Guideline for Outsourcing Records Storage to the Cloud

An ARMA International Guideline
# TABLE OF CONTENTS

Foreword ........................................................................................................................................... v

Acknowledgments ............................................................................................................................ vi

1 Scope and Purpose ....................................................................................................................... 1
   1.1 Scope ...................................................................................................................................... 1
   1.2 Purpose .................................................................................................................................. 1

2 Definitions .................................................................................................................................... 2

3 Exploring the Cloud .................................................................................................................. 3
   3.1 Characteristics of Cloud Computing ..................................................................................... 3
   3.2 Cloud Solutions ......................................................................................................................... 4
      3.2.1 Software as a Service (SaaS) .......................................................................................... 4
      3.2.2 Hosted Applications ......................................................................................................... 4
   3.3 Benefits and Risks of the Cloud ............................................................................................. 4
      3.3.1 Benefits ............................................................................................................................ 4
      3.3.2 Risks ................................................................................................................................ 5

4 Information Retention and Disposition ................................................................................... 6

5 Other Technology Issues ......................................................................................................... 7
   5.1 APIs to Records Management Systems ............................................................................... 7
   5.2 Virtual Storage ......................................................................................................................... 7

6 Legal Considerations ................................................................................................................. 8
   6.1 General .................................................................................................................................. 8
   6.2 Records Preservation for Litigation....................................................................................... 8
   6.3 Ephemeral Data ....................................................................................................................... 9
   6.4 The Transnational Problem .................................................................................................. 9
   6.5 Recommendations to Mitigate Legal Risk ........................................................................... 10

7 Vendor-Related Considerations ............................................................................................... 11
   7.1 Information Management Practices ..................................................................................... 11
   7.2 Access Interruptions .............................................................................................................. 12
   7.3 Privacy .................................................................................................................................. 12
   7.4 Subcontracting ....................................................................................................................... 12
   7.5 Multi-Tenancy ....................................................................................................................... 13
   7.6 Public vs. Private Clouds ...................................................................................................... 13
   7.7 Data Location ......................................................................................................................... 14
   7.8 Data Backup and Recovery ................................................................................................... 14
   7.9 Data Retention ....................................................................................................................... 15
   7.10 Physical Security .................................................................................................................. 15
   7.11 Environmental Conditions .................................................................................................. 15
   7.12 Network Access .................................................................................................................. 15
7.13 Uptime ..................................................................................................................................................................................15
7.14 Vendor Continuity ....................................................................................................................................................................16

8 Standards and Best Practices........................................................................................................................................................16

9 Summary ....................................................................................................................................................................................16

Appendix A : Checklists and Questionnaire ............................................................................................................................17
   A.1 Cloud Technology Checklist ..............................................................................................................................................17
   A.2 Legal Issues Checklist ..........................................................................................................................................................18
   A.3 Vendor Concerns Questionnaire .....................................................................................................................................19

Bibliography ................................................................................................................................................................................21

About ARMA International..............................................................................................................................................................22
There has been much hype around cloud computing—referred to in this guideline as “the cloud.” Many organizations are either jumping on the bandwagon or dipping their toes into the water, but most are still talking about whether to take advantage of this new trend. As with any new technology, there are many issues to consider before using the cloud for records and information management (RIM). RIM professionals should be ready to highlight the RIM-related concerns and assist with decision making when cloud services are under consideration by the organization. This guideline cuts to the core of those issues with a concise and focused discussion.

Readers are also encouraged to consult the following ARMA International guidelines on related topics:

- Website Records Management
- Guideline for Evaluating Offsite Records Storage Facilities
- Guideline for Outsourcing Electronic Records Storage and Disposition

As well, ARMA International’s Generally Accepted Recordkeeping Principles® (GARP®) may provide helpful information to users of this publication. Refer to the Bibliography for complete citations of these publications or consult the ARMA International website (www arma.org).
ACKNOWLEDGMENTS

ARMA International gratefully acknowledges the contributions provided by the following individuals who were instrumental in the development of this guideline. Company affiliations listed are those on record with ARMA International at the time of printing.

Project Leader:
Galina Datskovsky, Ph.D., CRM – Autonomy, Fair Lawn, NJ

Project Team Members:
Debra Logan – Gartner, Stamford, CT
Carol E. B. Choksy, Ph.D., CRM, PMP – Indiana University, Bloomington/Greenwood, IN
Ronald J. Hedges, J.D. – Ronald J. Hedges LLC, Hackensack, NJ
Brent Gatewood, CRM – PelliGroup Consulting, Waukesha, WI
Glen R. Sanderson, CRM – Infosys BPO, Houston, TX

With appreciation, the following ARMA International staff member and consultant are recognized for their assistance: Vicki Wiler, Director of Publications, and Nancy D. Barnes, Ph.D., CRM, CA, Standards Consultant for ARMA International.
1 • Scope and Purpose

1. Scope and Purpose

1.1 Scope
This guideline discusses cloud-based solutions for records and information management (RIM). These include software as a service (SaaS) and hosted applications. After providing a brief explanation of the cloud in general, this guideline investigates RIM and legal issues when using cloud technology. Checklists and questionnaires are provided in the Appendix to aid in decision making when an organization is considering the outsourcing of records storage to cloud service providers.

This guideline does not address the outsourcing of long-term storage of electronic records.

1.2 Purpose
The purpose of this guideline is two-fold:

1. to offer guidance for professionals in records management, information technology, and legal settings regarding outsourcing information and records storage and access to the cloud, and

2. to provide assistance with decision making (via checklists) so that outsourcing information to the cloud will move forward more efficiently and effectively while minimizing risks to the organization.
2 Definitions

This section contains definitions of terms central to this document. Definitions marked [ARMA – Glossary] are taken from ARMA International’s Glossary of Records and Information Management Terms, 3rd edition. The definitions marked [7 Steps] are from 7 Steps for Legal Holds of ESI and Other Documents by John J. Isaza and John Jablonski. See the Bibliography for complete citations for both publications.

**application programming interface (API)**
A language and message format used by an application program to communicate with the operating system or some other control program such as a database management system or communications protocol. [ARMA – Glossary]

**elasticity**
The ability to rapidly change the provision of computing resources to scale up or down as needed.

**encryption**
The rendering of electronic data or documents unintelligible to unauthorized users.
[ARMA – Glossary]

**firewall**
A computer security mechanism that is designed to control access to or from a specified system according to the network policy. [ARMA – Glossary]

**hosted application**
A software application that runs on another party’s computer rather than on a system owned and operated by the using organization.

**legal hold**
An affirmative act by an organization to prevent the destruction of documents, including physical documents on paper as well as electronically stored information (ESI), which are relevant to a lawsuit or governmental investigation. [7 Steps]

**multi-tenancy**
The process of running a single instance of software on a server with access to multiple client organizations.

**resource pooling**
A computer systems management technique where computing resources (e.g., servers, software, or data storage) are collectively used by multiple organizations (clients).

**software as a service (SaaS)**
A computing delivery model where software is provided, usually remotely, on the provider’s computers and is used on demand. Payment is often by subscription or metered use.

**spoliation**
The legal term courts in the United States use to describe the intentional or negligent destruction of evidence. [7 Steps]

**scalable**
The ability of a computer system, application, or product—either hardware or software—to be easily increased in size or volume to meet a user need.

**virtualization**
The capability to run multiple virtual machines—each with its own operating system, applications, and data—on a single physical machine in such a way that each virtual machine is independent of the underlying hardware.
3 Exploring the Cloud

3.1 Characteristics of Cloud Computing

As with any new technology, the definition of cloud computing is still evolving and may mean different things to different people. According to Gartner, the definition of cloud computing is:

“A style of computing where scalable and elastic IT-enabled capabilities are delivered as a service to external customers using Internet technologies.”

A second definition comes from the National Institute of Standards and Technology (NIST):

“Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

A comparison of the Gartner and NIST definitions of cloud computing shows five essential and defining characteristics that are broadly overlapping as shown in Table 1.

| Table 1: Comparison of Gartner and NIST Defining Characteristics for Cloud Computing |
|-------------------------------------------------|-----------------|-----------------|
| Gartner                                         | NIST            | Difference      |
| 1. Massively scalable and elastic               | 1. Rapid elasticity | None (NIST includes scalability in its description of elasticity.) |
| 2. Shared                                       | 2. Resource pooling        | None            |
| 3. Delivered as a service                       | 3. On demand self service | Gartner does not specify self service. |
| 4. Uses Internet technologies                   | 4. Broad network access    | NIST does not specify Internet technologies. Gartner’s definition is a superset of NIST. |
| 5. Metered by use                               | 5. Measured service       | None            |

These defining characteristics lead to an array of choices for those who are considering cloud computing. Scalability drives down the cost of the services because the user can take advantage of the vendor’s economies of scale, which are spread across multiple clients. Elasticity, which builds on the concept of scalability, further emphasizes the ability to easily move both up and down in capacity as needed. Depending on the vendor’s policies and the services contracted, this change in available capacity level can occur automatically or be requested as needed.

Cloud computing shares computing resources among many users from different organizations. NIST calls this “resource pooling.” The service provider’s computing resources are shared dynamically among many clients who are generally unaware of the exact physical location of the resources in use or their application data. Shared resources used by multiple users can lower the cost compared to individual ownership of similar resources because there is less idle time.


Cloud computing is delivered as a service. Clients pay for usage of the services, rather than making a fixed investment in physical assets. Therein lies the appeal of the cloud business model—not owning or having to manage the physical assets while also having the flexibility to turn services on and off as required. Organizations are charged only for the services they use. This model provides for financial flexibility and offers an operational expenditure versus a capital expenditure.

Cloud computing uses Internet technologies. Use of the Internet as a delivery tool enables pervasive and accessible standardization. Cloud computing is outward facing and does not make any assumptions about its users, only that they have access to the Internet for basic connectivity. Services are loosely coupled using Internet identifiers, formats, and protocols. Service assembly, orchestration, and control are managed using web-oriented architectures or web technologies such as Really Simple Syndication (RSS).

The business model for cloud computing necessitates that the services be measured as they are billed entirely on demand or based on metered usage, which can vary in any given billable time period. If contracted and managed correctly, this feature may also provide cost savings over in-house computing.

3.2 Cloud Solutions

3.2.1 Software as a Service (SaaS)

Software as a service (SaaS) is a term that has been around since the late 1990s. With SaaS, the software is owned and/or managed remotely by one or more providers and accessed by users with web browsers over the Internet. SaaS solutions generally use resource pooling and are often built on cloud infrastructures, but do not necessarily have all the characteristics of the cloud. For example, a SaaS provider need not be massively scalable to deliver value.

3.2.2 Hosted Applications

A hosted application is similar to SaaS in that it does not run on the user’s own system; however, unlike SaaS, the application infrastructure is dedicated on an organization-by-organization basis. Therefore, it does not achieve economies of scale in the same way as SaaS. Hosted applications, which also may or may not utilize the cloud, trade security and control for the lower cost and flexibility of SaaS.

3.3 Benefits and Risks of the Cloud

The benefits and risks of the cloud flow directly from its characteristics. The benefits fall into two broad categories: cost savings and value creation. The enumerated risks require that an organization fully understands the functionality of the cloud service(s).

3.3.1 Benefits

3.3.1.1 Cost Savings

Cost savings from using a cloud service can result from several aspects:

- Because it is a metered service, organizations can often pay for actual usage. They also have better data to manage how the service is utilized and to do accurate cost-benefit calculations.
- Cloud computing expenditures are operational rather than capital. The cycle of planning and approval for capital monies will typically result in a longer time-to-implementation than when contracting for a cloud service—and in business, time is money. Additionally, the operational expenditures do not require all the costs to be spent up-front.
• With the scalability and elasticity characteristics of the cloud, the needed capacity can expand and shrink, often on demand, with the organization paying more or less as its demand warrants. For many organizations, this flexibility is appealing.

• Some if not all IT developments costs can be eliminated as the application has already been developed (although organizational set-up or customization may still be required). Since large IT projects can sometimes go over budget and beyond the projected timeline, use of a cloud service may provide better cost controls and result in faster implementation.

3.3.1.2 Value Creation

The second category of benefits is value creation, which could include, but is not limited to the following:

• Application development that would not be technically or economically feasible in an enterprise application could be feasible if done in the cloud.

• Organizations can launch new services for internal or external use and then increase or decrease scope as needed.

• Since the capital outlay is zero, there is opportunity for low-cost experimentation and even project failure in a way that does not waste significant time and/or money. Failing small in the cloud and learning from the experience can speed development cycles and increase efficiencies in future projects.

3.3.2 Risks

There are risks associated with the cloud that may need to be mitigated prior to outsourcing:

• Accessibility – Many providers may state they have 24/7 access. But this is difficult to guarantee. Find out what the provider is doing to prevent access outages, e.g., mirroring of servers at different locations, alternate Internet routing for network outages, etc.

• Data security – The security of the organization’s data and access to the application is completely dependent on the service provider’s policies, controls, and staff. Before contracting with the organization, determine what these controls are and if they are as good as or better than internal controls would be. If the organization is placing data in the cloud that is a potential target for legal document requests (e.g., e-mail), the organization must have a protocol and an agreement with the provider to lock down the data (initiate a legal hold) in the face of an obligation to preserve it to avoid spoliation issues and unwanted sanctions.

• Data location – Sharing resources can mean, in the worst-case scenario, that data and applications are not in a specific, physically identifiable location. Because many cloud providers are global enterprises, they have the ability to share resources and data in physical locations around the world. Certain geographies, most notably the European Union countries, have strict data protection and privacy regulations forbidding data transfer beyond specific borders. Indeed, certain individual countries have very strict regulations. The pooling and sharing of resources may, by definition, violate these requirements. (See section 6.4 for more on transnational issues.)

• Data segregation – When multiple organizations are sharing an application and resource, e.g., the same server, it is critical to know and understand the methods used to
segregate and protect each organization’s data from the others. Commingling of data can make subsequent segregation problematic, and confidential data could be inadvertently shared with others.

- **Data integrity** – Backup and recovery of the entire application, not just the data, should be included in the provider’s services. From a records perspective, it is equally important that backup data is destroyed when required by retention schedules. Audit trails are also needed to prove the integrity of electronic records’ creation, change, and destruction. The provider may use third parties to back up and secure its repositories. If so, the location of the third-party facilities adds to the data location issue mentioned above.

- **Data ownership** – Most organizations assume they own their data, but that is not always the case or not necessarily straight-forward. If a contract is canceled or not renewed, does the organization get its data back and how quickly? If there is a contract dispute, can the service provider hold the organization’s data hostage? What happens in the event the provider goes bankrupt or is acquired by another organization? There is also an issue of separating the data and the application; without the application’s context, is the data still understandable and usable?

Organizations must understand the functionality of the particular cloud-based software utilized to allay the potential risks. And, if using social networking in relation to cloud services, it is important to remember that any electronically created and stored information developed or used during the routine course of business is subject to an organization’s recordkeeping requirements and legal scrutiny.

Storing data or using applications in the cloud does not relieve the organization of the responsibility for the protection or management of its data. When it comes to security and risk, there are obligations to consider. The organization must ensure that private data, or data with a limited scope of accessibility, remain secure and that access is managed. Leaks, attacks, and mistakes can result in the loss or exposure of sensitive data. This exposure of data will reflect on the owner of the data more severely than the provider of the cloud service. The owner of the data has the duty to preserve—not the service provider.

# 4 Information Retention and Disposition

Storing data in the cloud does not relieve an organization of its information retention and management obligations. Business records must still be kept for specified periods of time and those retention periods must be enforced (both minimum and maximum timeframes). Given that many organizations have a difficult time doing this inside their own enterprises, it can be even more difficult to specify and manage retention periods for data stored in the cloud, where ultimate disposition controls may be in question. In addition, many cloud providers may not be aware of how retention periods are enforced; it is important to question the provider and seek clarification on this issue.

It is vital for IT and RIM to have a consolidated policy and goal in relation to the storage, retrieval, and ultimate disposition of information stored offsite for the organization. Unless the records management group has strong ties with the information technology group, there could be two distinct policies concerning the retention and disposition of information in the organization.

The records management policy would likely focus on the legal, risk, and operational requirements of the information. The information technology policy relating to retention and disposition
would probably focus on the business continuity, infrastructure requirements, and access needs for the information. As a result, communication and collaboration between these two groups are essential to the development of a consolidated policy.

This policy also needs to be agreed upon and reviewed by the legal department prior to investigating any potential vendors.

Unless vendors have a strong focus on providing services to the records management community, their retention and disposition policies may be very simplistic. Traditionally, cloud service providers are focused on the storage and retrieval of information as needed for the particular application—not on records management. Vendors in cloud computing may not be familiar with records management standards or best practices. It is likely that the vendors’ past experience will have been to recover information that was deleted accidentally rather than to prove something was deleted permanently. Vendors will probably be more prepared to hold information indefinitely than to ensure its timely and permanent destruction.

If the vendor relationship must be terminated for any reason, it is also important to understand the terms and conditions for returning data or providing it to a new vendor, including costs to the organization. To ensure the integrity of the information from the records perspective, the audit trail needs to be transferred along with the actual data.

All of the above points should be considered when reviewing vendors’ policy statements concerning records management.

5 Other Technology Issues

5.1 APIs to Records Management Systems

Most of the records management software systems on the market today can be configured to manage items in remote repositories. This is most commonly done with information under the direct control of the information-owning organization—not with a third party. As systems become more sophisticated, their ability to communicate with other systems is often enhanced programmatically through an application programming interface (API) that can allow two disparate systems to communicate with each other and pass information and commands. Such an interface could be beneficial in the management of offsite records information stored in a third-party-controlled environment, if the cloud provider’s software can satisfy the requirements specified by the API.

5.2 Virtual Storage

Many larger organizations have made the change from dedicated servers and repositories to virtualized environments, clustered storage, and internal or “private clouds” for their information management. Virtualization portends opportunities for cost cutting and more efficient use of resources, as well as flexibility for the organization. Cloud-based storage can enhance these benefits.

It is possible to store records with a third-party service provider in the cloud and feel confident that records are secure. However, care must be taken to ensure that the records are appropriately safeguarded and access is controlled. The largest concern is that the management of the records is out of the organization’s direct control. As these records will be actively managed by the vendor and somewhat passively managed by the organization, it is vital that all parties understand their respective responsibilities as they relate to retention, access, security, destruction, and exception management.

To aid in decision making, a variety of technology-related issues are included in the cloud checklist in Appendix A.1. Consult this checklist prior to finalizing plans for records storage in the cloud.
Chapter 6  Legal Considerations

6.1  General

What might be the legal implications for organizations outsourcing records storage to the cloud? Those implications derive from traditional principles of American contract and tort law (and, perhaps under limited circumstances, constitutional law).

How does preservation work when information “leaves” an organization and is maintained or appears on a third-party site? Under long-accepted contract and tort principles, the organization may be responsible if information is not preserved by the third party. The organization’s responsibility may also extend to being required to secure and produce information maintained by a third party. That responsibility may lead to disputes between the organization and its third-party provider as to information that, for example, the latter maintains on a proprietary system or database.

Similarly, the organization may be responsible for the wrongful acts of the third party under principles of actual, apparent, or implied authority. These situations arise when an organization, in one manner or another, cloaks a third party with permission (actual or not) to undertake certain acts. Thus, contract and tort principles are likely to apply to relationships between organizations and third parties when the organization is confronted with a legal dispute or litigation.

6.2  Records Preservation for Litigation

Within most jurisdictions throughout the world—and particularly in the United States—an organization has a duty, by law, to preserve relevant information once it knows, or has a reasonable basis to know of actual or threatened litigation. The event that gives rise to this duty to preserve is known as the “trigger.” Parenthetically, separate obligations to preserve information may be imposed by statutes or regulations.

Organizations should have records retention policies in place that take into account the need to preserve information that is subject to a hold. In particular, the Federal Rules of Civil Procedure (FRCP) apply to the provision of information during litigation. To ensure compliance with the FRCP, the following points should be considered when using cloud-based services for the creation or storage of data that may be requested during the course of litigation:

- The disclosure of the existence and form of electronically stored information (ESI) is forced at an early stage of the case (FRCP Rules 16 and 26), and this disclosure must include a description of ESI that may be used to support claims or defense.

- Plaintiffs and defendants are required to have a detailed discussion about the preservation and production of any ESI that may be deemed relevant or potentially relevant; this is called the meet and confer, or Rule 26, conference.

- Data must be translated by the defendant into a usable form, which typically requires the information to be presented in its native electronic format.

- A framework for dispute resolution and for relief from burdensome requests must be set.

- The FRCP specifically refers to documents and ESI within the organization’s “possession, custody or control,” which includes information created or modified by the organization in the cloud or stored for the organization in the cloud. FRCP requirements include the initial disclosure to the opposing party of the location of such information as well as the production of the information (FRCP Rule 26 and Rule 34).
• The FRCP imposes sanctions related to failures of disclosure but prevents the imposition of sanctions for ESI that is "lost as a result of the routine, good-faith operation of an electronic information system" (Rule 37(e)). Such routine operation, however, is expected to be suspended, when relevant, as part of a legal hold. This could be difficult in a cloud environment where such suspension could affect other clients.

These implications should be discussed with the organization’s legal counsel. Given the increasing involvement of ESI in litigation, organizations should anticipate that they will be required to meet these special ESI discovery requests, as well as more typical preservation orders. For more information on the legal obligations related to litigation holds, consult the ARMA International publication 7 Steps for Legal Holds of ESI and Other Documents.

6.3 Ephemeral Data

Related to the concept of preservation is that of so-called ephemeral data: electronic information that is fleeting in nature and not generally considered to be “stored” in an electronic information system, but may reside temporarily in random access memory.

Some judicial decisions have recognized the concept of ephemeral data and have held that it need not be preserved. Other decisions have rejected the concept and have held that relevant information, fleeting or not, must be preserved—at least if the party possessing the information knows of its relevance and has been requested to preserve it by an adversary.

Given the different interpretations regarding such discovery, organizations using cloud technology should understand which ephemeral data might potentially warrant preservation in the event of litigation and how the service provider would enable such retention.

6.4 The Transnational Problem

Organizations located outside the United States or located within the United States but exporting data to the cloud may face another challenge. Data may flow to or within the cloud across national borders, thus giving rise to so-called “transnational” issues. There are no decisions by American courts that squarely address these issues in the context of the cloud or the Internet, (other than generally requiring parties before American courts to produce information regardless of foreign laws). This lack of precedent in the United States contributes to uncertainty for decision makers when they consider what law(s) must be followed.

Organizations exporting data to the cloud may find that the data becomes subject to privacy or confidentiality rules of foreign countries, such as those of the European Union. Or data may be subject to “blocking” statutes, such as those of France, under which the export of certain commercial types of information is prohibited. More generally, organizations might become subject to the jurisdiction of other countries and be exposed to civil or criminal penalties for the “wrongful” release of protected data to the United States. This challenge calls for caution by organizations, whether data is “native” to a foreign country because the organization is located there or because the organization has data located or stored in foreign countries.3

There are ways to minimize risk for organizations transferring information across borders. For example, the U.S. Federal Trade Commission maintains what is referred to as “Safe Harbor Certification.” Organizations registering for Safe Harbor protection certify on an annual basis that they comply with privacy principles consistent with those of the European Union.

Organizations transferring information can also incorporate model contract clauses in agreements or adopt binding corporate rules. Above all, it is important to remember that American courts can compel parties before those courts to respond to discovery requests and produce information maintained in a foreign country, even if doing so might expose the organization to penal consequences in that country4.

6.5 Recommendations to Mitigate Legal Risk

Information created by an organization is one of its most important assets, and protection from unauthorized access or dissemination must be considered when operating in a cloud environment. Organizations may be reluctant to store data and use applications on systems they do not ultimately control. When information is compromised, it may lead to regulatory or legal problems and/or a loss of reputation for the organization.

Specific recommendations to mitigate these legal risks are:

- Establish clear rules for employee use of corporate information systems that include use of systems outsourced to the cloud, including access to the employees’ personal accounts. Once such rules are established, the organization should monitor employee use and take appropriate disciplinary action when the rules are violated. Social networking sites provide examples of the cloud being used for both personal and business purposes; using these types of sites for business purposes may allow information to be compromised unless specific policies and protections are in place.

- Establish ownership of data and include language in any cloud provider’s service contracts that addresses the organization’s ownership. This should avoid the risk that a third party will claim ownership of an organization’s data. Be aware, however, that once the organization establishes ownership, it is likely to be compelled to produce the data directly, rather than be able to successfully argue that the data should be subpoenaed from the third party.

- Prohibit subcontracting by the cloud provider, or at least limit the number and location of subcontractors. This serves two purposes. First, this prohibition should contribute to data security by reassuring the organization that the party it contracted with is the only service provider. Second, the prohibition can minimize or eliminate data transfers, in particular, cross-border data transfers.

- Limit the locations(s) where data are stored. Again, this contributes to data security and restricts data transfers and cross-border transfers.

- Establish a mechanism with the cloud provider for communicating and implementing legal holds. Make it clear in the service contract what the cloud provider’s obligation is for implementing and, possibly, managing legal holds.

- Establish how data will be stored and segregated from or commingled with other organizations’ data. Storage of confidential data or vital records should be handled with their unique requirements in mind, e.g., storing such data in a separate location from anyone else’s data or even other types of data from within the organization. For general guidance regarding vital records

---


- Establish access rights to data hosted by cloud providers. This is intended to eliminate or at least reduce additional costs the cloud provider might impose for “unusual” access, such as when an organization must produce data in response to a request for information, subpoena, or discovery request.

- Establish the allocation of liability for loss or wrongful disclosure of data, preferably as part of the contract. Although regulatory agencies or courts will likely hold the organization owning the data responsible for the event, the owning organization will want the ability to hold the cloud provider liable for what it did (or failed to do). Conversely, the service provider will usually seek to contractually reduce or eliminate any liability.

- Establish appropriate security and confidentiality measures to be taken by the cloud provider, including a communication plan for notification to the organization in the event of a breach by any unauthorized party of the provider’s technology, even if it is believed that the organization’s data was not affected.

- Establish appropriate procedures and protocols for data disposition, which may include multilevel approvals and audit trail.

*The Legal Issues Checklist* in Appendix A.2 provides a convenient guide to the major legal considerations involved in records storage in the cloud. The checklist is not all-inclusive and is not intended to offer legal advice. Readers are urged to seek appropriate legal counsel as needed.

7 Vendor-Related Considerations

This section details the issues that should be investigated as part of the selection process and addressed in the contract with the cloud vendor. The *Vendor Concerns Questionnaire* in Appendix A.3 includes a summary of the considerations described in this section, as well as some additional issues of interest. The questionnaire may be useful when vetting a set of chosen vendors.

7.1 Information Management Practices

When outsourcing information to the cloud, it is important to investigate the vendor’s practices regarding information management. It is possible for the vendor to replicate information to redundant systems both within its facility and elsewhere. As a result, it is important to understand where information will be stored, as well as where information could be stored.

It is also important to understand the vendor’s policies concerning data backup and archiving. Quite often, information exists for years in a backup scenario long after the “live” data have been deleted.

Prior to signing an agreement with a vendor, it is important to inquire about client audit policies. An organization’s external auditor may want to audit the vendor’s facility and its practices relating to the security and management of records and information.

Records managers must be aware that the weakest point of security for cloud applications is the point of integration. In the past, when computing services were available only within the organization, the point of integration was always behind the firewall; hence, it remained within the purview of the organization. Cloud computing takes the point of integration and places it outside the firewalls of the purchasing organization and the cloud vendor, making security the responsibility of all parties.
An advantage of the cloud is the ability to access information anywhere and anytime, as long as there is an Internet connection. This allows increased mobility and flexibility for employees. However, without specific safeguards in place, this also exposes information to unauthorized access. When information is managed outside an organization’s normal operating environment, security controls need to be in place to ensure that access is not compromised. Management of users (creation and deletion) must be in place and should also include user authorization and authentication. If internal IT systems already do this, synchronization with the cloud provider is desirable.

7.2 Access Interruptions
Dependence upon a cloud vendor also implies dependence upon Internet access. Although the vendor may have redundancy to permit 99% uptime availability, organizations should still prepare for the inevitable failure of access. Electrical outages, Internet service provider down time, damage to cables, and weather interference with satellite access at either the vendor’s or the organization’s location are only a few of the situations that could affect access. Part of any disaster recovery or business continuity plan should include how the organization will operate in the event the cloud provider’s services are not accessible. This is especially important because of the mobile nature of today’s workforce.

7.3 Privacy
Privacy has become a key issue in the management of information. It is important to understand the type of information to be stored and where this information will reside, as there are legal implications involving storage of personally identifiable information (PHI) or confidential information. If the organization does not have a specific policy concerning the privacy of its information, one should be developed and undergo a thorough legal review prior to entering into an agreement with any vendor who will have custody of an organization’s information.

Vendors in the business of managing other companies’ information should have their own policies and protocols surrounding the privacy and protection of stored information. Organizations must obtain, read, and understand the vendor’s privacy policy and thoroughly vet it with legal counsel. Where the organization’s and vendor’s policies conflict, additional contract negotiation will be required.

The vendor’s privacy safeguards go beyond the technologies employed in the storage and protection of information. Various personnel at the vendor’s site could have administrative or other types of access to the organization’s data and applications. The vendor should be asked to identify how many and what type of personnel will have such access. Additionally, the vendor should be asked about its hiring and employee screening practices.

7.4 Subcontracting
Careful attention must be paid to the vendor’s structure and subcontracting relationships. In order for cloud providers to offer uninterrupted access, scalability, and elasticity, they may need to have infrastructure and hardware in diverse global locations or depend on third parties for services such as storage mirroring or backup.

The purchasing organization needs to thoroughly review and understand the vendor’s business relationships. Are the vendor’s subcontractors bound to the same security and privacy policies that the vendor has? How is the information protected as it is transmitted between the vendor and its subcontractors? What safeguards are in place as information is managed and replicated within the vendor’s subcontracting organization and structure? Can the agreement be structured so that data will reside with only one or two vendors that have been thoroughly vetted by the organization?
Answers to these and other questions will provide the purchasing organization with an understanding of the vendor’s management of subcontractors and attention to related security issues.

7.5 Multi-Tenancy

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

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

When investigating this issue with cloud vendors, it is important to understand the organization’s own view on this matter. Is multi-tenancy covered in the organization’s own privacy and security policies? If not, formal understanding and guidance on the issue will need to be addressed and should involve input from its information technology, records management, and legal departments. The organization’s policy then needs to be compared to the vendor’s policy and any differences negotiated contractually.

7.6 Public vs. Private Clouds

To accommodate a variety of organization needs, a cloud vendor may offer different, customized solutions (e.g., SaaS) and may include public, private, or hybrid cloud options. A public cloud allows open access in that anyone can contract for the services (with specific data access controlled by authentication or similar security) and the customer has little if any control over how the services are implemented. Private clouds allow the customer to control how the service is supplied even to the extent of dictating the software and/or hardware to be used and they generally allow data to be easily moved between the internal data center and the private cloud. Access security is frequently controlled on the private cloud through the organization’s internal system and in some cases the private cloud is inside the organization’s own firewall. Hybrid clouds allow for the combination of public and private cloud computing services in a coordinated fashion.

There are differences between public and private cloud environments and the security levels offered. A user of a public cloud can access services wherever there is an Internet connection. The risk of security breaches with public clouds can be reduced if user authentication (passwords or token) and encryption over a secure connection are used. In addition, the organization should determine whether the information is being stored on virtual machines and what the disclosure policy says before using a public cloud.

A private cloud may be external or internal to a company. Internal private clouds have additional layers of security control by virtue of physical access and internal organizational controls. It provides a secure environment for access via the Internet or a private network. A private cloud should be protected by a firewall. The right to use and access is provided through the authentication and authorization of users. Private clouds allow information to be separated (virtually) and are more secure. However, there is a higher cost for that security.

A public cloud may not be appropriate when information is covered under specific regulatory requirements (e.g., the Health Information Portability and Accountability Act (HIPAA)) or when an internal risk analysis determines that the information’s exposure would jeopardize the company. Information of this nature may be better managed in a private environment where the risk of access
can be reduced or mitigated. When engaging a company to manage information in an external cloud, the risk assessment must include a full review of practices for accessing the cloud, hiring practices of the cloud-hosting organization, oversight of the physical architecture administration, and data access to the cloud itself.

A hybrid cloud can be appropriate when there is a solution requiring ongoing exchange and coordination between public users and private applications. An example would be an externally facing customer relationship management (CRM) program that links to proprietary organizational data sources. Similar to public and private cloud options, security and governance must be properly addressed. With a hybrid cloud, integration at all layers (data, process, management, security) is essential.

Some general issues to consider when choosing between public, private, and hybrid cloud computing options are:

- How sophisticated is the solution and does it require complex integration between public and private environments? A hybrid cloud option offers the opportunity to create collaborative solutions.
- What are the security requirements for the type of information being managed? If a more hands-on type of management is needed, then a private or hybrid cloud option may be more appropriate.
- If the information stored and managed is deemed to be low-risk, then a public cloud option may be suitable as long as authentication and encryption are available.
- If storage in a virtualized environment is prohibited, then a private cloud may be the answer—unless the vendor can guarantee that the public cloud will not utilize virtual machines.

7.7 Data Location

Information in the cloud can be hosted anywhere in the world, so it is necessary to identify the location of the provider’s repositories and identify the countries where the provider may store data. It is also important to identify any third-party providers the vendors may use and note the physical locations of their operations. Compliance with all applicable laws should be assured. During contract negotiations, ensure the vendor is obligated by contract to store information where required, and validate that privacy issues are addressed.

7.8 Data Backup and Recovery

External service providers should offer demonstrative proof of backup plans. During the development of a service agreement, language should include processes such as backup and recovery within a specified time and prioritization of application and data stores, including the identification of critical applications to be restored first.

The cloud is frequently used specifically to back up data. While this service has been around for several years, it is now gaining in popularity for both personal and business use. For workers who travel, this type of service offers a convenient way to provide information backup on a regular basis.

When considering this type of solution, it is important to review the vendor’s policy and practices for backing up the data prior to contract finalization. Is the information being backed up to another system for redundancy? What type of controls does the vendor have in place regarding access to the information? Periodic tests should be performed to ensure that the backup recovery systems and processes are working as specified in the contract or service level agreement. The physical location of the alternate system should also be checked.
7.9 Data Retention

Whether information is stored in the cloud or on a network, it is subject to a retention schedule. If information is stored on virtual machines and can be spread among multiple locations and countries, each country’s regulations can impact the retention time for that data. When data are stored on multiple servers in multiple countries, retention issues become more complicated, and the contract language should address these concerns. Additionally, the contract language needs to have provisions for the destruction of records on all media (including backups) when the retention period ends and for retaining information past the retention period in the event of a legal hold.

7.10 Physical Security

Data center security is critical to ensure that proper controls are in place to protect the building, the data, and the employees. The cloud provider’s data center must be evaluated for its geographical location and physical security features, including management of secured, authorized access. Consider a facility that provides a 100% power agreement, offers 24/7 security surveillance, has a secure or hardened facility, and uses strong security features for physical access.

Building security includes monitoring by camera, monitoring by the presence of a security guard, and the existence of a physical enclosure such as fencing. There should be sign-in and sign-out procedures, especially for any visitors. Background checks should be performed on employees. Contract terms should reflect all of these physical security requirements and allow the customer to conduct periodic facility audits.

7.11 Environmental Conditions

Review the site to ensure that no environmental issues exist, e.g., proximity to existing or potential environmental or industrial hazards. The internal environment should be reviewed, as well. Ensure proper temperature and humidity controls are in place, and include appropriate language regarding environmental conditions within the contract.

7.12 Network Access

Information in the cloud is being transmitted over networks. Review the compatibility of the vendor’s architecture with the organization’s, as they must work together. As more data are placed on and retrieved from the cloud, network saturation is another consideration and bandwidth capacities should be investigated. Determine the accessibility to high-speed trunk lines and who maintains them. Contract terms should address these network requirements.

7.13 Uptime

No matter where information is stored, system uptime must be a consideration. Uninterrupted access to information is a key to effective business operations. One of the benefits of the cloud is that services can be extended to different locations to accommodate scaling of a business and to protect users from outages. The contract should identify whether such an arrangement exists or is required.

Of particular concern is the use of a cloud for critical organization applications. Any critical applications that are in the cloud need to have rigorous service agreements that equal or exceed what in-house information technology would provide for uptime accessibility.

The process for restoring data or an entire application should be tested to determine if adequate recovery can be demonstrated to ensure business continuity.

Uptime requirements should be clearly defined and negotiated with the vendor.
7.14 Vendor Continuity

Review and validation of the vendor’s credit worthiness should be performed by the organization to assess the vendor’s long-term viability. The organization’s contract should document the application, data, and platform migration strategies that will be used in the event that a vendor goes out of business or is acquired. During the negotiating process, the organization should devise contractual terms to provide flexibility in accessing data and define how the organization’s information will continue to be accessible during any migration.

When a service provider is being selected, the geopolitical climate needs to be assessed, as information could be compromised due to the destabilization of a location. Before finalizing the vendor agreement, conduct a thorough risk assessment and review of the hosting country’s current social, political, and economic conditions. Determine what strategies the vendor has in place, for example a mirror or backup in another country, to accommodate these concerns.

8 Standards and Best Practices

There are several standards and best practices publications providing requirements specific to electronic records management. There are currently no standards specifically for RIM in a SaaS or social networking application utilizing the cloud. Until a defined set of standards is produced, RIM professionals must create their own requirements applicable to their physical and electronic environments and the proposed cloud solution.

Readers should consult the latest edition of these two standards that provide guidance for electronic records and could be adapted to the cloud environment:

- DoD 5015.2 – In the United States, the Defense Department’s Electronic Records Management Software Applications Design Criteria Standard (DoD 5015.2) has become the de facto standard for electronic records management technology. It defines the requirements for applications as well as the management of record objects.

- MoReq2 – The Model Requirements for the Management of Electronic Records (MoReq2) is a European Union standard that includes the storage and management of data by third parties; however the third-party specifications are not a required component for certification. Outsourcing and Third Party Management of Data is currently part of the Non-Functional Requirements section of MoReq2 and is described as both “important to success” and “difficult to define.” Readers should bear in mind that these are requirements for software vendors to strive for as part of the MoReq2 certification. These are not requirements designed specifically for third-party custodians of records, such as cloud providers.

9 Summary

There are many considerations to include in the decision-making process when weighing the benefits and risks of outsourcing records storage to the cloud. While operational and cost concerns are paramount, appropriate protection for records and information must be in place as well. RIM, IT, and legal professionals will find this guideline to be useful as an advisory document. In particular, the checklists in the Appendix provide direction from a variety of perspectives: technology, legal, and vendor-related.

---

5 At the time of writing, ARMA International is engaged in a project to develop an American National Standard: BSR/ARMA 18-20x1, tentatively titled Implications of Web-Based Technologies in Records Management. Check the ARMA International website (www.arma.org) for the current status of this publication.

6 At the time of writing, a MoReq 2010 revision was underway to address suggestions, clarifications, and bug fixes for the specification. This new edition is also expected to be more modular and scalable, and allow for future customization by industry.
Appendix A

Checklists and Questionnaire

The checklists and questionnaire in this appendix offer assistance to readers who wish to evaluate their decision-making preparedness when considering the outsourcing of records storage to the cloud. Separate forms are provided for cloud technology matters, legal issues, and vendor considerations. RIM personnel completing these forms may want to consult personnel from information technology, legal, or other relevant functional areas to determine readiness for outsourcing.

An editable Word version of the checklists and questionnaire is available as a free download for purchasers of this guideline at: www arma.org/bookstore/materials/cloudstorage.

A.1 Cloud Technology Checklist

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Cloud Type:</td>
<td>□ Public</td>
<td>□ Private</td>
</tr>
<tr>
<td>2.</td>
<td>Data Type:</td>
<td>□ Public</td>
<td>□ Private</td>
</tr>
<tr>
<td>3.</td>
<td>Information Types:</td>
<td>□ Personally Identifiable Information</td>
<td>□ Confidential Information</td>
</tr>
<tr>
<td>4.</td>
<td>Type of Access:</td>
<td>□ Unsecure</td>
<td>□ Public</td>
</tr>
<tr>
<td></td>
<td></td>
<td>□ Secure</td>
<td>□ Private</td>
</tr>
<tr>
<td>5.</td>
<td>Are user permissions validated?</td>
<td>□ Yes</td>
<td>□ No</td>
</tr>
<tr>
<td>6.</td>
<td>Is user logging implemented?</td>
<td>□ Yes</td>
<td>□ No</td>
</tr>
<tr>
<td>7.</td>
<td>Are account changes such as user additions and user deletions handled promptly?</td>
<td>□ Yes</td>
<td>□ No</td>
</tr>
<tr>
<td>8.</td>
<td>Are user permissions reviewed on a regular basis?</td>
<td>□ Yes</td>
<td>□ No</td>
</tr>
<tr>
<td>9.</td>
<td>Is someone responsible for reviewing user permissions?</td>
<td>□ Yes</td>
<td>□ No</td>
</tr>
<tr>
<td>10.</td>
<td>Do user permissions and security need to be synchronized with the contracting organization?</td>
<td>□ Yes</td>
<td>□ No</td>
</tr>
</tbody>
</table>
## A.2 Legal Issues Checklist

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Are rules established for employee use of organizational information systems that are extended to cloud applications? □ Yes □ No</td>
</tr>
<tr>
<td>2.</td>
<td>Is employee use of information systems, including cloud applications, monitored? □ Yes □ No</td>
</tr>
<tr>
<td>3.</td>
<td>Is disciplinary action enforced when employee rules regarding information systems use are violated? □ Yes □ No</td>
</tr>
<tr>
<td>4.</td>
<td>Has ownership of data been established? □ Yes □ No</td>
</tr>
<tr>
<td>5.</td>
<td>Are there specific policies in place regarding the use of information system subcontractors? □ Yes □ No</td>
</tr>
<tr>
<td>6.</td>
<td>Have any limits been placed on the locations where data are stored or located? □ Yes □ No Where?</td>
</tr>
<tr>
<td>7.</td>
<td>Are there policies and procedures in place for addressing legal hold and e-discovery with information systems, including cloud technology? □ Yes □ No</td>
</tr>
<tr>
<td>8.</td>
<td>Has it been established how data will be stored when it is outsourced? □ Yes □ No</td>
</tr>
<tr>
<td>9.</td>
<td>Have access policies for data hosted by parties outside the organization been established? □ Yes □ No</td>
</tr>
<tr>
<td>10.</td>
<td>Has allocation of liability for loss or wrongful disclosure of data by the vendor and any subcontractors been established? □ Yes □ No</td>
</tr>
<tr>
<td>11.</td>
<td>Is a plan in place by the vendor and any subcontractors to notify the data owner in the event of a security breach? □ Yes □ No</td>
</tr>
<tr>
<td>12.</td>
<td>Overall, are appropriate security and confidentiality measures in place (from a legal perspective)? □ Yes □ No</td>
</tr>
</tbody>
</table>
### A.3 Vendor Concerns Questionnaire

1. Are vendor terms and conditions consistent with the organization’s goals and objectives?  □ Yes  □ No

2. Under what conditions, if any, will the vendor allow independent audits of systems and processes?

3. Where are the vendor’s physical servers located?

4. Can the vendor provide international diversification, with hubs in various geographic locations?  □ Yes  □ No

5. How long has the vendor been in business?

6. How long has the vendor been providing cloud-based services?

7. Who are some current clients of that vendor?

8. Can the vendor provide public, private, or hybrid cloud environments? (Check all that apply.) □ Public □ Private □ Hybrid

9. Can the vendor separate data depending on the data type?  □ Yes  □ No

10. Does the vendor have a firewall that will adequately address security-related needs?  □ Yes  □ No

11. Are data encrypted when using a public cloud environment?  □ Yes  □ No

12. What does the disclosure policy say about data on the vendor’s systems?

13. Does the vendor offer redundant systems?  □ Yes  □ No

14. Does the vendor offer guaranteed uptime?  □ Yes  □ No

15. Does the vendor have redundant Internet connections?  □ Yes  □ No

16. Does the data center have adequate environmental control features?  □ Yes  □ No

17. Is the data center conveniently located (geographically)?  □ Yes  □ No

18. Is the perimeter of the data center protected?  □ Yes  □ No

19. Does the data center have a visible security presence such as a guard or monitoring cameras?  □ Yes  □ No

20. Is the data center location secured with systems to provide authorized access?  □ Yes  □ No

21. Is the data center located in a country where geopolitical instability may be problematic?  □ Yes  □ No

22. Identify the geographic locations the virtual environment spans.

23. Is the data center located near known or potential hazards?  □ Yes  □ No

24. Are applications and information distributed across systems?  □ Yes  □ No

25. Will data be stored so that it is segregated from (rather than commingled with) other organizations’ data? If yes, specify how, i.e., what hardware and software are used?  □ Yes  □ No

26. Has the vendor’s backup strategy been reviewed?  □ Yes  □ No

27. Is a backup done using disk to disk or tapes or other methods? (Check all that apply.) □ Disk-to-disk □ Tape □ Other – Describe:
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>28.</td>
<td>Where are backup media located?</td>
</tr>
<tr>
<td>29.</td>
<td>What types of drives are used for backups and are replacements available?</td>
</tr>
<tr>
<td></td>
<td>Replacements:</td>
</tr>
<tr>
<td>30.</td>
<td>How often are backup media rotated?</td>
</tr>
<tr>
<td>31.</td>
<td>What types of redundant network links are available?</td>
</tr>
<tr>
<td>32.</td>
<td>Can the vendor demonstrate a business continuity plan?</td>
</tr>
<tr>
<td>33.</td>
<td>Are business-critical applications being hosted?</td>
</tr>
<tr>
<td>34.</td>
<td>Is the data center designed around a virtualized environment?</td>
</tr>
<tr>
<td>35.</td>
<td>Are the data on virtualized servers?</td>
</tr>
<tr>
<td>36.</td>
<td>How is retention managed in a virtualized environment?</td>
</tr>
<tr>
<td>37.</td>
<td>Is access to system configuration and/or administrative functions tightly controlled?</td>
</tr>
<tr>
<td></td>
<td>Who can make changes to settings?</td>
</tr>
<tr>
<td>38.</td>
<td>Are encryption and control lists in place to reduce the risk of inappropriate access?</td>
</tr>
</tbody>
</table>
Bibliography


© 2010 ARMA International. Purchaser of this PDF file is entitled to print one copy for reference. Other reproductions or redistribution is prohibited.
About ARMA International

ARMA International is the leading professional organization for persons in the expanding field of records and information management.

As of September 2010, ARMA has about 10,000 members in the United States, Canada, and more than 20 countries around the world. Within the United States, Canada, Japan, Jamaica, Trinidad, and the European region, ARMA has about 120 local chapters that provide networking and leadership opportunities through monthly meetings and special seminars.

The mission of ARMA International is to educate, advocate, and provide resources that enable professionals to manage information as a critical element of organizational operations and governance.

The ARMA International headquarters office is located in Overland Park, Kansas, in the Kansas City metropolitan area. Office hours are 8:30 a.m. to 5:00 p.m. (CT), Monday through Friday.

ARMA International
11880 College Blvd., Suite 450
Overland Park, KS 66210
913.341.3808
Fax: 913.341.3742
headquarters@armaintl.org
www.arma.org