

ARMA International's

hottopic

MAKING THE JUMP TO THE CLOUD?

How to Manage Information Governance Challenges



www.arma.org





Some days I scan 60,000 documents.
Then there are the busy days.



The Canon DR-X10C Color Production Scanner. If you've ever had the need for scanning speed, this is your machine. Now you can convert documents at a rate of up to 256 color images-per-minute with the high standard of quality you would only expect from Canon. Extremely reliable and durable, the DR-X10C allows you to automate the scanning process — adding productivity and value to your business, as you fly through mountains of documents. **1-800-OK-CANON ScanningSuccess.usa.canon.com**

Canon
*image*ANYWARE



Governance

for Protecting Information in the Cloud

Barclay T. Blair

If your organization is not already using cloud computing, it likely will be soon. The market for cloud computing services is worth billions and is growing dramatically. “Worldwide cloud services revenue is forecast to reach \$68.3 billion in 2010, a 16.6 percent increase from 2009 revenue of \$58.6 billion,” according to Gartner Inc. “The industry is poised for strong growth through 2014, when worldwide cloud services revenue is projected to reach \$148.8 billion.”

Cloud computing promises to enable organizations to do more with their information for less, fundamentally changing the way they use and pay for IT resources. However, cloud computing also creates new risks and challenges.

A recent survey in *Network Computing*, “IDC Survey: Risk in the Cloud,” found that although most organizations see cloud computing as “the way of the future,” most are also very concerned about the availability of their information, performance, interoperability, and security. These concerns are well founded: Although cloud computing may change where and how an organization’s information is stored, it does not remove its legal responsibilities to manage it properly.

Organizations adopt cloud computing for a variety of reasons, but a desire to reduce IT cost and complexity typically plays a prominent role. This focus on cost may mean that information governance issues are not fully considered as part of the transition, thus creating unnecessary risk.

Information governance professionals have to help their organizations recognize and address these risks.

Making Sense of Cloud Computing

At the simplest level, *cloud computing* can be defined as the accessing of shared data and IT services (i.e., computing) over a network (i.e., the cloud). On a more detailed level, however, the phrase “cloud computing” is really a catchall for a range of technologies and business models – each with different information governance implications.

Common cloud computing models are described below.

Software in the Cloud

This type of cloud computing is

what most people think about when they think about cloud computing. Delivering software-as-a-service over a network is not a new concept, but it is one that has been re-energized with the recent popularization of cloud computing. In this model, instead of buying and installing software on computers in an organization, software is licensed and delivered as needed over the Internet. Well-known providers in this space include Google Apps, which provides office software-as-a-service, and *Salesforce.com*, which changed the market for customer relationship management software by offering it as a service. In cloud computing jargon, this type of cloud computing is often referred to as application-as-a-service.

Storage in the Cloud

Another cloud computing model is the provision of storage services over a network. There are varying varieties of this type of cloud computing. Some are designed to provide cheap, offsite backup of data. Others focus on archiving, and still others focus on providing a location for specific types of data (i.e., video or structured database information) to be stored and accessed. In cloud computing jargon, accessing storage in the cloud is often referred to as infrastructure-as-a-service, which can also refer to providing other capabilities and hardware, such as networking equipment and servers, through the cloud.

Building and Hosting Custom Applications in the Cloud

Cloud computing can also be used to deliver customized software applications. A variety of tools and business models exist to enable organizations to build, customize, and host cloud-based applications. For example, Amazon has leveraged its expertise in running large-scale data centers and Internet infrastruc-

Potential Benefits of Cloud Computing

- Reduces capital outlay by “paying as you go”
- Reduces “shelf ware” – software licenses that are paid for, but never used
- Provides access to more storage capacity for less money
- Reduces the size, cost, and complexity of your data center
- Reduces the cost of building custom applications by using standard components and platforms
- Allows you to add or remove capacity easily, as needed
- Expands IT capability without the need for new IT staff
- Provides small and medium-sized businesses access to more sophisticated technology that they could normally not afford

Key Contractual Provisions for Information Governance in the Cloud

Contracts with providers should provide for:

- Access to information for e-discovery
- Enforcement of retention periods
- Preservation of metadata
- Availability and appropriate handling of information during provider acquisitions or divestitures
- Exportability and portability of information
- Adherence to standards
- Audit of provider
- Review of provider policies and documentation

ture to provide Amazon EC2, which is used to host cloud applications. Other companies provide the tools and services to help build the applications themselves. In cloud computing jargon, these types of services are often referred to as platform-as-a-service or development-as-a-service.

It is also important to understand that cloud computing services can be delivered on both public and private networks. In other words, cloud computing can be delivered over the public Internet, but the model also

has benefits when applied to a controlled community or in a private cloud, such as business partners or customers.

Addressing Information Governance Issues

The National Archives and Records Administration in its 2010 “Frequently Asked Questions about Managing Federal Records in Cloud Computing Environments” commented, “Various cloud architectures lack formal technical standards gov-

erning how data is stored and manipulated in cloud environments. This threatens the long-term trustworthiness and sustainability of the data.”

Cloud computing has a number of clear benefits (see sidebar on page HT2). But, it also creates new kinds of information governance risks that must be identified and addressed. Some of the most significant risks are discussed below, along with key planning questions that should be asked and addressed when building an information governance strategy for cloud computing.

1. Availability of information. Fears about the lack of access to their own information is probably the most common concern organizations have regarding cloud computing. This fear is naturally triggered when an organization first makes the shift in thinking about IT that is required to adopt cloud computing.

It’s important to realize that, although cloud computing does introduce significant new availability issues, many access challenges are the same regardless of whether a service provider or an organization’s own IT department manages the data (e.g., hardware failure, natural disasters, and data corruption through user errors). The difference is that, when using cloud computing, each of these issues must be explicitly addressed by contract. Key planning questions include:

- What is the provider’s business continuity and disaster recovery plan for its operation and data?
- What level of backup is provided for your data, and is it sufficient to meet your legal and business obligations?
- What have the provider’s experiences been with significant availability events, and how were they handled?

2. E-discovery requirements. Litigation is a fact of life for most organ-

izations, and as such, so is the need to quickly and efficiently locate and produce information that is relevant to the lawsuit. The e-discovery process can be costly, as shown by a December 2009 survey formulated by Lawyers for Civil Justice, Civil Justice Reform Group, and U.S. Chamber Institute for Legal Reform. The results, published in “Litigation Cost Survey of Major Companies,” found that the average cost of discovery per case for *Fortune* 200 companies ranged from approximately \$2 million to nearly \$10 million. Cloud computing is a new factor to consider when planning for

services providing commodity storage, were not designed with the complex requirements of records and information management (RIM) in mind. Similarly, applications operating over the cloud often have reduced functionality compared to desktop or local versions of the same applications, so key RIM functionality may be missing. When planning an information governance strategy for cloud computing, begin talking to IT early in the process to understand what is being planned and the implications for information retention. Key planning questions for you to ask IT include:

When planning an information governance strategy for cloud computing, begin talking to IT early in the process to understand what is being planned and the implications for information retention.

e-discovery. Key planning questions should include:

- Has e-discovery been addressed contractually with your cloud service providers? Complex search protocols can put a massive strain on computing infrastructure and may create performance issues and drive extra charges.
- Can your cloud provider interface with your software for e-discovery collection, producing, processing, and review or with your providers of those services?
- How easy is it to search within individual cloud computing environments or across multiple environments?

3. Retention requirements. Most cloud computing services, such as

- How do we ensure that our retention obligations are met for information that is generated or stored in the cloud?
- Can we enforce retention and disposition periods through our cloud-based application or cloud storage interface?
- Do our cloud computing services and applications adequately manage the metadata we need, as well as the records themselves?

4. Privacy requirements. Cloud computing often separates the geographic location where an organization conducts business from the geographic location where information is stored. It can raise a number of information governance issues, especially issues relating to privacy. The movement of personally identifiable

information (PII) between jurisdictions is regulated by a variety of laws and regulations, including the EU Data Protection Directive. Organizations must ensure that they do not violate these requirements by using cloud services. Key planning questions include:

- How do you ensure that PII or other information that has specific information protection requirements (e.g., health information) is not inadvertently stored or managed in cloud environments that do not provide adequate protections?
- What is the physical location of your cloud provider, and would the movement of data to its

and acquisition activity?

- How will it affect the availability of your data?

6. Portability of information. One of the primary risks identified by many organizations in the cloud computing industry is the lack of standards. Several groups, including the Open Cloud Consortium and the Object Management Group, are working to create these standards, but today this gap can create significant information governance risk.

For example, it may make it more difficult to move records and information from one cloud provider to another or from a cloud provider to an in-house application. It may also

standardized services and will generally not accommodate customized requirements. Those providers with more customized business models will be more accommodating, at least within a range that still enables them to be profitable enterprises.

Participate in the Process Early

For RIM professionals, cloud computing may come into their organizations in a largely transparent way, as applications that manage records and information are configured to access and store information on the cloud. However, it seems just as likely that many of the mistakes made within an organization (e.g., mismanaging shared drives and e-mail) may simply be repeated in the cloud, but with new risks and complexity.

As such, it is critical that information governance professionals get involved as early as possible when their organizations are considering a transition to cloud computing. It is easier and more effective to address information governance requirements early in the process. Involvement should include participating in the review and evaluation process for providers, including the review of contracts and service agreements. It may also be necessary to review and adapt existing information governance policies to cloud computing, and this is a task that should be started early in the transition process.

Barclay T. Blair is a consultant to Fortune 500 companies, software and hardware vendors, and government institutions. He is an author, speaker, and internationally recognized authority on a broad range of policy, compliance, and management issues related to information governance and information technology. He has led several high-profile consulting engagements that helped companies globally transform the way they manage information. Blair can be contacted at btblair@vialumina.com.

It is critical that information governance professionals get involved as early as possible when their organizations are considering a transition to cloud computing.

facility create any legal issues related to PII?

- Can you ensure that any custom applications built in the cloud will adequately protect private and sensitive information?

5. Multiple providers. Given the proliferation of cloud computing services and providers, it seems likely that organizations will end up with a variety of vendors and contracts as part of their cloud computing strategy. For large companies, this will result in complexity that may create some information governance risk. Contract management alone becomes a significant challenge. Also, the cloud computing market, like other markets, will eventually begin to consolidate. Key planning questions include:

- What happens to your data and services as a result of merger

cause unpredictable results related to metadata and retention periods when data is moved from one provider to another. Key planning questions include:

- What capability does your cloud provider offer for exporting data from its services? What types of metadata are preserved? What are the costs and timeframes?
- What standards does your cloud provider adhere to, and are those standards sufficient to address your data portability requirements?

An organization's leverage with any particular cloud computing provider will depend primarily on the provider's business model and the significance of the organization's business to that provider. Mass providers of commodity applications and services survive by providing



Are your records ready for litigation?

Gauge your level of litigation readiness with a free 8-Point Inspection.



If your organization were sued tomorrow, would your records management, IT, and legal teams be ready to respond effectively and efficiently?

Being “litigation ready” is often too vague and subjective to be meaningful. Our free 8-Point Inspection adds objectivity so that you can more clearly assess how prepared your organization truly is. **Download the free self assessment guide today!**

zylab.com/arma8point | 1-866-ZYLAB NA

ZyLAB[®]
eDiscovery & Information Management

IT's Responsibility

for Security, Compliance in the Cloud

Patrick Cunningham, CRM, FAI



In many respects, cloud computing takes the end user back to the early days of computing – the computer is somewhere else, in a highly secured environment, tended by faceless hordes of brilliant white-coated technicians. The end user accesses that computer through a limited interface, having few choices about how data is arranged and organized. Nothing is stored locally. This description could be of mainframe computing in the 1970s or aspects of cloud computing today; but there are

some significant differences between then and now.

Today's end user can access data from a variety of devices and often from virtually anywhere on the planet. The end user of the 1970s was also oftentimes part of a select group of special users; today's computer user is nearly every employee within the organization. Cloud computing is represented by the next generation of computing and a key element of the ultimate expression, "ubiquitous computing."

With cloud computing come many fundamental challenges to the legal and IT landscape. The shift to the cloud means that IT begins to stop managing technology (infrastructure, hardware, and software) and starts to focus on the information. IT no longer needs to spend considerable resources managing a consistent user environment and controlling an internal network. IT's role is to ensure connectivity with the cloud and assess the providers of cloud services. Within that responsibility is accountability for standards for information governance, including security, data privacy, and information retention and disposition.

Changes to legal considerations are immense. Organizations moving to the cloud must give considerable attention to data privacy issues, limitations of liability, security of intellectual property, and the challenges of electronic discovery (e-discovery). While these issues are each significant, the larger issue is the relative inexperience of global legal systems with the technical complexity and fundamental differences of cloud computing over traditional IT-driven computing environments.

Threatening Cloud Concerns

A white paper prepared by the Cloud Security Alliance in March of

2010 (<http://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf>) lists the most significant cloud concerns:

- Abuse and nefarious use of cloud computing
- Insecure application programming interfaces
- Malicious insiders
- Shared technology vulnerabilities
- Data loss and leakage
- Account, service, and traffic hijacking
- Unknown risk profile

Similarly, a recently published survey, “The Global State of Information Security Survey, 2010,”

Make sure you understand the risks – and are adequately prepared to mitigate, transfer, or accept them.

of 7,200 executives responsible for IT and security by PricewaterhouseCoopers (PwC) indicates additional areas of concern:

- Uncertain ability to enforce security policies at a provider (23%)
- Inadequate training and IT auditing (22%)
- Questionable privileged access control at the provider site (14%)
- Uncertain ability to recover data (12%)
- Proximity of the company’s data to that of others (11%)
- Uncertain ability to audit the provider (10%)

While all of the threats mentioned above are focused on the risks associated with cloud computing, they could apply equally to existing IT systems within most organizations. At the same time, the surveys point to the uneasiness that many executives have with moving critical data and applications to the cloud. As noted by the authors of the PwC survey: “Make sure you understand the risks – and are adequately prepared to mitigate, transfer, or accept them.”

Understanding the Risks

1. Data security

The most critical aspect of cloud computing is protecting the organization’s data. Measures to protect the data need to include consideration of data at rest (stored) in the cloud and data in transit to and from the cloud. An organization should give consideration to ensuring that data at rest is encrypted or, at least, stored in a manner that makes unauthorized retrieval of data difficult at best. In addition, the cloud provider’s security measures, including basic physical security measures of the data centers, need to be considered.

it can be monitored by the existing DLP infrastructure. This can have significant impacts on costs and bandwidth requirements.

2. Identity and access management

The most careful protection of data at rest and in transit is for naught if an unauthorized individual can gain access to it. Unfortunately, many cloud providers are unable to provide sophisticated protection in this area, relying upon single factor authentication (user name and password) with minimal integration to the organization’s existing identity and access management infrastructure. The good news is that this is evolving favorably, but challenges remain.

The critical considerations include multi-factor authentication, privilege management, and deauthorization or expiration of accounts. There are a number of emerging standards in this arena, including Security Assertion Markup Language, Service Provisioning Markup Language, eXtensible Access Control Markup Language, and Open Authentication. The challenge is that cloud providers adopt different standards, and the organization may need to provide support for multiple standards. Regardless of the standard chosen, it is critical the provider maintains extensive logging of access and provides those logs in real time and on demand to the organization. These logs will be the primary means of reference for an investigation should a data breach occur.

3. Resiliency

A major benefit of moving to the cloud is the reduction of IT’s costs associated with disaster recovery and business continuity. The burden is shifted to the cloud provider, and most cloud providers are capable of providing considerable resiliency and protection of data from a variety of disruptive events.

It is critical for the organization to fully understand the provider's disaster recovery plans and the full scope of resiliency associated with the provider's infrastructure. Most providers are prepared for normal disaster scenarios (e.g., natural disasters and power interruptions), but many are unprepared for disruptions caused by hackers (e.g., denial of service attacks) or failures of hardware or software. Likewise, the move to the cloud does not excuse the organization's IT department from providing multiple paths to the cloud provider and ensuring quality of service for those critical connections.

One of the challenges of cloud computing is validating the locus of a disruption. The IT department must retain the ability to diagnose its own internal network, the connections (public and private) to the cloud provider, and the health of the cloud provider. In addition, since many cloud applications can be accessed via the Internet directly, the organization's IT staff will need to be concerned with issues affecting various Internet service providers, cellular phone providers, and cable companies.

Within this space, the organization should also understand when the provider will perform maintenance and be unable to provide service. These maintenance windows need to be carefully managed, particularly for critical applications impacting a global business.

4. Legal issues

The legal considerations related to cloud computing are enormous. Some cloud providers are unwilling to negotiate their standard terms and conditions. In addition, some services can be obtained with a credit card and agreement through a click-through agreement by an end user. While most organizations limit the ability of employees to sign legal agreements, the ease of access to cloud services likely means that

The ease of access to cloud services likely means that many organizations may have existing relationships with cloud providers that have never been reviewed.

many organizations may have existing relationships with cloud providers that have never been reviewed by the organization's counsel. For example, the following is quoted from the May 26, 2010, standard online agreement for Amazon Web Services (<http://aws.amazon.com/agreement/>):

7.2. Security. We strive to keep Your Content secure, but cannot guarantee that we will be successful at doing so, given the nature of the Internet. Accordingly, without limitation to Section 4.3 above and Section 11.5 below, you acknowledge that you bear sole responsibility for adequate security, protection and backup of Your Content and Applications. We strongly encourage you, where available and appropriate, to (a) use encryption technology to protect Your Content from unauthorized access, (b) routinely archive Your Content, and (c) keep your Applications or any software that you use or run with our Services current with the latest security patches or updates. We will have no liability to you for any unauthorized access or use, corruption, deletion, destruction or loss of any of Your Content or Applications.

Under certain circumstances, this may be a perfectly acceptable agreement for an organization to agree to, but without legal review and com-

pensating security controls, an unwitting, but well-meaning, employee could expose sensitive data to unauthorized persons with no recourse to the cloud provider.

Cloud computing generally changes the complexion of e-discovery. Computer forensic techniques that are possible within an organization may be difficult or impossible with a cloud provider. The organization that expects to utilize data that resides with a cloud provider for legal purposes should fully understand how data can be retrieved when needed for litigation or investigation. The means of retrieval may require more detailed explanation and documentation than is required with standard computer forensic tools and processes. In addition, access to, and retrieval of, data in the cloud may take longer than is customary to expect. IT and the organization's counsel should partner closely in this space to fully understand and document the differences and service level expectations.

Also of concern, is the ability to establish legal holds on data residing in the cloud. Legal and IT must work closely with the cloud provider to understand the capabilities and limitations of the cloud provider's infrastructure to apply and account for legal holds.

Geographic location of data is a particularly difficult subject. This has significant data privacy implications, as well as legal jurisdiction issues. For example, in a criminal investigation, the physical location of certain data can impact whether

A chain is only as

strong

as its
weakest link

With Autonomy Information
Compliance, there are no weak links

Autonomy seamlessly links information across the entire enterprise using a single, powerful platform. With the ability to manage over 14 petabytes of data and understand the meaning of complex information, organizations can archive sensitive information and apply the correct risk management, security and compliance policies to data of any kind in real time, including audio and video, based on an understanding of the actual content. This continuous chain provides absolute control and visibility to manage the inherent risk in business information according to corporate, regulatory and legislative rules.

Leverage the strength of the Autonomy chain:

- 86 of the Fortune 100 use Autonomy Technology
- De Facto Standard for Global Enterprises, Securities Firms, and Regulators
- Only Vendor to Lead in Email Archiving, eDiscovery and Enterprise Search
- World's Largest Private Cloud

Build a chain that works for you—onsite or in the cloud:

www.autonomy.com/compliance

*“The fastest growing vendor
in the sector.”*

—IDC, 2009



the laws of a certain geography come into play (e.g., in the United States, whether state or federal laws have been broken). It is critical to understand, at least broadly, where data will be stored and whether or not the provider has the capability to prevent data from being stored in certain geographies.

Generally, records retention is a subject many cloud providers have yet to address in depth. Most of them will suggest blanket retention

For many organizations, this will include compliance with, among others:

- The Sarbanes-Oxley Act of 2002
- Payment Card Industry Data Security Standard
- Health Insurance Portability and Accountability Act
- The Gramm-Leach-Bliley Act

Cloud providers may be required to produce The American Institute of Certified Public Accountants' Statement on Auditing Standards

sive checklists, tasks, and procedures that an organization can tailor to its needs.

An organization should determine which standards and guidelines will be applied and monitored. Internal and external auditors will need access to the cloud provider in order to assess compliance and risk.

Evolving and Becoming Mainstream

For many organizations, the movement of data to the cloud will accelerate. The costs associated with basic maintenance of IT systems and applications increase on an annual basis. Since many large organizations have already outsourced IT operations, moving to the cloud is the next logical step. Smaller organizations gain the ability to utilize the robust IT infrastructure and capabilities of the cloud and obtain the benefits of capacity on demand.

With this shift, security and compliance will move to the forefront of many IT organizations – focusing attention on the data and its management. This shift may transform IT or information technology to IG or information governance.

Patrick Cunningham, CRM, FAI is senior director, information governance, at Motorola Inc., where he has worked since 2007. He has more than 20 years of records and information experience with organizations, including Hewitt Associates, Whittman-Hart, Household International, Archdiocese of Chicago, and Illinois State Archives. Cunningham is a frequent speaker on various topics to the records and information management community and has authored several articles on technology topics for ARMA International. He was the recipient of ARMA International's Britt Literary Award in 2009. Cunningham can be contacted at patrick.cunningham@ameritech.net.

Read More About It

***Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*, by Tim Mather, Subra Kumaraswamy, and Shahed Latif explores the implications of cloud computing security on privacy, auditing, and compliance for both the cloud service provider and the customer. Available at <http://oreilly.com/catalog/9780596802769/>.**

periods for information, regardless of content or use. They leave the responsibility solely to the organization and provide few tools to allow purging or archiving of obsolete data. The organization should also understand the extent to which end users can delete or archive data.

Lastly, the organization must fully understand what happens if the cloud provider enters bankruptcy protection or is involved in litigation. Likewise, since data belonging to multiple customers may be physically stored across many storage devices, the organization needs a full understanding of the likelihood of exposure of its data due to litigation or investigation involving another customer.

Measuring the Risks

Within the constraints of the service agreement, an organization needs the ability to measure compliance with the agreement and information security standards.

(SAS) 70 or SysTrust audit results.

Other applicable standards include:

- ISO/IEC 27001 *Information Technology – Security Techniques – Information Security Management Systems – Requirements*
- ISO/IEC 27002 *Information Technology – Security Techniques – Code of Practice for Information Security Management*
- *Control Objectives for Information and related Technology*, more commonly referred to as COBIT, from the Information Systems Audit and Control Association and the IT Governance Institute®
- *Internal Control – Integrated Framework*, from the Committee of Sponsoring Organizations of the Treadway Commission, more commonly referred to as COSO
- ITIL®, from the U.K. Office of Government Commerce, gives detailed descriptions of IT practices and provides comprehen-

Legal Implications

of Working in the Cloud

Stuart Rennie



Information governance is a daily feature of business practice, but being legally compliant when working “in the cloud” has made it more complicated.

Since the 1990s, use of the Internet has exploded worldwide. As of June 30, 2010, according to “The Internet Big Picture: World Internet Users and Population Stats,” nearly 2 billion of the world’s 6.8 billion people – almost one in three – are Internet users. This represents a 445% growth in just the last decade.

As the Internet expands, so does cloud computing. In its 2010 “Flying Blind in the Cloud: The State of Information Governance” study, the Ponemon Institute reported that most organizations plan to use cloud computing much more intensively by 2012 than they do now. In that same

study, the most popular cloud computing applications used by organizations today are business applications, such as webmail, computing platforms (e.g., Java, PHP, and Python), and infrastructure (e.g., storage and computing).

Among multiple users, *cloud computing* shares diverse computing resources by using the Internet as a platform and supports Internet communications using laptops, desktops, notebooks, and hand-held wireless devices. While the average Internet user does not know what cloud computing is, nearly 69% of American online users access cloud computing for webmail, data online storage, or Internet software, according to the 2008 “Cloud Computing Gains in Currency: Online Americans Increasingly Access Data and

Applications Stored in Cyberspace” from Pew Research Center.

Currently, the main driver of cloud computing is the private sector. Corporations and businesses of all sizes see the benefits in using cloud computing, said Jeffrey F. Rayport and Andrew Heyward in “Envisioning the Cloud: The Next Computing Paradigm.” These include:

- 24/7 worldwide access to information
- Collaboration among Internet users
- Computing on demand
- Cost-effective remote computer storage
- Lower management costs for organizations

While the benefits of using cloud computing are tempting for organizations, the legal risks can be high,

encompassing private and public law, civil and criminal law, and domestic and international law. Organizations engaging cloud computing service providers (CCSP) need to manage the legal risks and adopt information governance strategies to ensure legal compliance.

Protecting Proprietary Information

Protecting an organization's intellectual property in the cloud presents specific problems. Whether it be about patents, copyrights, trademarks, or trade secrets, use of cloud

Meeting E-Discovery Requirements

Using cloud computing can create legal obstacles to meeting e-discovery obligations in U.S. civil litigation. E-discovery is governed by the *Federal Rules of Civil Procedure* and state law, specifically the Uniform Rules Relating to Discovery of Electronically Stored Information Act from the NCCUSL. Organizations using cloud computing must be able to answer these questions:

- Can the organization, when subject to an e-discovery demand, execute a valid litigation hold to

... if the organization's data is transferred to another legal jurisdiction, it should know if that transfer violates the privacy laws of its home jurisdiction.

computing has blurred the legal landscape.

As the Internet has developed, it has spurred U.S. laws to be created to address its use. For example, the Digital Millennium Copyright Act (DMCA), which applies to CCSPs, makes anyone civilly liable for offering a product or service that purports to allow Internet users to avoid digital rights management copyright protection.

The Uniform Trade Secrets Act (UTSA), which was drafted by The National Conference of Commissioners on Uniform State Laws (NCCUSL) and adopted by most states, requires an organization to use reasonable efforts to maintain the confidentiality of its trade secrets.

Contracting with a CCSP may violate these legal principles, making a CCSP liable under DMCA for file sharing or causing an organization to lose trade secret protection under the UTSA.

prevent destruction or loss of records when its records are stored with a CCSP, perhaps offshore and comingled with other customers' data?

- Can the organization demonstrate it meets the legal requirements that its records with the CCSP are authentic, reliable, and have integrity?
- Can the organization preserve and produce its records needed for litigation?
- Will the costs paid by an organization to access its records via a CCSP outstrip the costs of any legal claim against it?

Protecting Privacy Rights

Breach of privacy is another risk, especially if new data created by transfer of records to the CCSP creates new privacy obligations to be met by the organization. For instance, if the organization's data is transferred to another legal jurisdiction, it should

know if that transfer violates the privacy laws of its home jurisdiction.

Europe

According to Articles 25 and 26 of the European Union (EU) Directive 95/46/EC, organizations doing business in Europe may transfer EU personal data to a "third country" (i.e., any country outside of the 27-member EU or the European Economic Area countries of Iceland, Liechtenstein, and Norway) only if they ensure an "adequate level of protection." The European Commission has identified several countries that meet that level of protection. In addition, some limited exemptions allow the transfer of data. For example, one exemption is that data may be transferred to companies that adhere to the Safe Harbor framework (see www.export.gov/safeharbor). For more information, see:

- "Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries," http://ec.europa.eu/justice_hom/fsj/privacy/docs/international_transfers_faq/international_transfers_faq.pdf
- "Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries," http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm.

Canada

Likewise, the Federal Court of Canada, in *Lawson v. Accusearch Inc.*, held that a U.S. organization transferring data to Canada must comply with the Canadian Personal Information Protection and Electronic Documents Act, notwithstanding the extraterritoriality of the organization or its website, if the privacy commissioner of Canada has jurisdiction over the subject matter of a complaint and can establish a real and substantial connection to

ARMA International's

Generally

Accepted

Recordkeeping

Principles®

What's GARP® Got to Do with It?

Find out with the **Generally Accepted Recordkeeping Principles® Overview** online course. This four-hour seminar will outline why the principles are the standard for excellence for record systems and why your organization should be **GARP®** compliant.

Vital information will help you sell the importance of information governance and the perils of ignoring compliance to your executive-level managers and other key staff in your organization.

ARMA members save

\$60

on the **Generally Accepted Recordkeeping Principles® Overview** online course



www.ama.org/learningcenter/onlinecourses/garp

Canada. This finding was based on “Reaching for the Cloud(s): Privacy Issues related to Cloud Computing” from the Office of the Privacy Commissioner of Canada.

United States

In addition to jurisdictional matters, the U.S. Privacy Act applies to cloud computing and lays down security and records management requirements to be met for the collection, maintenance, use, and disclosure of personal information held by federal agencies.

... the contract an organization has with its CCSP [cloud computing service provider] is a key tool to help reduce its legal risks.

The federal Electronic Communications Privacy Act (ECPA) regulates U.S. government access to e-mail and computer records held by third parties, such as CCSPs, and it is complex and wide-reaching. For example, the ECPA permits a CCSP to disclose to government an organization’s records used for remote storage without a warrant. As a result of the continued growth of the Internet and cloud computing, there is general consensus the ECPA is in need of modernization. Digital Due Process, a coalition of privacy advocates, major companies, and think tanks, has been advocating for ECPA reform, which may soon affect cloud computing.

Another statutory requirement affecting cloud computing for U.S. federal agencies (or their contractors) is the Federal Information Security Management Act, which spells out compliance requirements to be met to ensure information security.

Protection for personal health information held by federal and specified entities is required by the Health

Insurance Portability and Accountability Act (HIPAA) and the HIPAA Privacy and Security Rules, which protect electronic health information and give patients specific rights over their health information.

The Sarbanes–Oxley Act requires public companies to comply with financial accounting standards and comply with the auditing standards issued by the Public Company Accounting Oversight Board.

The USA PATRIOT Act was created to compel disclosure of data and records to the government held by

CCSPs to protect against foreign and domestic terrorism. And, as originally drafted, the act required CCSPs and other providers who received a subpoena or national security letter (NSL) from the Federal Bureau of Investigation (FBI) not to notify an organization for which it was storing or processing data that it had disclosed records to the government.

However, in *John Doe Inc. v. Mukasey*, the U.S. Court of Appeals found that the NSL provisions violated the free expression guarantees in the First Amendment, and the court narrowed the rule prohibiting CCSPs and other providers from disclosing NSLs. While the FBI is now subject to increased judicial review as a result of this decision, it can continue issuing NSL requests.

The federal Computer Fraud and Abuse Act (CFAA) imposes civil and criminal sanctions on those individuals who commit computer fraud or gain unauthorized access to protected computers. The courts have interpreted the unauthorized access provisions

in the CFAA broadly. In *EF Cultural Travel BV v. Zefer Corp.*, the First Circuit held that a lack of authorization could be established by an explicit statement on a website restricting access.

Negotiating Contractual Protection

Given the current state of the law and cloud computing, the contract an organization has with its CCSP is a key legal tool to help reduce its legal risks. Central to cloud computing is that an organization cedes control of its records to the CCSP. In its “Flying Blind in the Cloud” study, the Ponemon Institute reported that few organizations take proactive steps to protect their own sensitive business information and that of their customers, consumers, and employees when they contract with CCSPs to store their records. In addition, fewer than one in 10 organizations says it uses any kind of product vetting or employee training to determine that the CCSP meets all appropriate security requirements.

It is common for CCSP standard form contracts to be “as is,” where goods and services are provided without promise of being suitable or achieving performance levels. Some contracts allow a CCSP to change or terminate service at any time without notice to the organization. The risk to an organization legally bound by these contractual terms can be enormous:

- Data can be inaccessible when there is a loss of service by the CCSP.
- Data can be lost or destroyed by spoliation.
- Data can be subject to unlawful access by malicious insiders or others.
- Data loss may compromise intellectual property, confidential business information, and trade secrets.
- Data loss may breach an organi-

Helpful Cloud Security Laws and Regulations

United States

- Cloud Security Alliance, www.cloudsecurityalliance.org/cm.html
- Computer Fraud and Abuse Act of 2006, www.law.cornell.edu/uscode/18/1030.html
- Digital Due Process, www.digitaldueprocess.org
- Electronic Communications Privacy Act of 1986, www.it.ojp.gov
- Federal Information Security Management Act of 2002, <http://csrc.nist.gov/groups/SMA/fisma/index.html>
- Federal Rules of Civil Procedure, www.law.cornell.edu/rules/frcp/
- Health Insurance Portability and Accountability Act of 1996 www.hhs.gov/ocr/privacy/
- International Organization for Standardization (ISO) / International Electrotechnical Commission publications, www.iso.org/iso/iso_catalogue.htm
- The National Conference of Commissioners on Uniform State Laws, www.nccusl.org
- National Institute of Technology (NIST) Special Publication 800-53 – Recommended Security Controls for Federal Information Systems, Revision 2 (Dec 2007), <http://csrc.nist.gov/publications/PubsSPs.html>
- Payment Card Industry (PCI) Data Security Standard (DSS) Requirements and Security Assessment Procedures, Version 1.2 (Oct 2008), www.pcisecuritystandards.org/index.shtml
- Sarbanes–Oxley Act of 2002 and the Public Company Accounting Oversight Board, <http://pcaobus.org/Pages/default.aspx>
- The Statement on Auditing Standards (SAS) No. 70, Service Organizations, <http://sas70.com>
- USA Patriot Act of 2001, www.justice.gov/archive/ll/highlights.htm
- U.S. Privacy Act of 1974, www.justice.gov/opcl/privstat.htm

Europe

- www.enisa.europa.eu
- <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/30&format=HTML&aged=0&language=EN&guiLanguage=en>
- <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/130&format=HTML&aged=0&language=EN&guiLanguage=en>
- http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp170_en.pdf

Canada

- Office of the Privacy Commissioner of Canada, www.priv.gc.ca/

Other Resources:

- ARMA International Generally Accepted Recordkeeping Principles® (GARP®), www.arma.org/garp/index.cfm
- “Cloud Computing Gains in Currency: Online Americans Increasingly Access Data and Applications Stored in Cyberspace,” Pew Internet and American Life Project, <http://pewresearch.org/pubs/948/cloud-computing-gains-in-currency>
- “Envisioning the Cloud: The Next Computing Paradigm,” Marketspace Advisory, www.marketspaceadvisory.com/cloud/
- “Flying Blind in the Cloud: The State of Information Governance,” Ponemon Institute, sponsored by Symantec, www.symantec.com/business/theme.jsp?themeid=cloud
- World Internet Usage and Population Statistics, www.internetworldstats.com/stats.htm

zation's privacy duties.

- Terms of service may not be compliant with an organization's e-discovery obligations.
- Terms of service may not comply with government subpoenas.

Organizations can mitigate their legal risks by negotiating specific terms into their contracts with CCSPs to:

1. Ensure continuity of service to access its data
2. Protect the data with encryption and segregation
3. Provide that data will be stored in local jurisdictions

... organizations can employ GARP® to have an effective, responsible, and legally compliant recordkeeping system when enjoying the benefits of cloud computing.

4. Prevent unlawful access or transfer
5. Allow data access for law enforcement

These negotiated contracts may have protections for intellectual property and provisions ensuring e-discovery obligations are met. In addition, an organization may seek to have the CCSP agree to subject its procedures and operations to audits and to provide indemnities to the organization if the CCSP breaches its contract.

In a similar way, an organization can protect itself from CCSP negligence for a breach of duty of care regarding the access, maintenance, use, and disposition of the organization's records, such as negligent destruction of records by the CCSP.

Suggesting Compliance with Standards

Where the current law is unclear or absent, CCSPs have adopted voluntary standards as a way to comply with industry best practices, mitigate their legal liability, and provide bet-

ter service to organizations. For example:

- ISO/IEC 27002:2005 *Information Technology – Security Techniques – Code of Practice for Information Security Management* sets out information security management guidelines for CCSPs to follow.
- The American Institute of Certified Public Accountants' Statement on Auditing Standards (SAS) 70 requires an audit of a CCSP's information technology and processes, including sensi-

tive data, in order for it to be SAS 70 certified.

- The National Institute of Technology's 2007 *Recommended Security Controls for Federal Information Systems* provides guidelines for federal agencies' information systems security controls.
- The Cloud Security Alliance's Cloud Controls Matrix provides fundamental security principles for users and CCSPs to assess the CCSPs' overall security risk.
- The Payment Card Industry Data Security Standard is a widely accepted security assessment tool for certifying credit card transactions by CCSPs, merchants, and others.

Comforting with a Chance of Risk

CCSPs' compliance with security standards provides organizations with a level of comfort and works to minimize legal risks. None of the standards listed here specifically addresses records management concerns as

comprehensively as the ARMA International Generally Accepted Recordkeeping Principles® (GARP®) for information governance.

Providing guidance for accountability, integrity, protection, compliance, availability, retention, disposition, and transparency of recordkeeping systems, the GARP® principles are comprehensive enough to account for the challenges posed by cloud computing, but general enough in nature for application, irrespective of organization, industry, or jurisdiction. Consequently, organizations can employ GARP® to have an effective, responsible, and legally compliant recordkeeping system when enjoying the benefits of cloud computing.

In a 1908 letter, Mark Twain said, "Thunder is good, thunder is impressive; but it is lightning that does the work." In the same way, policies are good, procedures are important, but it is an organization's continued vigilance in executing its information governance strategies that is the lightning that does the needed work of providing legal protection for cloud computing.

Stuart Rennie is a lawyer and records management consultant in Vancouver, British Columbia, Canada. He is the co-author of the Local Government Management Association of British Columbia Records Management Manual. (3rd Ed.). Rennie is a researcher at the InterPARES (International Research on Permanent Authentic Records in Electronic Systems) Project at the University of British Columbia (UBC) and an adjunct professor at the School of Library, Archival and Information Studies at UBC. He is a member of Sedona Canada and participated in the development of "The Sedona Canada Principles Addressing Electronic Discovery." Rennie can be contacted at stuart_rennie@telus.net.

Claim Your Seat at the Table.



Complete Your Organization's Information Management Strategy with the most-powerful Physical Records Management Software.

FileTrail makes Physical Records Management part of the bigger solution with:

- ▶ Physical and Electronic Records Integration
- ▶ Automated Compliance, Legal Holds, and Retention
- ▶ File Room Automation and Space Management
- ▶ Global Scalability Across Borders and Languages

ARMA Attendees:



Scan this bar code for a chance to win \$1,000 dollars.

*Offer limited to first 500 scans.

See www.FileTrail.com/arma 2010 for your complimentary whitepaper:
Achieving Physical Records Management Goals within a SharePoint Content Solution

FILETRAIL[®]
FileTrail for SharePoint[™] - Complete Records Management

111 N. Market Street, Suite 715 | San Jose, CA 95113-1108 | Phone: 800.310.0314

www.filetrail.com



Information Governance

- Risk mitigation
- Litigation readiness
- Operational efficiency

www.rsd.com



Reduce business risk:

- Centralize information governance policy creation and management
- Enforce policy across locations, jurisdictions and repositories

Improve litigation readiness:

- Ensure compliance at content creation time
- Respond swiftly to discovery in the event of litigation

Enhance productivity:

- Search and retrieve governed content in any format from anywhere in the enterprise
- Reduce operating costs by optimizing use of hierarchical storage systems



Are your records ready for litigation?

Gauge your level of litigation readiness with a free 8-Point Inspection.



If your organization were sued tomorrow, would your records management, IT, and legal teams be ready to respond effectively and efficiently?

Being “litigation ready” is often too vague and subjective to be meaningful. Our free 8-Point Inspection adds objectivity so that you can more clearly assess how prepared your organization truly is. **Download the free self assessment guide today!**

zylab.com/arma8point | 1-866-ZYLAB NA

ZyLAB[®]
eDiscovery & Information Management