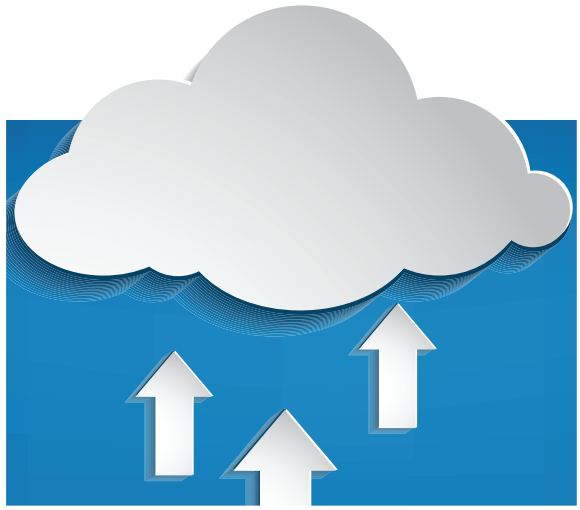
Vendor Considerations

When Outsourcing Records Storage to the Cloud



This excerpt from *Guideline for Outsourcing Records Storage to the Cloud* details the issues that should be investigated as part of the selection process and addressed in the contract with the cloud vendor.

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.

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 work force.

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 (PII) 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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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. E

About the Standards and Best Practices Workgroup
The workgroup project leader was Galina Datskovsky, Ph.D., CRM. Team members were: Debra Logan; Carol E. B. Choksy, Ph.D., CRM, PMP; Ronald J. Hedges, J.D.; Brent Gatewood, CRM; and Glen R. Sanderson, CRM.