

Cloud-based solutions, such as web-based e-mail, have many advantages. But organizations must be aware of the compliance issues related to storing their information outside of their own control.

# CLOUDS ON THE INFORMATION HORIZON: HOW TO AVOID THE STORM

**Brent Gatewood, CRM**



**W**hile much has been written about cloud computing, there has been little focus on the implications for applying records management rules to information stored in the clouds. Without that understanding, organizations cannot make informed decisions about using these resources. This understanding begins with a couple of definitions.

Generally, *clouds* are large collections of easily usable and accessible virtualized resources (i.e., hardware, development platforms, and/or services). These resources can be easily reconfigured to match varying service demands (loads) allowing the service provider to adjust for optimal resource utilization. A few examples include resources offered by Amazon, Google, and IBM.

There is an interdependence between cloud computing and software-as-a-service (SaaS). *SaaS*, which is commonly defined as a software delivery method that provides access to applications and functionality through remote access to a web-based service/infrastructure, typically operates in the cloud. With SaaS, applications are not owned by the user; access and use are licensed for a defined period of time from an application service provider. This can save the licensing organization money for software, hardware, support, and maintenance.

This article relates to records and information being stored in a SaaS/cloud environment – whether created in an organization's captive environment or outside of its in-house computing systems. Information in the cloud resides in server farms and data warehousing facilities that may be spread throughout the country or even globally. Even though an organization may be doing business with a vendor down the street, its data may be stored many states away – or even in a different country.

As vendors identify needs and applications in the market and rush to develop and present cloud-based solutions, their ideas may not be fully developed or include records management rules-based control.

Not knowing where their information is stored and not having records management control over it are two major compliance concerns for organizations storing their records in the cloud environment.

### Typical Cloud Matter

The number and variety of cloud-based applications is growing rapidly, and many organizations either already use a SaaS solution or are considering one. Following are some of the most common types of solutions.

#### Communications

Communications are a natural fit for cloud computing solutions because they almost uniformly rely on the same basic infrastructure – the Internet. E-mail and instant messaging rely on the Internet for their delivery – and as such, it makes sense that e-mail was one of the first solutions to be offered in the cloud.

Having communications hosted by a SaaS provider has many benefits to an organization, especially because e-mail is one of the largest consumers of technology resources in most organizations. Outsourcing some or all e-mail infrastructure can free IT/IS resources for tasks more central to the organization's business. However, due to e-mail's pervasiveness, many of an organization's records and a substantial amount of risk reside in e-mail; managing these records and associated risks in the cloud can be problematic.

#### Document Management

Many organizations are also experimenting with some form of document management in the cloud. These applications range from *ad*

*hoc* repositories for external access to very specific point solutions for defined departments and document sets. Typically the level of control surrounding the application and content rises as the solution becomes more narrow and specific to a task or function. More generalized implementations typically have fewer controls compared to highly specialized point solutions.

#### Structured Data Services

Some structured data services have also been very prominent in the SaaS environment. Customer relationship management solutions have been successfully moved to the cloud. There has also been some success in moving enterprise resource planning toward cloud-based applications. These examples rely on a structured data set and capture methodologies, as well as an enterprise need for the information they contain. This broad need and tightly managed capture methodology and controlled data set work well in the structured environment. The caution arises because, in some cases, the complexity of the information captured may require more stringent management controls.

#### Business Continuity

Another good application for cloud computing is disaster recovery and business continuity. Utilizing the cloud infrastructure for storing or managing business-critical information makes sense if the proper controls are in place. Running parallel systems offering failover capabilities (the ability to automatically switch to a redundant system in case of system failure) makes sense for many business-critical systems. Of course, running duplicate systems can be costly, so the value of the potential reduction in risk for a critical system must be measured carefully to ensure the investment is worthwhile.

## Storm Clouds on the Horizon

Cloud computing has a definite place in today's organizations and is likely to become even more prevalent. However, records management compliance ramifications of SaaS solutions must be fully considered before they are implemented. Although the cloud has its advantages, it also has disadvantages. An organization's RIM, IT, and legal staff must understand those disadvantages in order to identify possible problems and minimize risks of any SaaS solution that is being considered or has already been implemented. Primarily, they must understand the legal and regulatory environment and risks associated with cloud use.

To say the legal environment is changing would be an understatement. The current economic situation and its causes ensure that regulatory oversight around the world will grow in the coming years. But current requirements associated with how an organization handles its information are already very demanding. Following is an examination of some of the more prominent issues surrounding records management and how they are affected by cloud computing.

### *FRCP Related to Discovery*

The most recent update to the *U.S. Federal Rules of Civil Procedure*, which occurred in December 2006, places a large burden on an organization preparing for discovery.

Rule 26(a)(1)(A)(ii) states that, in a lawsuit, an organization must provide to its opponent a copy – or a description by category and location – of all documents, electronically stored information, and tangible things the disclosing party has in its possession, custody, or control and may use to support its claims or defenses, unless the use would be solely for impeachment.

Rule 26(a)(1)(C) states the time for initial disclosures – in general. A party must make the initial disclosures at or within 14 days after the parties' Rule

26(f) conference unless a different time is set by stipulation or court order, or unless a party objects during the conference that initial disclosures are not appropriate in this action and states the objection in the proposed discovery plan. In ruling on the objection, the court must determine what disclosures, if any, are to be made and must set the time for disclosure.

Consider what these statements mean to organizations preparing for a pretrial meeting. Putting together a listing and map of all relevant and responsive data within an organization within the 14-day time frame will be difficult enough. Add to that the difficulty of identifying and documenting

**Organizations must identify the location of relevant information and verify the information has not been and cannot be altered. How is this done in the cloud?**



vendor relationships and data stored with multiple vendors in the cloud. It is unacceptable to say, "The information is out there, someplace." Organizations must identify the location of relevant information and verify the information has not been and cannot be altered. How is this done in the cloud?

### *Regulatory Requirements*

Regulatory agencies also require information be accessible for review and audit purposes. If the information has been used to report compliance activities, it is critical to show the requesting agency the information remains unaltered from its previous state.

It may also be necessary to run routines and produce reports in a manner similar (or exactly) as they were run for the original reporting purposes. With in-house systems, it is fairly easy to show regulatory agencies and audit personnel the current state of a system and the upgrades, if any, that have been performed over a specific period of time. Again, how is this done in the cloud?

### *Privacy Concerns*

Privacy is one of the longest standing and most important concerns with cloud computing. Consider the lengths organizations must go to ensure information repositories are secure in their own controlled environments. Now, consider the difficulty of that task in a typical cloud environment, remembering that a large-scale solution with multiple clients and shared architecture is what makes cloud computing powerful and economical. In fact, a SaaS provider may be relying on other external providers for its backbone, infrastructure, and storage.

An organization's information may be resident in several locations and may coexist with other clients' data. Depending on the type of data or the location of the data, this may result in a host of legal issues and legal violations. At the very least, an organiza-

tion's clients – internal and external – may have a strong, negative reaction to learning their information is not being held internally by the organization. Everyone, from management to individuals, wants to know their private information is secure. How is this done in the cloud?

One of the reasons that SaaS and cloud computing are appealing is the solution can be globally deployed much easier than if the organization had to push hardware and software out to each and every location around the world. The allure of an easy and cost-efficient global deployment may mean a shorter review and development cycle – and less initial attention to privacy and compliance issues. This shorter cycle is often where trans-border issues are missed. However, if an organization does business internationally, it has no choice but to consider the international data management and compliance obligations and restrictions that are implicated by a cloud computing model.

Personally identifiable information (PII) is subject to many restrictions worldwide. Transferring this information to a SaaS provider may violate some countries' laws. PII is not the only issue. Country restrictions vary, but information potentially subject to privacy, location, and other restrictions can include financial data, intellectual property, health information, and much more. It is imperative to understand where this data resides and how to restrict its movement and access to it as necessary. With cloud computing, this may not be possible.

The combination of a widely deployed infrastructure in multiple locations makes managing these issues problematic. If a SaaS provider is utilizing a second or even third tier of vendors to help manage its systems, as is often the case, the problem is aggravated – not only does an organization not know what is being done with its data, it may not even know who the other providers are. Cloud computing

## CHECKLIST FOR EVALUATING CLOUD-BASED INITIATIVES

Organizations considering a cloud-based initiative – or reviewing a solution already in place – must explore the answers to the questions about the following issues:

### CONTRACTS

- What service are we contracting for and what are the vendor's records management and compliance obligations?
- What kind of controls does the vendor have in place?
- How is information destroyed?
- Can we set minimum and maximum retentions and at what level?
- Are there secure destruction options?
- What are the vendor's policies for backups, replication, or failover?
- How do we confirm disposition takes place on a timely basis and according to our rules?

### AUDIT CONTROLS

- What is the provider's internal audit process?
- How often is the provider audited by external agencies?
- What standards is the provider held to?
- Is the vendor open to being audited for compliance? (If not, this may be a sign of bigger issues.)

### INTEGRATION POINTS

- Is the vendor open to integration with our systems and applications?
- Has the vendor integrated with any systems that provide a structure for compliance?

### POLICIES AND PROCEDURES

- Are the vendor's policies and procedures related to handling and managing our information acceptable?

If they are not, either move or don't store the data or have the vendor make an auditable change specific to the needs of your data and organization.

### FOLLOW THE DATA

- Can the vendor provide a data map detailing where the information resides?

A data map is mandatory. As necessary, ask for help in reviewing this information since it will likely be complicated as it details infrastructure and possible third-party relationships specific to your data. You need to understand the implications of this scheme to your organization.

models can ignore these problems and make compliance and verification of compliance difficult, if not impossible.

### Coming Regulations

Looking forward, new regulations and case law that will affect how records are kept and managed are on the horizon in the United States and abroad. The current U.S. administration has mandated transparency and accountability. These tenets will be the cornerstones of new regulations that will soon be in force. Transparency and accountability will drive future records management directives much like the Sarbanes-Oxley Act of 2002 did before them. It is critical that any solution, inside the organization or outside, be prepared for this new mandate as it relates to records and information.

This means, while organizations must maintain easy access to information, having appropriate management controls will be even more important tomorrow than it is today. Where information is maintained, how it is managed, and how the information is used to support an organization will drive the development of new compliance strategies and tools. "How is this done in the cloud?" is a question that organizations must answer specific to its records requirements.

### Compliance in the Cloud?

Records management compliance is difficult enough inside of an organization, even when it is using its own best practices tool set. Is it possible for an organization that is storing information in the cloud to be compliant with the many rules and regulations specific to it and its information? The answer is likely, "No."

Yes, it is possible to define rules to manage aspects of the life cycle and disposition of the information that is resident in the cloud. But these rules are difficult to enforce, unlike a consolidated rule set managing information resident within an organization's internal environment.

Proper records management requires a centralized control point, as well as effective enforcement for an organization's records management tool set to be effective. Today, the controls in place with most SaaS providers are too non-specific. The controls in place are collection-focused and largely managed according to the provider's rules, not those of the organization whose information is being stored.

To truly satisfy the records management needs of most organizations, control and management of data in the cloud would need to reside inside of the organization itself and extend to cloud-based repositories. A centralized tool managing life cycle rules for

the organization would need to have the proper hooks into the data resident in the cloud. True federation of records management controls will need to expand beyond the organization itself and into the data repositories outside of the organization. These tools need to have a complete view of the information owned by the organization to be responsive to internal and external requests. These tools do not exist today.

### Steps Toward Compliance

The reality is this: The tools may not exist, but organizations are moving – or have already moved – data into the cloud. Now what?

Data relationships and management controls inside of organizations are more important than ever. Unless the management controls are already in place, it is unlikely that individuals are going to seek advice about extending controls to cloud-based repositories.

Education and proactive relationships driven by a strong records management function will help identify cloud-based initiatives early and raise awareness throughout the organization. Once it has been identified, an organization can look at an initiative's scope and explore deployment of reasonable controls that it can put in place. The sidebar "Checklist for Evaluating Cloud-Based Initiatives" on page 35 includes questions about issues an organization must answer when considering a cloud-based solution.

Cloud computing is not going away. It can be a valuable tool to an organization. But, it's a tool that needs to be understood and managed. Records management, with the proper relationships in legal and information technology and services, can help to reasonably manage information in the cloud. **ENR**

*Brent Gatewood, CRM, can be contacted at [bagatewood@pelligroup.com](mailto:bagatewood@pelligroup.com). See his bio on page 54.*

