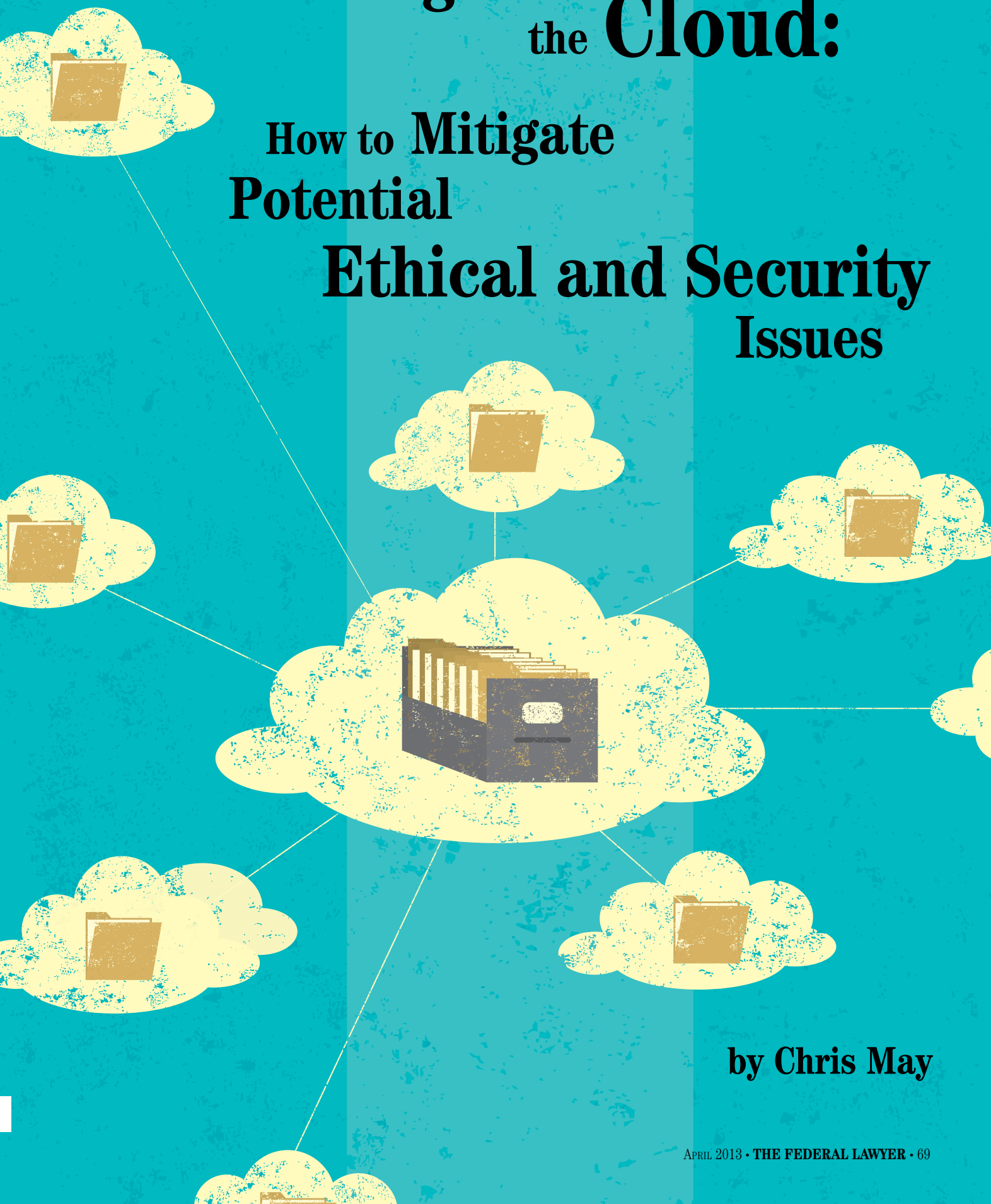
Seeing Into the Cloud:

How to Mitigate Potential Ethical and Security Issues



by Chris May

Federal lawyers may be used to a dizzying array of acronyms, but recent government security initiatives are beginning to sound a lot like alphabet soup—FISMA, NIST, FedRAMP, FIPS, and the list goes on. These are security initiatives for information technology (IT) that represent a fundamental shift in the way that agencies manage data, and they will have wide-ranging impacts across agencies for lawyers involved with litigation, particularly the e-discovery phase. If attorneys haven't done their homework on security initiatives and the federal government's push to the cloud, they need to start now. They can begin by understanding what this means for how agency data is secured, where it resides, who actually owns it and how the changes will impact the way attorneys work with IT and provide information to opposing counsel.The government and many private businesses have already moved some of their data to cloud environments or are considering the move. Consider that two-thirds of mid-size businesses are either planning or currently deploying cloud-based technologies to improve IT systems management while lowering costs, according to a 2011 survey by IBM. The survey, *Inside the Midmarket: A 2011 Perspective*,[1] found that respondents anticipate that cloud computing will help them reduce costs, better manage IT, and improve system redundancy and availability.

While cloud computing can bring numerous advantages, the road to the cloud is not smooth or easy. While moving infrastructure, data storage, software, and other IT components to the cloud can save money and ultimately make e-discovery easier and faster, there are significant security risks. Government lawyers must understand that their colleagues or third-party contractors in IT, who are already under significant pressure from these initiatives, may not be thinking of legal holds, chain of custody, spoliation, and other e-discovery-related issues when they develop contracts and service-level agreements (SLAs) with cloud-based providers. In order to stay ahead of these issues and ensure that cloud computing ultimately benefits agency employees and taxpayers, federal lawyers need to know what their IT departments are doing now with the move to the cloud and what they plan to do in the future. They also need to understand the ethical implications involved with cloud computing and moving client data to a virtual environment.

Security and Cloud Concepts

For attorneys, the first step involves becoming familiar with how "the cloud" works, along with basic security issues that it entails. As part of the Obama administration's cloud initiatives, in 2011, the National Institute of Standards and Technology (NIST) released *The NIST Definition of Cloud Computing*,[2] which laid out essential characteristics of cloud computing and different service models for cloud-based environments

According to the NIST, there are five essential characteristics, three service models, and four deployment models of cloud computing.

The Five Essential Characteristics of Cloud Computing

1. On-Demand Self-Service: Through cloud computing, consumers can unilaterally and automatically provision computing capabilities as they are needed, such as server time and network storage, without requiring human interaction with each service provider.
2. Broad Network Access: The cloud offers capabilities over the network that can be offered through different platforms, such as mobile phones, tablets, laptops, and workstations.
3. Resource Pooling: The cloud allows providers to serve multiple consumers with different resources, such as storage, processing, and bandwidth, based on demand. Consumers generally don't know exactly where the resources are provided.
4. Rapid Elasticity: Cloud resources can be quickly scaled up and down based on demand, sometimes automatically. Consumers have virtually limitless options and can request more or fewer resources at any time.
5. Measured Service: With the cloud, resources can be automatically controlled and optimized, based on what is appropriate for the type of service, such as storage and bandwidth. The cloud allows for transparent resource usages, so providers and consumers know what they are getting and using.

The Three Basic Service Models for Cloud Computing

1. Software as a Service (SaaS)**:** The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based e-mail), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.[3]
2. Platform as a Service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming."[4]
3. Infrastructure as a Service (IaaS): The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).[5]

So, what do the different service models actually mean for non-IT folks? For one thing, it means that software that used to be loaded on to computers or network storage servers that used to exist down the hall are now virtual. With the cloud, there are no physical servers.

SaaS is the cloud service model most people are familiar with—anyone with a Hotmail, Yahoo, Gmail, or other free e-mail account uses SaaS. The e-mail provider, whether it's Microsoft, Google, or someone else, controls the software that powers the e-mail program. Users don't get to decide when their e-mail software is upgraded, how their inbox will look, or where their e-mail is actually stored online. Someone who works for the service provider makes all those decisions.

One common use of IaaS is hosting websites. By using the cloud, agencies don't manage disaster planning, continuity, and other issues. No one on staff needs to be on call 24/7 in case the website crashes, since that is the responsibility of the IaaS provider.

PaaS tends to be the most difficult model for non-IT people to understand, as well as the least known. One of the more familiar examples of PaaS is Facebook. Developers create a specific application using the Facebook proprietary application programming interface (API) and make that application available to users. An example of this is the game Farmville which is only available on the Facebook platform.

The level of control that agencies have will depend on which service model they use, although cloud-based service models by definition include a lesser degree of control than what most agencies are probably used to having. They will have less control over SaaS than PaaS, but more control with the IaaS model than the PaaS model.

The Four Deployment Models of Cloud Computing

1. Private Cloud: With a private cloud, the agency or organization is the only one who uses it. Private clouds may be owned, managed, and operated by the agency or a third party, or a combination of the two groups. They may be located on-site or off-site. These types of clouds are generally very reliable, but they are also very expensive.
2. Community Cloud: A community cloud is used by specific groups that share certain standards, such as security requirements and compliance considerations. One or more of the group members may own, manage, and operate the cloud, a third party may do so, or a combination of the provider and groups may do it. It can exist on or off the premises of one of the members.
3. Public Cloud: This model is open to the general public and may be owned, managed, and operated by a company or academic or government group, or a combination of them. The cloud provider hosts a public cloud. This is the cheapest model, but the least secure one.
4. Hybrid Cloud: This model brings together aspects of private, community, and public clouds that are linked through standardized or proprietary technology.

The different service models and deployment models that agencies choose to use will have a significant impact on the agency's data, including how much control the agency has, what the destruction and retention policies are, where data resides, and how quickly and in what formats agency attorneys can access their information.

Why the Push to the Cloud?

For agency attorneys, the cloud isn't something they can ignore

Making Sense of the Alphabet Soup

The Obama administration's cloud-first policy introduces an entirely new vocabulary to many attorneys. Some of the key terms federal lawyers need to know include:

3PAO: Third-party assessment organization, an accredited group that performs initial and ongoing assessment of CSP systems under FedRAMP requirements.

API: Application programming interface.

C&A: Certification and accreditation.

CCACL: CIO Council Cloud Computing Advisory Council, established at the behest of the CCESC to serve as a collaborative environment for senior IT experts from across the federal government.

CCESC: The CIO Council Executive Cloud Computing Executive Steering Committee, which the federal CIO Council established to provide strategic direction and oversight for the Federal Cloud Computing Initiative.

CSP: Cloud service provider.

ESI: Electronically stored information.

FAR: Federal acquisition regulation.

FCCC: Federal Cloud Compliance Committee.

FDCCI: Federal Data Center Consolidation Initiative launched in February 2010 that has issued guidance for Federal CIO Council agencies.

FedRAMP: The 2010 Federal Risk and Authorization Management Program, which defined requirements for cloud computing security controls, including vulnerability

and hope it goes away. The Obama administration has made it very clear that every agency will be expected to move to the cloud as a way to save money on the IT budget and improve IT services.

The push to the cloud began in earnest in December 2010, when then-U.S. Chief Information Officer (CIO) Vivek Kundra released a memo that laid out how and when agencies must move more data and services to cloud environments. The memo acknowledged previously less-than-successful attempts to streamline IT services and improve performance while cutting costs. Initially, IT and legal departments were forgiven for failing to embrace the mandates, but subsequent memos and reports over the last two years have shown just how serious the federal government is about the initiative.

December 2010—25 Point Implementation Plan to Reform Federal Information Technology Management[6]

Starting with this memo, the U.S. CIO laid out an ambitious agenda to require agencies to default to cloud-based services whenever that "secure, reliable, cost-effective" option exists. The memo highlighted multiple advantages that moving agencies to the cloud would bring, including cost savings, greater flexibility, and faster procurement and certification processes.

The memo outlined how the government's current approaches to data management contained serious flaws and were very expensive. One example was the Car Allowance and Rebate System (CARS), also known as "Cash for Clunkers." That program stumbled when demand far exceeded the initial projections of consumers looking to trade in their older cars and receive a subsidy for new, more fuel-efficient vehicles. The National Highway Traffic Safety Administration's customized commercial application, which was hosted in a traditional data center environment, crashed under the number of people applying for it. "The Federal Government must be better prepared in the future," the memo stated.

The implementation plan included:

- Shifting to a "cloud-first" policy. This point required every agency to identify 3 services within 3 months, move 1 of those services to the cloud within 12 months and the remaining 2 within 18 months.
- Of the existing 2,094 federal data centers, reducing those by at least 800 by 2015.

Among other aspects, the plan also required IT to turn around or eliminate at least one-third of underperforming IT projects in the next 18 months and limit funding approval of major IT programs to those with a dedicated program manager and a fully staffed integrated program team.

The memo also promised that within six months, the U.S. CIO would publish a strategy to help agencies set up safe, secure cloud computing, which the NIST would lead. Of course, after the strategies were published, agencies would only have six more months to move their first program to the cloud.

February 2011—Federal Cloud Computing Strategy[7]

The next significant memo came two months later, when the Obama administration began to provide some guidance on how agencies could implement the cloud-first policy. It also pushed agency IT departments to adopt cloud computing services more quickly.

This publication reported that in fiscal year 2010, about 30 cents

scanning, and incident monitoring, logging, and reporting.

FIPS: Federal Information Protection Standard.

FISMA: Federal Information Security Management Act of 2002, which outlines security requirements, including compliance with Federal Information Processing Standards agency-specific policies; authorization to operate requirements; and vulnerability and security event monitoring, logging, and reporting.

FRA: Federal Records Act.

IaaS: Infrastructure as a Service.

JAB: Joint Authorization Board.

NIST: National Institute of Standards and Technology.

PaaS: Platform as a Service.

PIA: Privacy Impact Assessments, designed to ensure that federal agencies evaluate and consider how they will mitigate privacy risks and comply with applicable privacy laws and regulations governing an individual's privacy, to ensure confidentiality, integrity, and availability of an individual's personal information at every stage of development and operation.

PII: Personally Identifiable Information, which can include information about federal agency employees, internal users, and members of the public.

PMO: Program Management Office.

SaaS: Software as a Service.

SAJACC: Standards Acceleration to Jumpstart Adoption of Cloud Computing project.

TIC: Trusted Internet Connection.

of every dollar invested in federal IT was spent on data center infrastructure. The document also identified that the federal government spends $80 billion a year on IT, and that it believed approximately one-quarter of that ($20 billion) could be a target for migrating to the cloud.

At this point, the Obama administration also began to speak about IT in a different way, with a focus on providing services rather than assets such as hardware and software. "Cloud computing can allow IT organizations to simplify, as they no longer have to maintain complex, heterogeneous technology environments. Focus will shift from the technology itself to the core competencies and mission of the agency."[8]

IT was also urged to adopt a different mindset regarding its mission. "To be successful, agencies must manage cloud services differently than traditional IT assets," according to the memo. "[C]loud computing will require a new way of thinking to reflect a service-based focus rather than an asset-based focus."[9]

This new mindset should encompass a focus on output metrics, such as SLAs, instead of input metrics, such as the number of servers. While this memo didn't specifically refer to e-discovery litigation (unlike future memos), it did call on agencies to "actively track SLAs and hold vendors accountable for failures. Agencies should stay ahead of emerging security threats and ensure that their security outlook is constantly evolving faster than potential attacks."[10]

The memo also introduced some of the NIST's definitions of basic cloud computing standards, which were described above.

December 2011—Security Authorization of Information Systems in Cloud Computing Environments (FedRAMP)[11]

This memo, issued by then-new U.S. CIO Steven VanRoekel, introduced the term FedRAMP to most agency employees. As the U.S. General Services Administration (GSA) says on its website: "The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services."[12] This memo also provided the first introduction for many to cloud service providers (CSPs).

The goal behind FedRAMP is to improve consistency and allow each agency to avoid reinventing the wheel and duplicating similar cloud-related efforts that other agencies have already undertaken. By creating transparent standards and processes and letting agencies leverage security authorizations government-wide, it is designed to significantly speed up adoption of the cloud. Under the FedRAMP framework, once one agency has certified a CSP, other agencies can utilize that CSP with minimal paperwork. It is a "certify once, use many places" approach.

This memo continued the previous CIO's cloud-first strategy, and it outlined the interaction among the four key stakeholders that make up FedRAMP: the U.S. Department of Homeland Security, the FedRAMP Joint Authorization Board (JAB), a Program Management Office (PMO), and executive departments and agencies.

February 2012—Creating Effective Cloud Computing Contracts for the Federal Government: Best Practices for Acquiring IT as a Service[13]

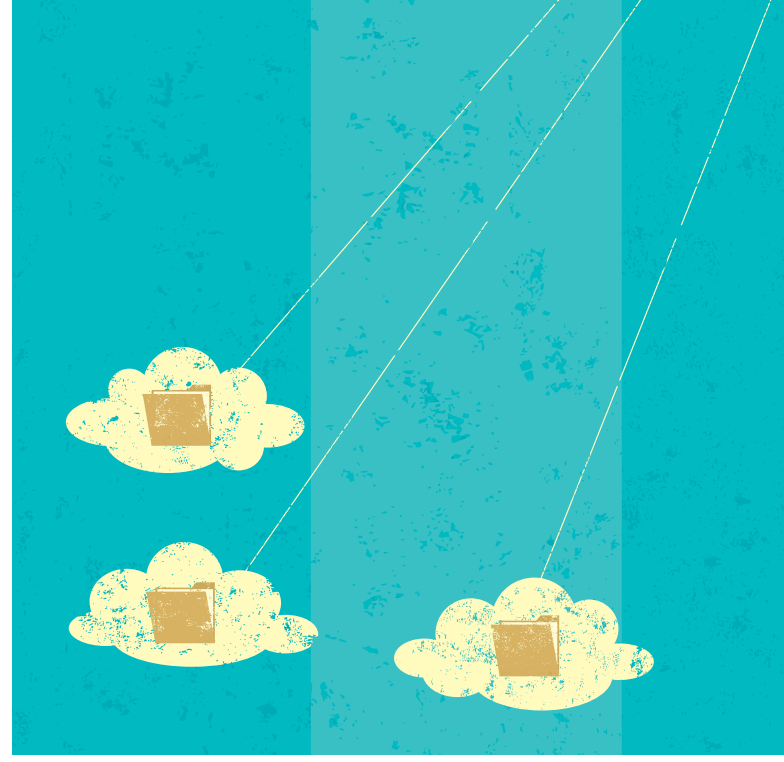
Earlier this year, the CIO Council and the Chief Acquisition Officers Council, in cooperation with the Federal Cloud Compliance Committee (FCCC), directly tackled the issue of IT procurement and how it affects e-discovery.

> Cloud computing presents a paradigm shift that is larger than IT, and while there are technology changes with cloud services, the more substantive issues that need to be addressed lie in the business and contracting models applicable to cloud services," the document stated. This new paradigm requires agencies to re-think not only the way they acquire IT services in the context of deployment, but also how the IT services they consume provide mission and support functions on a shared basis. Federal agencies should begin to design and/or select solutions that allow for purchasing based on consumption in the shared model that cloud-based architectures provide.[14]

If attorneys are only now catching up to speed with the cloud movement and the conversations they need to have with IT, this document provides extremely useful talking points. Lawyers can use the issues highlighted in it when meeting with their IT colleagues to discuss procurement contracts and to better ensure that their litigation and e-discovery concerns are embedded in the process.

Creating Effective Cloud Computing Contracts[15] highlights 10 areas where agency programs, CIO, general counsel, privacy, and procurement offices must collaborate and align on contracts for cloud computing services, although different agencies may have additional areas of concern:

1. Selecting a cloud service: Choosing the appropriate cloud service and deployment model is the critical first step in procuring cloud services.
2. CSP and End-User Agreements: Terms of Service and all CSP/customer-required agreements need to be integrated fully into cloud contracts.
3. SLAs: SLAs need to define performance with clear terms and definitions, demonstrate how performance is being measured, and what enforcement mechanisms are in place to ensure SLAs are met.
4. CSP, Agency, and Integrator Roles and Responsibilities: Careful delineation between the responsibilities and relationships among the federal agency, integrators, and the CSP are needed in order to effectively manage cloud services.
5. Standards: The use of the NIST cloud reference architecture as well as agency involvement in standards are necessary for cloud procurements.
6. Security: Agencies must clearly detail the requirements for CSPs to maintain the security and integrity of data existing in a cloud environment.
7. Privacy: If cloud services host "privacy data," agencies must adequately identify potential privacy risks and responsibilities and address these needs in the contract.
8. E-Discovery: Federal agencies must ensure that all data stored in a CSP environment is available for legal discovery by allowing all data to be located, preserved, collected, processed, reviewed, and produced.
9. Freedom of Information Act (FOIA): Federal agencies must ensure that all data stored in a CSP environment is available for appropriate handling under FOIA.



10. E-Records: Agencies must ensure CSPs understand and assist federal agencies in compliance with the Federal Records Act (FRA) and obligations under this law.

Of further interest to attorneys, the document specifically focuses on e-discovery and the challenges and issues that cloud computing will bring for the legal department and their colleagues in IT. As a precautionary tale, it cites *In re Fannie Mae Securities Litigation*,[16] where the agency was held in contempt for failing to meet discovery deadlines even though it had already spent $6 million on the discovery process.

The government identified five key areas where cloud solutions intersect with e-discovery: information management, locating relevant documents, preserving data, moving documents, and potentially avoiding costs by incorporating e-discovery tools in CSP environments. In order to ensure that contracts and SLAs are written in order to allow federal lawyers to conduct e-discovery, attorneys need to understand how each area works in the cloud and what pitfalls to avoid.

Information Management

When agency data resides on its servers down the hall, there is no question about who "owns" the data and when it can be accessed. When data lives in the cloud, it becomes much more complicated. When choosing CSPs, drafting contracts, and crafting SLAs, attorneys need to ensure that they can get to data without IT involvement, and that the agency's ownership of their own data is explicitly spelled out. They must also consider data requests and demands by third parties, including court subpoenas that could be sent directly to the CSP, and include in the agreement that the agency must be notified when the CSP receives a third-party data request.

Locating Relevant Documents

Finding potentially responsive electronically stored information (ESI) is challenging enough when it resides on the agency's servers, but it can become even more time-consuming when the CSP has to do it. Contracts and SLAs need to explicitly state the process, time frame, and expense for the cloud provider to act upon agency requests. The contract should also take into consideration what the costs will be when the agency has an exceptionally large request or needs data particularly fast. Software is another consideration, and attorneys need to clarify the provider's exact duties and capabilities to search, preserve, collect, and produce data using the agency's programs, a cloud-based system, or other approach.

Preserving Data

Litigation holds present another area that is made more complicated by the cloud. Attorneys should assume that the CSP has data retention and destruction policies that apply to its other clients, not just their own agency. When those policies have to be suspended for one agency, they may be suspended for others as well—and the reverse may be true. The process for litigation holds must be clear and explicit and built into the contract. When considering data retention and preservation policies, metadata should be included as well.

The E-Discovery Lifecycle

Along with securing and storing data in the cloud, attorneys also need to think about how it will be exported and produced for litigation. When done right, storing ESI in the cloud should actually make it much easier, cheaper, and faster to find, de-dupe, and index responsive records. Attorneys should be sure that their contracts allow for robust enterprise search capabilities with an integrated, centralized approach. They want to be able to dictate how the CSP will export data into the agency's preferred software environment and in the formats it dictates, while at the same time being able to document the chain of custody.

Cost Control in the Cloud

When it comes to e-discovery budgets, a cloud-based environment can actually live up to the administration's goals. Litigation is enormously expensive, but with the right e-discovery tools built into the CSP contract, such as data search and collection capabilities, the legal department may be able to save a great deal of money while improving IT efficiencies.

In order to make the process easier, the administration has offered a list of questions that attorneys can take to the IT and procurement departments, then together address them to potential CSPs. Those questions include:

1. How does the agency or CSP halt the routine destruction of agency information in the cloud when a litigation hold has been implemented?
2. Does the agency or the cloud provider's document retention/management plan apply to the agency's data stored in the cloud? Is it understood whose plan has priority in cases when they conflict?
3. Is the metadata preserved when agency data is migrated into, out of, and within the cloud? (i.e., are transfers forensically sound)?

    a. Will the agency be able to search the data in the cloud by metadata field? For example, will the agency be able to batch search for all agency data in the cloud by original date created, file type, or author?

b. Does the cloud provider ensure that metadata remains linked to records during data migration?

4. Pursuant to the agreement, does the agency itself have the ability to search, retrieve, and review agency data in the cloud? Using the agency's own tools? Agency's e-discovery contractor's tools?
5. What are the agency's file format export options for exporting agency data out of the cloud? What are the expenses associated with this process?
6. Is the cloud provider or a third party providing e-discovery services to the agency?
   a. What specific e-discovery services by the cloud provider are included in the contract?

      i. E-discovery services can include the process of managing, identifying/locating, preserving, collecting, processing, reviewing, and producing electronically stored information (ESI). What specific tools are being utilized for these e-discovery services?

   b. Will the cloud provider or third party provide training on the e-discovery tools offered?
   c. What project management resources will be available for the e-discovery services?
   d. Have the e-discovery services of the cloud provider or third party been tested? If collection is one of the e-discovery services provided, is the collection method forensically sound?
   e. Can the agency modify the e-discovery protocol/process of the cloud service provider or third party as warranted?
   f. How will e-discovery of data in the cloud be handled during user migration?
   g. Does the cloud provider have forensic or litigation experts available to answer questions and/or sign affidavits regarding the e-discovery services provided in the cloud?
   h. Will the cloud provider and third-party employees sign chain of custody affidavits to demonstrate the integrity of the ESI when needed for litigation purposes?
   i. If requested, will the cloud provider be able to supply the agency with audit trails, exception reports, and transaction logs?
   j. What if any additional charges will be required for e-discovery services discussed above?

7. Does the contract require that the agency fund or otherwise support the cloud provider's response to a third party?
8. Is the contract clear that the cloud provider and all associated subcontractors shall not release any agency information and/or data without written agency approval or about circumstances when such approval is not needed?
   a. Is the contract clear that the cloud provider will notify the agency within a mutually agreed upon time frame when a request for agency information or data is received by the cloud provider or subcontractor? Who is the designated agency point of contact(s) for this notice?

9. If the agency desired to extract the data so that it can be loaded into a separate review platform, will work product from the cloud review platform be transferable to a separate review database?
10. Will attorneys and staff have immediate access to review the data in the review platform if hosted by the cloud provider in the cloud?
    a. Is there 24/7 access to the review platform?
    b. Can approved, non-agency personnel (i.e., other agencies or contractors) access the review platform in the cloud?

Attorneys should consider these the basic questions to ask. The memo also spells out other, more general questions and concerns that may apply to different agencies, depending on the amount and type of litigation the legal department manages and the general security concerns a specific agency has. High-level employees at one agency may require stricter security measures regarding e-mail than those at another agency, for example. When dealing with a CSP, attorneys should never forget that they are not the only ones using the cloud. The agency may not be able to customize upgrades and security features like it can with an in-house, hosted environment. In order to do that, agencies would fundamentally lose the benefits and cost savings derived from a cloud-based environment.

The Ethical Challenges

To further complicate the situation, government lawyers must also consider the ethical implications involved with the cloud, particularly under the ABA *Model Rules of Professional Conduct*[17]:

- *Rule 1.1: "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."* For lawyers today, that means they must have a basic understanding of today's technology, including the cloud.
- *Rule 1.6: "A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent…."* This rule goes to the heart of ensuring that any data that resides in the cloud is secure from hacking and inadvertent disclosures.
- *Rule 1.15: "A lawyer shall hold property of clients or third persons that is in a lawyer's possession in connection with a representation separate from the lawyer's own property…. Other property shall be identified as such and appropriately safeguarded."* "Property" includes client information, and attorneys need to safeguard it in the cloud just as they would if it were stored on a server.

So What Does It All Mean?

While the cloud-first policy and FedRAMP may seem to be primarily IT procurement process mandates, they impact e-discovery in three significant ways:

Clients' ESI, Including E-Mail and Other Communications, Will Reside Outside the Agency's Firewall

By its very definition, cloud computing means that data exists on a network that a third party will have access to. In order to ensure that data is secure and available for e-discovery and other litigation issues, attorneys need to find out where the IT department is in the process of signing up CSPs, which systems they have moved to the cloud, and which are lined up to move next.

The IT Department Is Facing Sweeping Mandates, Difficult Timelines, and a Great Deal of Uncertainty Right Now

The move to the cloud is designed to significantly change how IT thinks of its mission, and it could vastly alter budgets and staffing. IT colleagues may not be focused on how their actions will affect legal, even if they are considering moving services to the cloud that directly impact e-discovery, including e-mail and litigation review platforms. Attorneys need to proactively work with IT and procurement to stay involved with the process and ahead of any problems. No lawyer wants to be wrapping up production for discovery, only to find out that the IT department has been testing a cloud e-mail pilot program. That could mean that the custodians' e-mails that legal swore to the court had been destroyed after 30 days still existed in a CSP's cloud environment.

Through FedRAMP, FISMA and other initiatives, the security model has expanded.

A new framework is being developed, and every agency will need to understand that framework and live within it.

"Procuring IT services in a cloud computing model can help the Federal Government to increase operational efficiencies, resource utilization, and innovation across its IT portfolio, delivering a higher return on our investments to the American taxpayer," FedRAMP states that if attorneys haven't been involved in the process of moving to the cloud, they need to start now. If done correctly, the move to the cloud should ultimately make e-discovery faster, more cost-efficient, and more defensible. But getting to that point will be challenging for everyone involved, and the legal department needs to start meeting those challenges as soon as possible. ⊙

Chris May is a principal with Deloitte Financial Advisory Services LLP.

Endnotes

[1]www-03.ibm.com/press/us/en/pressrelease/33390.wss.[2] Computer Security Div., U.S. Dep't of Commerce, The NIST Definition of Cloud Computing (NIST Special Publication 800-145, 2011), *available at* csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[3]GSA, Info.Apps.Gov, *What Are the Services*, www.infoapps.gov/content/what-are-services.

[4]National Archives, NARA Bulletin 2010-05 Guidance on Managing Records in Cloud Computing Environments (Sept. 8, 2010), *available at* www.archives.gov.

[5]*Id.*

[6]CIO Council, 25 Point Implementation Plan to Reform Federal Information Technology (Dec. 9, 2010), *available at* www.cio.gov/documents/25-point-implementation-plan-to-reform-federal%20it.pdf.

[7]CIO Council, Federal Cloud Computing Strategy (Feb. 2011), *available at* www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf.

[8]U.S. Dep't of Homeland Security, Federal Cloud Computing Strategy (Feb. 8, 2011), *available at* www.dhs.gov/sites/default/.../federal-cloud-computing-strategy.pdf.

[9]*Id.*

[10]*Id.*

[11]CIO Council, Security Authorization of Information Systems in Cloud Computing Environments (FedRAMP) (Dec. 8, 2011), *available at* www.cio.gov/fedrampmemo.pdf.

[12]GSA, Concept of Operations (Feb. 7, 2012), *available at* www.gsa.gov/graphics/staffoffices/FedRAMP_CONOPS.pdf.

[13]CIO Council, Creating Effective Cloud Computing Contracts for the Federal Government: Best Practices for Acquiring IT as a Service (Feb. 24, 2012), *available at* www.cio.gov/cloudbestpractices.pdf.

[14]*Id.*

[15]*Id.*

[16]No. 08-5014, ___ F.3d___, 2009 WL 21528 (D.C. Cir. Jan. 6, 2009).

[17]Model Rules of Prof'l Conduct R. 1.1, 1.6, 1.15, www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/model_rules_of_professional_conduct_table_of_contents.html.