunction with the Services, or (c) develop or use in connection with the Services." Therefore, ProfitBricks users hold rights to the content stored in their cloud, including (as inferred from the above language) any data or metadata derived form the use of ProfitBricks services.

Group 4: General Privacy - ProfitBricks General Terms and Conditions of Service s. 10.2

"We will not disclose Your Content, except: (a) if you expressly authorize us to do in connection with your use of the Services; (b) as necessary to provide the Services to you; or (c) as ProfitBricks deems necessary, in its sole discretion, to comply with the Agreement or the request of a governmental or regulatory body, subpoenas, court orders, or other legal authority."

Contained under the intellectual property section of the *Terms*, this brief section addresses disclosure of data to the public or legal or regulatory bodies.

11.2 Canada

Summary of Contract and Service Terms Offered by Cloud Service Providers - Canada		
Company Name	**Pathway Communications Cloud Path**	**Open Text**
Country	**Canada**	**Canada**
Group 1: General Destruction Guarantee	Terms and Conditions 8.2	Cloud Services Agreement - 4.1
Group 1: Specific Destruction Method	not addressed	not addressed
Group 1: Destruction on Contract Termination	Terms and Conditions 8.1	Cloud Services Agreement - 5.4
Group 2: Service Continuity	Terms and Conditions 8.4	Cloud Services Agreement - 5.4

Group 2: Outages	Terms and Conditions 4.1.2 Optional: 4.3.4	not addressed
Group 2: Disaster Recovery Plan	not addressed	not addressed
Group 3: General Security Provisions	Terms and Conditions 3.3	Cloud Services Agreement - 4.6
Group 3: Physical Security Specifications	Terms and Conditions 4.1.5 and Additional Details in the Service Level Agreement	not addressed
Group 3: Technological Security Specifications	Optional: Terms and Conditions 4.3.5	not addressed
Group 3: Tiered Security Provisions	not addressed	not addressed
Group 4: Territory of Storage	not addressed	not addressed
Group 4: Copyright/Ownership	Terms and Conditions - 20.1	Cloud Services Agreement - 4.2
Group 4: General Privacy	Terms and Conditions - 4.1.6 and Privacy Policy	not addressed
Group 4: Privacy Policy	Terms and Conditions - 4.1.6 and Privacy Policy	not addressed
Group 4: Privacy Legislation	Terms and Conditions 4.1.6 and Privacy Policy	not addressed

11--.2.1 Pathway Communications[110]

Group 1: General Destruction Guarantee - Cloud Path Terms and Conditions – 8.2
"8.2. We may destroy all but the most recent snapshot or backup. These snapshots or backups may not be available to you or, if available, may not be useful to you outside of the Pathway system. Although Pathway Services may be used as a backup service, you agree that you will maintain at least one (1) additional, current copy of your programs and data stored on the Pathway system somewhere other than on the Pathway system."

This language nearly meets the RIM concern/term type is corresponds to but for the uncertainty present with the word "may." A client would need to know that all but the most recent backup has been destroyed to satisfy this concern.

Group 1: Destruction on Contract Termination - Cloud Path Terms and Conditions – 8.1
"8.1. You will not have access to Client Data stored on the Pathway system during a suspension or following termination."

This language prevents a client from accessing information following termination. Because these is no other language dealing with the discontinuation of the service, "termination" could be extended to this and could prevent a client from accessing

[110] Pathway Communications, " CloudPath Terms and Conditions." Last modified August 14, 2013. Accessed February 5, 2014. http://cloudpath.pathcom.com/terms/. Also, Pathway Communications, " CloudPath Service Level Agreement (SLA)." Last modified February 01, 2011. Accessed February 5, 2014. http://cloudpath.pathcom.com/sla/.

records if the service ends.

Group 2: Outages - Cloud Path Terms and Conditions 4.1.2 Optional: 4.3.4
"4.1.2. Service at a level equal to that which is defined in the SLA which is relevant and applicable to the Service you have enrolled for through a Service Order."

This language directs to the SLA[111] for the service which guarantees that the service will be available for 99.9% of the time in a monthly billing cycle. For this service, there are again credits offered for a lack of service.

Group 3: General Security Provisions – Cloud Path Terms and Conditions 3.3
"3.3 Pathway agrees to follow security procedures at least as stringent, in Pathway's reasonable judgment, as those described in its Security Policies."

Group 3: Physical Security Specifications - Cloud Path Terms and Conditions 4.1.5 and Additional Details in Cloud Path SLA
"4.1.5. Physical security for the hardware (network, storage, and servers) and software that hosts your Service…." and from the SLA "Pathway will ensure the presence of on-site security guards in the Pathway Data Centre at all times, 24/7/365. These staff will follow Pathway's security policies and procedures, which include, amongst other things, that visitors wear badges and are authorized to visit the premises."

In these terms, Pathway Communications provides fairly firm language on the physical security it provides for clients.

Group 3: Technological Security Specifications - Optional: Cloud Path Terms and Conditions 4.3.5
"4.3.5. Firewalls."

As an optional service, the client may purchase firewalls in addition the standard service.

Group 4: Copyright/Ownership - Cloud Path Terms and Conditions - 20.1
"20.1. Each of us retains all right, title, and interest in and to our respective trade secrets, inventions, copyrights, and other intellectual property. Any intellectual property developed by Pathway during the performance of the Services shall belong to Pathway unless we have agreed with you in advance in writing that you shall have an interest in the intellectual property."

This language is very similar to others regarding copyright. The client keeps all its information, but metadata applied to records would likely remain with the service provider. There does appear to be the capacity to amend this with additional agreements, however.

[111] http://cloudpath.pathcom.com/sla/

Group 4: General Privacy – Group 4: Privacy Policy – Group 4: Privacy Legislation - Cloud Path Terms and Conditions - 4.1.6 and Privacy Policy
"4.1.6. Privacy for Client Data as required by Canadian Law and as outlined in the Pathway Privacy Policy."

This language not only commits Pathway Communications from adhering to Canadian privacy law, but also commits the service provider to the private policy, which quite extensively outlines its obligations to the client. It would be up to each client to determine how well the policy fits its needs, but the language exists.

11.2.2 Open Text[112]

Group 1: General Destruction Guarantee - Open Text Cloud Services Agreement - 4.1
"4.1 Customer must provide all data for use in the Services ("Customer Data"), and OT is not obliged to modify, delete or add to the Customer Data."

With this language, the service provider clearly states that records stored with it will not be guaranteed deletion.

Group 1: Destruction on Contract Termination - Group 2: Service Continuity - Open Text Cloud Services Agreement - 5.4
"5.4 Upon termination of this Agreement, OT will promptly provide all Customer Data to Customer. However, OT may retain Customer Data in backup media for an additional period of up to twelve (12) months, or longer if required by law. However, Customer agrees and acknowledges that OT has no obligation to retain the Customer Data, and may delete such Customer Data any time after thirty (30) days from termination."

This language provides a guarantee that client information will be deleted no later than 1 year after the end of the contract. While a period of time less than one year would likely be preferable for the client, it does provide the guarantee none-the-less. The language also ensures that the client will have its information returned should the service end.

Group 3: General Security Provisions - Open Text Cloud Services - 4.6
"4.6 OT shall take reasonable technical and organizational measures to keep Customer Data secure and to protect it against accidental loss or unlawful destruction, alteration, disclosure or access; and, must deal with the information only in accordance with Customer's instructions, provided they are reasonable and lawful."

This language provides general assurances toward security, but fails to provide any specificity.

[112] Open Text, "Open Text Cloud Services Agreement." Accessed February 5, 2014. http://semanticnavigation.opentext.com/terms-and-conditions/.

Group 4: Copyright/Ownership - Open Text Cloud Services Agreement - 4.2
"4.2 Customer Data belongs to Customer, and OT makes no claim to any right of ownership in it. By posting or permitting Customer Data to be posted, Customer represents and warrants to OT and other users of the Service that Customer is the owner of all rights to that Customer Data or that Customer otherwise have the right to reproduce and distribute it."

This language provides that the client will own the information it stores with the service provider, however metadata applied to records stored within the service are not addressed.

11.3 Europe

Summary of Contract and Service Terms Offered by Cloud Service Providers -Europe

	City Network	CloudSigma	GreenQloud
Country	**Europe (Sweden)**	**Europe (Switzerland)**	**Europe (Iceland)**
Group 1: General Destruction Guarantee	not addressed	not addressed	not addressed
Group 1: Specific Destruction Method	not addressed	not addressed	not addressed
Group 1: Destruction on Contract Termination	not addressed	not addressed	not addressed
Group 2: Service Continuity	General Conditions - 5	Terms of Service 3.13 and 10.2	End User License Agreement - 6
Group 2: Outages	General Conditions - 5	CloudSigma Service Level Agreement	GreenQloud - Service Level Agreement
Group 2: Disaster Recovery Plan	not addressed	Terms of Service - 3.11	not addressed
Group 3: General Security Provisions	not addressed	Terms of Service - 10.6 and Service Level Agreement	End User License Agreement - 10
Group 3: Physical Security Specifications	not addressed	not addressed	not addressed
Group 3: Technological Security Specifications	not addressed	Terms of Service - 10.6 and Service Level Agreement	not addressed
Group 3: Tiered Security Provisions	not addressed	Terms of Service - 10.6	not addressed
Group 4: Territory of Storage	not addressed	CloudSigma Privacy Policy	not addressed
Group 4: Copyright/Ownership	not addressed	Copyright Notice	not addressed
Group 4: General Privacy	General Conditions - 9	Terms of Service - 12	GreenQloud Privacy Policy
Group 4: Privacy Policy	General Conditions - 9	Company Privacy Policy	GreenQloud Privacy Policy

Group 4: Privacy Legislation	General Conditions - 9	not addressed	not addressed

11.3.1 City Network

Group 2: Service Continuality - Group 2: Outages - General Conditions for My City Cloud s. 5(a):
"In case of a breakdown, errors or no access to the services, customer can be reimbursed based on SLA available here: http://www.citynetwork.eu/100-uptime-guaranteed/[113]. Breakdown time starts after it is reported by the client and lasts until it is fixed. Total reimbursement is limited to a maximum of a monthly fee for a month in question."[114]

In this language City Network stands by a 100% uptime guarantee for which the company is willing to reimburse customers if and downtime occurs. These terms are qualified by sections 5(b) and (c) of the *General Conditions* that explain that any client error, including misuse of the service, or attacks from third parties, or scheduled maintenance downtime, that cause breaks in availability will not be subject to reimbursement. In section (d) the policy gives clients seven days to make claims for downtime reimbursement.

The company's informal *Service Level Agreement* page gives the reimbursement amount as "5% of the total monthly fee for each 3 hours interval."[115]

Group 4: General Privacy – Group 4: Privacy Policy – Group 4: Privacy Legislation – General Conditions – 9
"a) City Network manages Customer data according to personal data protection act. Customer data is not available to any third party. The exception is a situation in which the Customer violates the terms of the agreement, or the authority will require the provision of such data"[116]

This language encompasses the 3 privacy areas of Group 4. It provides that the company adheres to the Personal Data Protection Act, providing reasonable assurances to its client about the safety of that client's data.

---

[113] Link broken in policy. Page can be found here as of February 4, 2014: https://www.citynetworkhosting.com/100-uptime-guaranteed/.
[114] "General conditions for MY CITYCLOUD." . https://www.citycloud.com/wp-content/uploads/2011/09/SLA-City-Cloud-eng.pdf (accessed May 19, 2014).
[115] "SLA (Service Level Agreement) – Dedicated servers, co-location and virtual servers." . https://www.citynetworkhosting.com/sla-service-level-agreement-dedicated-servers-co-location-and-virtual-servers/ (accessed May 19, 2014).
[116] Ibid. "General Conditions…"

11.3.2 CloudSigma

Group 2: Service Continuity – CloudSigma Terms of Service s. 3.13 and 10.2
"We will endeavour to provide you with reasonable notice of any suspension under this clause unless it our reasonable belief that an immediate suspension or shorter notice is required to protect our network infrastructure and services to other customers from significant operational or security risk or because we are compelled to do so by law."[117]

"You or us may terminate the Agreement by giving thirty (30) days written notice (including without limitation email notice)."[118]

These sections provide some reasonable assurances that the service will not end abruptly so long as the client adheres to the terms of service.

Group 2: Outages – CloudSigma Service Level Agreement
CloudSigma gives three terms for availability in its *Service Level Agreement*[119]: virtual server availability (100%); network uptime (100%) and network latency (1ms or less). In the same document, it allows users to apply for credit 30 days following a disruption. Credit is defined at "50 times the fees for any period of lack of availability" for any of the above categories. Furthermore, the SLA guarantees "Credit of your entire fee for the previous 30 calendar days in case of permanent loss of your stored data resulting from hardware or software failure of CloudSigma's systems. This provision entirely excludes data loss or corruption resulting from software running within a virtual server." All credits are subject to further limitations including illegal uses of the services or third-party attacks.

Group 2: Disaster Recovery Plan - CloudSigma Terms of Service s. 3.11
"We shall not be responsible for any back up, recovery or other step required to ensure that data and information stored on the CloudSigma network and infrastructure as part of provision of Services to you is recoverable in the case of any data loss, system fault, software failure, hardware failure or other activity which results in any loss of data, information or other item that is being stored as part of our Services."

CloudSigma absolves itself of a disaster recovery plan by claiming no responsibility for any data loss. Section 4.1.7 on the use of the services gives the direction to "use reasonable security precautions in relation to your use of the Services."

Group 3: General Security Provisions – CloudSigma Terms of Service s. 3.18
"We have no obligation to provide security other than as stated in the Agreement. We disclaim any and all warranties not expressly stated in the Agreement, including the implied warranties of merchantability, fitness for a particular purpose, and non-

[117] CloudSigma "Terms of Service"
[118] Ibid.
[119] Ibid. "Service Level Agreement"

infringement."

Despite the language in this section, no other security guarantees except basic encryption details (contained in the *Privacy Policy*) are provided in any of the documents refereed to collectively as the "Agreement," particularly the *Service Level Agreement*. As above, the burden of security provision falls to the user in the *Terms of Service*.

Group 3: Technological Security Specifications – CloudSigma Privacy Policy
"All Virtual Drive Data is stored encrypted using a 256bit AES-TLX encryption cascade."

This language provides uncommon detail about the technological security that is employed by CloudSigma.

Group 4: Territory of Storage – CloudSigma Privacy Policy
"All Virtual Drive Data uploaded to CloudSigma is stored securely on our servers in our dedicated rack space in Switzerland."

In this language, CloudSigma again provides a very useful specification to its clients, who are able to know which jurisdiction their records will be stored in and determine if that jurisdiction suits their needs.

Group 4: Copyright/Ownership – CloudSigma Terms of Service s. 10.2 (USA only terms)
"You hereby grant us a royalty-free licence, for the duration of the agreement, to use the data provided by you in our provision of the Services to you."

Unlike other terms, the *Terms of Service* and *Copyright Notice* and *Terms of Use* do not address the ownership of data except in s. 11.2 of the USA-applicable terms in the *Terms of Service* where it is stated that "Each of us retains all right, title and interest in and to our respective trade secrets, inventions, copyrights, and other intellectual property." Rather, the above terms contained in s. 10.2 give the rights for CloudSigma to use data provided by the use of their services. More information on this data may be and what defines "use" is not given.

Group 4: General Privacy - Group 4: Privacy Policy - Terms of Service 12 and Privacy Policy
"All collection, storing and use of your data are governed by the Privacy Policy."[120]

CloudSigma refers clients to its Privacy Policy, which governs the privacy guarantees offered by the service provider. CloudSigma actually offers different privacy policies for clients in different jurisdictions: Switzerland and the United States.

11.3.3 GreenQloud

[120] CloudSigma "Terms of Service" Section 12

Group 2: Service Continuality
"If the Company thinks it necessary to suspend a customer's Service without cause, the Company will provide 14 days advanced notice."[121]

This language guarantees that the client will have two-weeks warning of the loss of access to records.

Group 2: Outages – Service Level Agreement
The GreenQloud Service Level Agreement ensures 100% uptime, and offers deductions from the billing cycle for a loss of service.

Group 3: General Security Provisions – End User License Agreement – 10
"…You are responsible for properly configuring and using the Service Offerings and taking your own steps to maintain appropriate security, protection and backup of Your Content…"[122]

With this language, GreenQloud removes security responsibilities from itself.

Group 4: General Privacy – Group 4: Privacy Policy – Privacy Policy[123]
GreenQloud has a privacy policy that outlines its position on protecting the privacy of its clients. The policy does not make any references towards legislation, however.

[121] GreenQloud "End User License Agreement" Section 6
[122] GreenQloud "End User Agreement" Section 10.
[123] "Privacy Policy." GreenQloud Privacy Policy Comments. https://www.greenqloud.com/privacy-policy/ (accessed May 19, 2014).

Appendix A
Project Proposal – North American Team Project 10

Title: Contract Terms for Cloud-based Record Keeping Services

Target domain: Infrastructure

Rationale: The proposed study is intended to contribute to understanding the degree to which contracts can be trusted to mitigate known record keeping risks. Through this understanding new or revised "boiler-plate" contract terms may be developed as a ITrust product.

Description: Cloud-based services (CBS) and the technological infrastructure (s/w, h/w) are primarily set by the vendors of these types of services and secondarily by the purchaser's needs/expectations. Terms of contracts for CBS thus represent interests from two perspectives: i) the service provider; ii) the purchaser.

Through empirical analysis, the research will

- categorize terms found in available contracts relating to record keeping requirements [to be defined within the context of ITrust] in terms of commonality or frequency of appearance;
- determine, to the degree possible, whether the terms represent primarily the interests of the service provider or the purchaser;
- categorize the types of services purchased, distinguishing, to the degree possible, which services are most commonly purchased;
- relate the terms, to the degree possible, to types of organizations, e.g., government, health sector, financial sector, etc.,
- Either relate the terms, to the degree possible, to a generally accepted (within the IT community) categorization of technological infrastructure; or use the terms themselves as a means to categorize cloud infrastructure from a specifically record keeping perspective. [The option selected might be dependent on the information that was gathered.]

Sources

- public sector service contracts (NB: this may require making access to information requests);
- statements of requirements from tender documentation issued to industry, i.e., Requests For Information/Proposals/Offers/etc.
- Standard or template CBS provider contracts;
- Industry articles and reports, e.g., Gartner, etc.

- Definitions, standards and studies by standards organizations, e.g., National Institute of Standards and Technology.
- Guidelines published by the record keeping community regarding record keeping in the cloud, such as
    - "Records management and the cloud" (National Archives of Australia)
    - FAQ "About Managing Federal Records in Cloud Computing Environments" (U.S. National Archives and Records Administration)
    - Advice on managing recordkeeping risks associated with cloud computing (Council of Australasian Archives and Records Authorities)
- Scholarly articles

Anticipated outcomes

A monograph, with detailed bibliography, that provides:

- A categorization of CBS infrastructure (based on contract terms) from a record keeping perspective
- A preliminary identification of gaps between services offered and services required. [Preliminary because those gaps may be addressed through means other than contract terms.]

Other potential outcomes, depending on the information available, might include preliminary information on conditions and costs of services.

Anticipated value of research:

- The categorization of CBS infrastructure will help set scope and context for further IP Trust research studies.
- The preliminary identification of gaps will inform development of model policies/contracts/risks relating to maintaining authentic records within cloud-based environments.

Timing: It is recommended that this study be undertaken as early as possible in the project as its value will likely diminish as other studies get underway.

Estimated effort: GRA for 8 weeks @ 40 hours/week. NB: if access to information requests are made, this period may be extended but also may not require GRA full-time for the longer period.

Recommended Lead: No lead recommended.

Appendix B
Annotated Bibliography

Amazon.com, "AWS Customer Agreement." Last modified March 15, 2012. Accessed February 5, 2014. http://aws.amazon.com/agreement/.

Amazon.com, "Amazon S3 SLA." Last modified June 01, 2013. Accessed February 5, 2014. http://aws.amazon.com/s3/sla/.

Amazon.com, "Products & Services." Accessed February 3, 2014. http://aws.amazon.com/products/.

ARMA International. “Generally Accepted Recordkeeping Principles.” (2013). Retrieved from http://www.arma.org/r2/generally-accepted-br-recordkeeping-principles.

Barnes, Frederick. ARMA International, "Putting a Lock on Cloud-Based Information." Last modified 2010. Accessed November 17, 2012. http://content.arma.org/imm/JulyAug10/ IMM0710puttingalockoncloud-basedinformation.aspx.

This article is a non-academic work that seeks to provide Records Managers with an introduction to cloud storage technologies. The article briefly summarizes what the technology is and its various iterations. It then briefly outlines seven concepts that records managers should consider before using the cloud for information storage: privilege user access, regulatory compliance, data location, data segregation, recovery, investigative support, and long-term viability. The article goes on to describe five layers of protection that a client and service provider should implement to protect data in the cloud. This article is useful because it very concisely describes professional concerns about cloud storage.

Baset, Salman. "Cloud SLAs: Present and Future." *ACM SIGOPS Operating Systems Review*. no. 2 (2012): 57-66.

This article is a study funded by IBM comparing the terms found within the Service Level Agreements of five cloud service providers. The study found that SLAs tend to differ in their use of jargon, how they measured timeframes, and how they measured accessibility. The study also found that the SLAs are primarily worded for the protection of the service providers, and that most SLA’s place the responsibility for reporting outages on the cloud service clients.

Blair, Barclay T. "How to Manage Information Governance Challenges." Last modified 2010. Accessed November 17, 2012. http://www.arma.org/HotTopic/HotTopic910.pdf.

This article is a non-academic work that seeks to describe the challenges of the cloud from a records management perspective. The article briefly describes how the cloud works as “hardware as a service” and as “software as a service”. It

then describes six concerns that exist with the use of cloud storage for information within organizations: availability of information, e-discovery, retention, privacy, use of multiple providers, and the portability of information. It concludes by offering ways in which the records manager can become involved early in the process of implementing these services so as to ensure that records are protected.

Cloud Security Alliance, "Top Threats to Cloud Computing V1.0." Last modified March 2010. Accessed February 4, 2014.
This White Paper seeks to describe the various threats to information that can exist for an organization that utilizes cloud technology. It describes seven threats: Abuse and Nefarious Use of Cloud Computing, Insecure Application Programming Interfaces, Malicious Insiders, Shared Technology Vulnerabilities, Data Loss/Leakage, Account, Service & Traffic Hijacking.

CloudSigma "Service Level Agreement." Last updated November 11, 2013. Accessed February 3, 2014, http://www.cloudsigma.com/legal/service-level-agreement/.

CloudSigma. "Terms of Service." Last updated July 1, 2013. Accessed February 3, 2014, http://www.cloudsigma.com/legal/terms-of-service/.

CloudSigma. "Terms of Use." Last updated July 15, 2013. Accessed February 3, 2014, http://www.cloudsigma.com/legal/terms-of-use/.

Council of Australasian Archives and Records Authorities. "Advice on managing the recordkeeping risks associated with cloud computing." *ADRI*. (2010).
This paper seeks to provide information and advice to archives of the Australasian region on the nature of cloud computing and the implications its use has for records stored within.

City Network. *General Conditions for My City Cloud*. Last updated 2011. Accessed February 3, 2014, https://www.citycloud.com/wp-content/uploads/2011/09/SLA-City-Cloud-eng.pdf.

City Network. "SLA (Service Level Agreement) – Dedicated servers, co-location and virtual servers." No updated date. Accessed February 4, 2014, https://www.citynetworkhosting.com/sla-service-level-agreement-dedicated-servers-co-location-and-virtual-servers. /.

Cunningham, Patrick. "IT's Responsibility for Security, Compliance in the Cloud." *Hot Topic: Making the Jump to Cloud*. : 6-10.
This article is part of a series of three articles published by ARMA International for organizations planning on moving into the cloud. This article presents an IT perspective, out-ling some of the risk that organizations will face as they place their records into cloud storage and IT's responsibilities to mitigating said risks.

Economist Intelligence Unit, "Business Resilience: Ensuring Continuity in a Volatile Environment." Last modified 2007. Accessed November 17, 2012. http://graphics.eiu.com/files/ad_pdfs/eiu_Bus_Resilience_wp.pdf.

This article is a non-academic work that provides the results of a study conducted on 181 executives from 500-million+ profit businesses around the world. The study sought to understand what challenges and opportunities executives faced in business resilience and found that data availability was a primary concern for many, with a lack of data availability being catastrophic for many businesses. This study was sponsored by ACE, IBM and KPMG.

European Commission. "MoReq2 Specification." (2008). http://www.moreq2.eu/moreq2

Ferguson- Boucher, Kirsten. "Cloud Computing: A Records and Information Management Perspective." *Security & Privacy, IEEE*. 9. no. 6 (2011): 63 - 66.

This article seeks to outline the concerns and considerations that records manager should be aware of as their organizations move information into the cloud. The paper begins by briefly explaining cloud computer and the different models that are available. It then lists some benefits of moving to the cloud as well as RIM concerns: compliance e-discovery; integrity and confidentiality; service availability and reliability; service portability and interoperability; information retrieval and destruction; and loss of governance, integration, and management. The paper then discusses how the cloud affects an organization's responsibility for their records and states that policies and procedures will need to be amended to incorporate the changes brought by the cloud, but does not state specifically what the changes should be. In regards to litigation it then states that contracts should ensure that records are available and reliable in the case of litigation. The paper wraps up by stating it is up to each organization to determine what information it is willing to store in the cloud, which the paper has established as a uncertain environment.

Google Inc., " Google Cloud Platform Terms of Service." Last modified December 16, 2013. Accessed February 5, 2014. https://developers.google.com/cloud/terms/.

Google Inc., " Google Cloud Storage, Google Prediction API, and Google BigQuery SLA." Accessed February 5, 2014. https://developers.google.com/storage/sla.

Google Inc., "App Engine." Accessed February 3, 2014. https://cloud.google.com/products/app-engine/?utm_source=google&utm_medium=cpc&utm_campaign=appengine-search&gclid=CPHg26nVsbwCFY1FMgodjR8AKw.

Google Inc., "Products." Accessed February 3, 2014.

https://cloud.google.com/products/.

Hickling Arthurs Low, Science & Technology Policy Research and Analysis Resource team. "Primer on Policy Implications of Cloud Computing." *Government of Canada*. (2012).

This paper was developed to advise agencies of the federal government on moving information and records into the cloud. It provides an overview of cloud services, describes the problems and risks that are associated with records stored in the cloud, and provides examples of how information has been placed into the cloud by public bodies, primarily geographic information.

Industry Engagement Day - GCNet Wan – July 9, 2013. Shared Services Canada. http://www.ssc-spc.gc.ca/pages/telecomm_gcnet-eng.html. Accessed February 4, 2014

ISO 15489 - Information and Documentation - Records Management, (International Standards Organization, 2001)

Ju, Jiehui, Jiyi Wu, Jianqing Fu, and Zhijie Lin. "A Survey on Cloud Storage." *Journal of Computers* 6. no. 8 (2011): 1764-1771.

This article is an attempt to explain cloud storage from a RIM and technical standpoint. The paper identifies what is calls determinators that must be in place to make cloud storage valuable: elasticity, automatic, scalability, data security, performance, reliability, ease of management, ease of data access, energy efficiency, and latency. It then identifies the various cloud services that are commonly offered by service providers and describes the benefits and detractions for each of these services, particularly in relation to RIM needs.

Kundra, Vivek. *Federal Cloud Computing Strategy*. February 8, 2011. Accessed February 3, 2014 from https://www.dhs.gov/sites/default/files/publications/digital-strategy/federal-cloud-computing-strategy.pdf.

This document was issued following the announcement of the US government's "Cloud First" policy. It defines the cloud and gives guidelines for federal agencies to adopt the cloud, including the use of a decision framework.

Lifka, David, Ian Foster, Susan Mehringer et. al. *XSEDE Cloud Survey Report*. September 2013. http://net.educause.edu/ir/library/pdf/CSD6239.pdf Accessed 2014-02-04.

This paper is the result of a survey conducted from September 2012 to April 2013 by the XSEDE Cloud Integration Investigation Team to understand how cloud is used across a wide variety of scientific fields and the humanities, arts, and social sciences. Data was collected from 80 cloud users from around the globe. The paper gives good primary information about cloud usage in post-secondary research and education.

National Archives and Records Administration. Government of the United States of America,
"Frequently Asked Questions about Managing Federal Records In Cloud Computing Environments." Accessed November 22, 2013. http://www.archives.gov/records-mgmt/faqs/cloud.html.

National Intitute of Standards and Technology. Special Publication 800-53, *Security and Privacy Controls forFederal Information Systems and Organizations*, Revision 4, Joint Task Force Transformation Initiative, U.S. Department of Commerce, April 2013, 460 pp., http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

National Institute of Standards and Technology. Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*, Revision 1, Joint Task Force Transformation Initiative, U.S. Department of Commerce, June 2010, 399 pp., http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf.

Ponemon Institute LLC, "Flying Blind in the Cloud: The State of Information Governance." Last modified 2010. Accessed November 17, 2012. http://eval.symantec.com/mktginfo/ enterprise/white_papers/b-ponemon_institute_flying_blind_in_the_cloud_WP.en-us.pdf.
This study was undertaken by the Poneman Institute on behalf of Symantec, Inc.

Profit Bricks. “General Terms & Conditions of Service.” Last updated December 3, 2014. Accessed February 3, 2014, http://www.profitbricks.com/sites/default/files/pb_generaltermsandconditionsofservice_us.pdf
Provides some general recommendations regarding moving to the cloud and what the benefits and concerns are, makes a few direct references to records management principles. States that contracts should ensure that the functionality for records is maintained, the links to metadata is maintained, and disposal is ensured. Outlines concerns of cloud storage: Security, ownership and control of data, data migration. Lists three requirements for RM that may not be fulfilled by cloud storage services: maintaining functionality and integrity, linking record and metadata, disposal (transferring records to NARA and destroying records that are no longer required according to retention schedule).

Open Text “Open Text Cloud Services Agreement.” No updated date. Accessed February 3, 2014, http://semanticnavigation.opentext.com/terms-and-conditions/.

Open Text “SLA (Service Level Agreement) – Dedicated servers, co-location and virtual servers.” No updated date. Accessed February 4, 2014, https://www.citynetworkhosting.com/sla-service-level-agreement-dedicated-

servers-co-location-and-virtual-servers. /.

Pathway Communications. “CloudPath Terms and Conditions.” Last updated August 14, 2013. Accessed February 3, 2014, http://cloudpath.pathcom.com/terms/.

Pathway Communications. “CloudPath Service Level Agreement.” Last updated February 1, 2011. Accessed February 3, 2014, http://cloudpath.pathcom.com/sla/.

Ponemon Institute LLC, "Flying Blind in the Cloud The State of Information Governance." Last modified 2010. Accessed November 17, 2012. http://eval.symantec.com/mktginfo/enterprise/ white_papers/b-ponemon_institute_flying_blind_in_the_cloud_WP.en-us.pdf.

This article is a study sponsored by Symantec and conducted by the Ponemon institute on the use of cloud services within organizations around the United States of America and how the organizations deal with the increased risk of the technology to their information. The study found that cloud storage and software-as-a-service are the most popular and that few organizations are vetting the cloud the way they vet other services, decisions are being made by individual employees without the input of IT, few organizations are taking proactive steps to protect themselves from risks associated with the cloud, amongst other findings.

Rackspace, "Cloud Terms of Service." Last modified October 22, 2013. Accessed February 5, 2014. http://www.rackspace.com/information/legal/cloud/tos.

Rackspace US Inc, "Cloud Files SLA." Last modified January 21, 2011. Accessed January 24, 2014. http://www.rackspace.com/information/legal/cloud/sla.

Rackspace, "Rackspace Private Cloud." Accessed January 26, 2014. http://www.rackspace.com/cloud/private/.

Rackspace Inc. "Understanding The Cloud Computing Stack SaaS, Paas, IaaS." *CloudU*. (2011).

Rennie, Stuart. "Legal Implications of Working in the Cloud." *Hot Topic: Making the Jump to Cloud*. : 11-16. http://www.arma.org/docs/hot-topic/makingthejump.pdf (accessed February 4, 2014).

This article is part of a series of three articles published by ARMA International for organizations planning on moving into the cloud. This article presents a legal perspective, out-ling some of the risk that organizations will face as they place their records into cloud storage.

Ruttrell, Yasin. NARA moved email to the cloud at ‘lightning speed’, GCN, December 17, 2013. http://gcn.com/articles/2013/12/17/nara-cloud-email.aspx. Access 2014-01-06.

State & Local Government Cloud Commission. *The Cloud Imperative: Better Collaboration, Better Service, Better Cost*. February 2012. 48 pp. TechAmerica Foundation (SLG-CCA. Accessed February 3, 2014, http://www.techamerica.org/Docs/fileManager.cfm?f=taf_slg_cc.pdf

This paper outlines cloud implementation practices and procedures for local and state governments. Aside from definitions of the cloud, the paper gives recommendations for cloud implementations and defines key contract terms for state and local government officials.

Stuart, Katharine, and David Bromage. "Emerald Article: Current state of play: records management and the cloud." *Records Management Journal*. 20. no. 2 (2010): 217 - 225. http://dx.doi.org/10.1108/09565691011064340 (accessed November 17, 2012).

This paper outlines the implications of the cloud to records management. The primary audience of this article is records managers and archivists and the article discusses topics on a level that takes this into account, incorporating topics such as diplomatics into its treatment of the issue. The article discusses issues of the lack of fixity, control, destruction, security (including challenges on over taxed virtual machines that cannot generate enough random numbers for encryption), challenges in preserving the records in their context, records stored in the cloud lacking traditional records management treatment, and an inability to access the records. The article concludes by stating that organizations must develop policies and procedures for the cloud prior to moving information into it at all and outlining questions that must be asked of service providers:

· "Asking where the records will be stored and processed and trying to find jurisdictions that are complementary to their own;
· Seeking contractual agreements to obey privacy requirements;
· Seeking assurance that at the termination of the contract, no trace of the records will be retained by the provider; and
· Understanding how the provider backs up stored information and can restore your information in case of emergency."

U.S. Department of Defense. "Electronic records management software applications design criteria standard." (2007). Retrieved from http://www.dtic.mil/whs/directives/corres/pdf/501502std.pdf

Appendix C
Legal Cases

compiled by Daniel Collins

Privacy

***United States v. Mitch Miller*, [April 1976], United States Supreme Court, (Washington DC)**

This case took place long before the term cloud computing became part of the common lexicon but still has implications for how the United States protects personal data.

The Court requested bank documents to convict Miller on charges of tax evasion on alcohol distilling equipment he owned. The banks complied and turned over the requested documents. When brought to Court, the defendant claimed that the bank had conducted an unreasonable search under the Fourth amendment. The Court ruled that information revealed to third parties is not protected and that it is the responsibility of the information owner to trust that the third party will only use the information for the purposes it intended.

***State of Oregon v. Donald Lee Bellar*, [August 2008] The Court of Appeals of the State of Oregon, (Salem, Oregon)**

This case does not involve cloud computing directly but could have future implications for the privacy of individuals who submit data to others. The defendant gave his computer to a repair technician who found images of child pornography. The technician transferred these files to a CD and submitted them to the police. As a result, the defendant Bellar was charged with 40 counts of encouraging child sexual abuse in the second degree.

In this case the judge stated that: “Nor are a person's privacy rights in electronically stored personal information lost because that data is retained in a medium owned by another. Again, in a practical sense, our social norms are evolving away from the storage of personal data on computer hard drives to retention of that information in the "cloud" of servers owned by internet service providers. That information can then be generated and accessed by hand-carried personal computing devices. I suspect that most citizens would regard that data as no less confidential or private because it was stored on a server owned by someone else.”

This opinion suggests that the privacy of Bellar was not lost when the material was transferred to the CD owned by the technician and that Bellar had a reasonable right to privacy on both the CD and his own computer hard-drive and indicates a change from the first case cited above. This has implications for cloud users in that data saved

in the cloud should be afforded the same expectation of privacy as that stored on one's own personal computer, but this is not always the case as seen in the next case.

***Charles A. Rehberg v. James P. Paulk*, [March 2010], United States Court of Appeals, (Dougherty County, Georgia)**

Rehberg was charged with harassment when copies of his e-mails were acquired by investigators. The defendant argued that this was a breach of his Fourth amendment right to protection from unlawful searches. Following appeal, the court ruled that the reasonable expectation of privacy was relinquished when the e-mails were sent because they were "voluntarily turn[ed] over to third parties." E-mails received by a recipient were found to no longer be protected by the Electronic Communications Privacy Act (ECPA), the Privacy Protections Act (PPA), the First Amendment or the Fourth Amendment.

The implications of this ruling could be significant for cloud computing if data sent to the cloud is no longer protected by theseActs, if given voluntarily. Users would have to attempt to protect the privacy of their information through the terms and conditions included in cloud service provider contracts.

Storage and Copyright

***Columbia Pictures Industries. v. Bunnell,* [June 2007], United States District Court, (CD, California)**

Columbia Pictures brought a suit against the owners of a website where users could download movies and television shows via peer-to-peer networks using BitTorrent files. Columbia Pictures requested that Bunnell preserve and produce its server log data. On appeal, the defendant argued that it could not meet the discovery demand since it recently employed a third-party data management provider who did not log this data. The court found that the defendant had intentionally routed the data through the third party and therefore was in "possession, custody and or control" of the data by being able to "manipulate at will" how the data was routed.

This case laid the groundwork for future e-discovery in the cloud, in that individuals or companies who use third-party storage of data can still be required to produce data and documentation upon an e-discovery request or face charges of spoliation of evidence. The third party in this case was also operating from the Netherlands. The judge dismissed the defendants claim that they were protected under Dutch law, also raising issues of jurisdiction. The defendant was ordered to preserve transient data stored in the third party's RAM (Random Access Memory) which raises interesting questions about the fixity of the records, since the content of the RAM is normally lost when a computer is powered down.

Cartoon Network v. CSC Holdings, Inc. **[August 2008], United States Court of Appeals, (Washington DC)**

The Cartoon Network brought a case against Cablevision, a cable network provider, for releasing a cloud-based remote storage digital video recorder system (RS-DVR) so users could record and re-watch shows at their leisure. The court ruled against the plaintiff in this case on the grounds that the shows were not meant to be distributed publicly. Also, the court claimed that because the copyrighted material was transferred to buffers where they remained for 1.2 seconds and were overwritten as soon as it was processed, this material did not count as a 'copy' under the Copyright Act. Also, because they were recorded by the user at their will, they were deemed to have been 'created' by them and therefore did not count under the Copyright Act as a genuine copy.

This case was somewhat unusual given the new technology, however the implications for cloud contracts seems to be that individuals or companies who use the cloud to distribute copyrighted material are leaving themselves open to being sued by the copyright owner. Contracts with cloud service providers should generally contain a section clarifying ownership and thus copyright of any material being stored in the cloud with a third party.

Arista Records, LLC v. Usenet.com, Inc.**, [June 2009] United States District Court, (S.D. New York)**

USENET Network, a cloud-based bulletin board site, allowed users to post messages or files and download files posted by others. A case was brought against them by a number of recording companies who felt this infringed on their rights by making their copyrighted material available to the public. The court found that USENET had encouraged copyright infringement and were promoting file sharing online. Similar to earlier cases like Napster, the website was ordered to shut down operations.

The case here is quite simple in that users operating in the cloud cannot make copyrighted material available to the public which has led to such clauses being included in cloud computing contracts that followed this ruling.

Jurisdiction

Pro-C Ltd. v. Computer City, Inc.**, [2001] Ontario Court of Appeal, (Ottawa, ON)**

Pro-C was the owner of the WINGEN trademark which was registered in the United States and Canada. Computer City began selling computers under the WINGEN name on their website solely to American customers. Seeing the advertisement,

Canadian customers then flocked to the Pro-C Website, www.wingen.com, causing it to crash, resulting in a loss of business for Pro-C. The trial judge, based in Canada, found that Computer City were in breach of copyright law and ordered them to pay damages, despite Computer City not selling computers to Canadian customers. However, upon appeal the ruling was overturned, with the judge claiming that there was no active attempt to sell the WINGEN brand to Canadian customers.

This case set an interesting precedent for cases involving the internet and jurisdiction. The case identified two specific elements for testing whether the courts will exercise jurisdiction over a website or web service: (A) whether or not the business is actively engaged in commercial activity with individuals or businesses, and (B) the extent to which the hosting organization has knowledge that they are making sales to residents of a particular region. In the case of Canada, the extent to which a company will directly target Canadians in their marketing will determine whether or not Canadian courts can claim jurisdiction over the provider of the service.

This case has implications for both the consumer and the provider of cloud services. The way in which the cloud service is advertised and the provisions laid out in the contract, will determine what jurisdiction might apply. A number of cloud contracts contain clauses which state specifically the jurisdiction in which challenges will take place. This serves to protect the consumer and the provider so that they cannot be challenged based on differences in the laws of other jurisdictions.