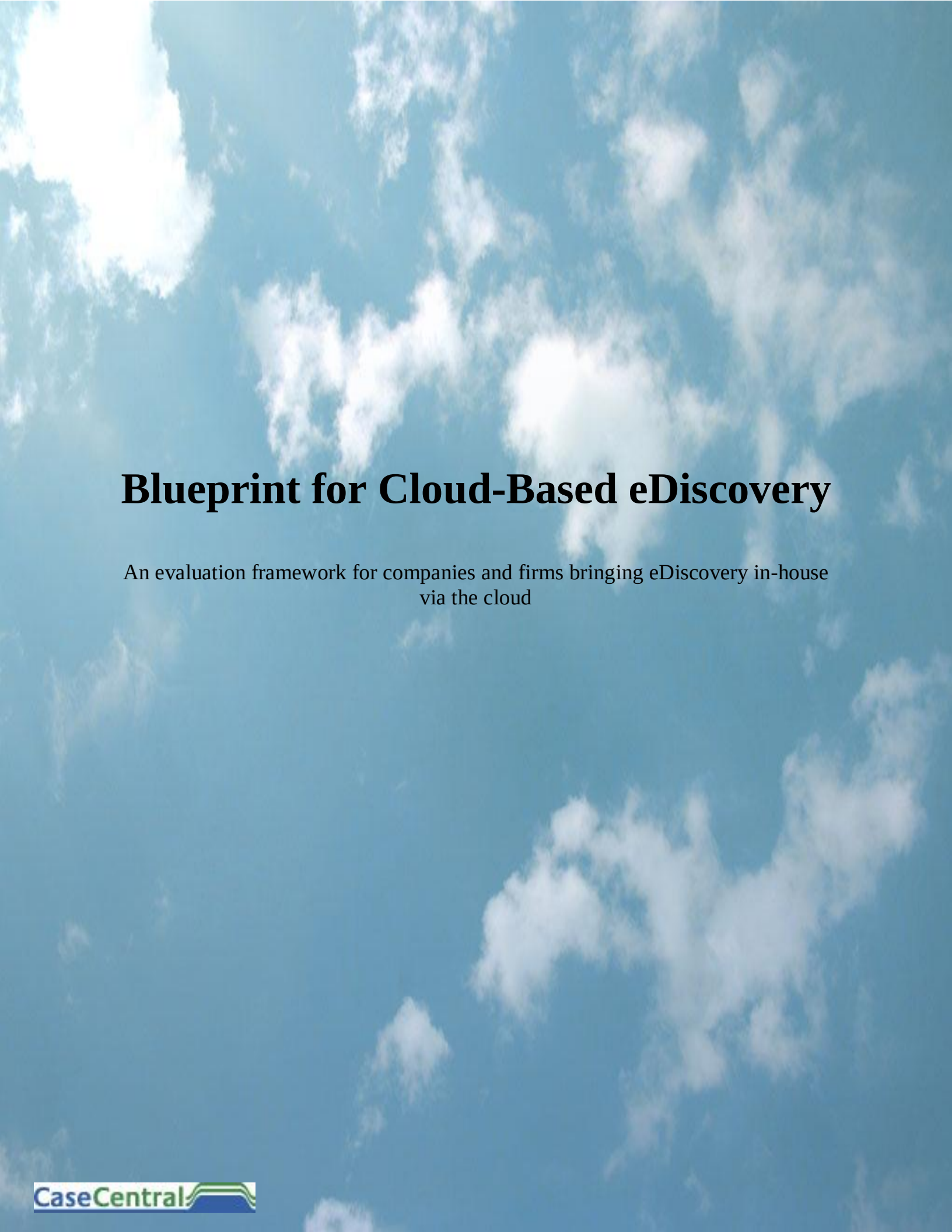


Blueprint for Cloud-Based eDiscovery

An evaluation framework for companies and firms bringing eDiscovery in-house via the cloud

CaseCentral

Blueprint for Cloud-Based eDiscovery

A Framework for Cloud Computing Security, Privacy, Control, Risk and Cost Concerns

Executive Summary

Cloud-based business applications have risen from relative obscurity to mainstream enterprise initiatives. Influential industry analyst Gartner, Inc., says, "Cloud Computing will be as influential as E-business."[1] Corporations and firms have flocked to cloud-based delivery models to reduce economic pressures and provide elastic scale across a wide range of business software. Perhaps most important is the simple notion that the use of cloud computing enables businesses to more completely focus on their core competency, whether that competency is practicing law, manufacturing or retail or finance, rather than on building and supporting IT infrastructure.

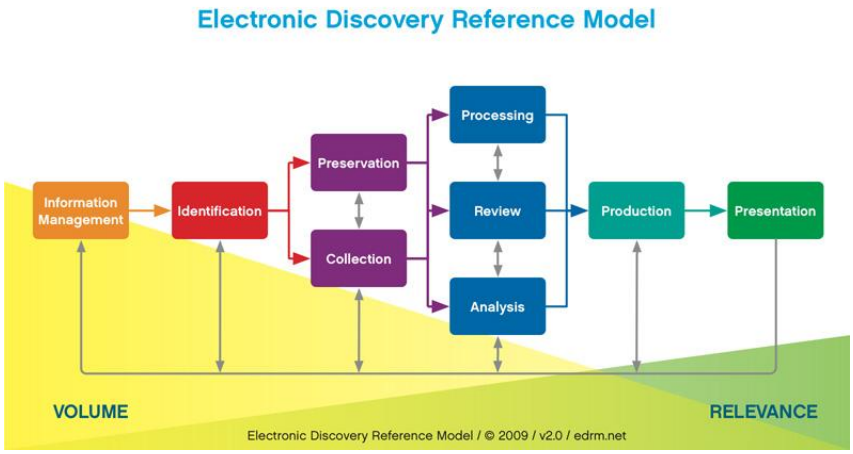
Nowhere has this trend been truer than in eDiscovery, where both corporations and law firms have been scrambling to find better methods of controlling costs and risks. In 2009, more than 84% of Am Law 200 firms and 76% of U.S. companies used at least one cloud-delivered application to lower capital expenditures and reduce dedicated headcount for support, while drastically accelerating application deployment time.

Cloud-computing has long been utilized in some parts of eDiscovery and as the market has evolved is challenging on-premise deployments as a serious contender for eDiscovery and compliance needs. But the prevailing hype and associated noise has made it hard to discern a workable framework for determining if a cloud-based application is the right deployment model and how to choose a cloud-based application for the purpose of eDiscovery.

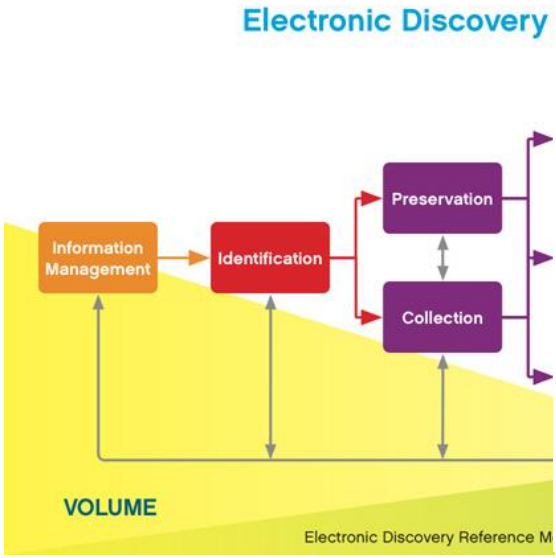
"The Blueprint for Cloud-Based eDiscovery" is in response to that need. This framework surfaces key points and guides decisions in terms of security, privacy, control, risk and cost practices at corporations and law firms looking to bring eDiscovery in-house via the cloud.

Using the Electronic Discovery Reference Model (EDRM) to define cloud-based eDiscovery initiatives

eDiscovery is made up of multiple phases and performing all of these in the cloud may not make sense for everyone. The Electronic Discovery Reference Model, launched in 2005 by independent consultants George Socha and Tom Gelbmann, provides a functional framework which can be used to divide up eDiscovery into more manageable processes and initiatives.



The processes on the "left side" of the EDRM, which include information management, identification, preservation and collection, often make sense to perform with on-premise software since the custodians and the data typically reside inside the company. An exception to this statement can be archiving and preservation, since some corporations choose to implement cloud-based file and email archives. The audience for these applications tends to be internal to the company and largely IT-driven.



Left Side:

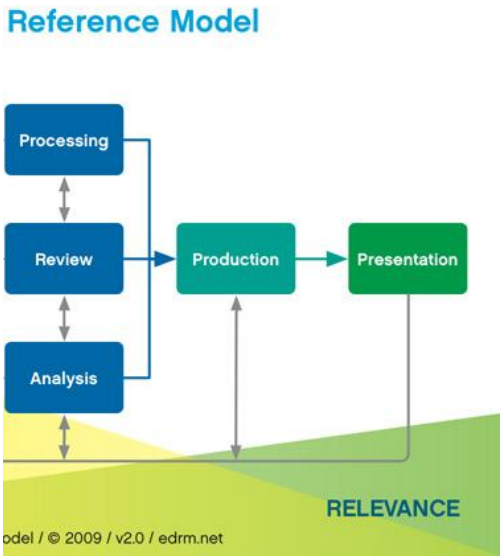
- **Audience**: Internal (IT, Compliance, Legal)
- **Focus:** information management, compliance
- Data resides inside firewall
- Traditionally served by on-premise software

"Application service providers, software-as-a-service delivery models and cloud solutions will dominate the review and analysis phases of e-discovery."[2]

The processes on the "right side" of the EDRM, which include processing, analysis, review, production and presentation, lend themselves to cloud-based software. A key reason for this is that when performing these processes you are usually involving multiple resources in multiple locations both inside and outside of your company and firewall. A collaborative, cloud-based application is the best way to provide a centralized, secure environment for multiple, geographically dispersed parties if you want to store only one copy of your confidential data, if you want to centrally control the eDiscovery business process and if you do not want to petition your IT department to punch holes through your corporate firewall to allow outside parties direct access to your corporate network.

Right Side:

- **Audience:** Internal and External (Legal, outside counsel, vendors)
- **Focus:** risk mitigation, litigation support, collaboration
- Data resides outside firewall
- Traditionally served by hosted or cloud-based software



Key Points:

- ***What phase(s) of eDiscovery is being addressed?***
- ***Is the audience internal or do outside counsel and service providers need access?***
- ***Is the primary focus IT or Legal?***

Bringing eDiscovery in-house: eDiscovery cloud versus on-premise software

When considering a cloud-based eDiscovery application versus an on-premise application, one must consider not only the audience and focus for the application being delivered, but also the hardware, systems, data centers and human capital necessary to deliver the application. For corporations and law firms looking to bring eDiscovery in-house, cloud-based eDiscovery can be very attractive. Cloud-based eDiscovery is often less risky, less costly and more efficient than purchasing, installing and maintaining on-premise software. eDiscovery practitioners control the process, data and access without incurring the costs, risks and time delays[3,4] inherent in on-premise software deployments or the headaches involved lobbying your IT department to modify your corporate firewall and security standards to allow outside parties to access on-premise eDiscovery software. Initial cloud computing application deployment is proven to be much faster and on-going maintenance costs are proven to be much less expensive than on-premise software deployments.[3,4] Additionally, cloud-based eDiscovery software can provide highly predictable costs that eliminate the expense spikes typically associated with on-premise software, hardware, and human capital.

There has been a lot of misinformation equating "bringing eDiscovery in-house" with the purchase, installation and on-going management of on-premise software for various eDiscovery tasks. The true nature of bringing eDiscovery in-house is that corporate legal teams and their executives are trending toward retaining control of eDiscovery decision-making, creating and owning the overall eDiscovery process and acting as collaborative partners throughout the life cycle of a particular matter. The delivery model for eDiscovery software and services, cloud-based or on-premise, is not directly related to the notion of "bringing eDiscovery in-house."

According to Forrester Research, Inc.[3] the benefits of cloud-based applications include:

Dimension	Software-as-a-service helps by . . .
Reduced cost of adoption	Reducing the licensing, training, and support costs of adding additional users.
Quicker adoption	Decreasing the time to ramp up new users, maximizing their productivity from using the application.
Improved adoption	Enabling more users to use the application.
On-premise cost avoidance	Eliminating maintenance costs. • Reducing full-time help desk and server support, and transferring staff to higher value, proactive roles.
Improved flexibility	Reducing spend on excess capacity.

"The biggest financial benefit of cloud computing, particularly in these capital-constrained times, is avoiding taking on debt and keeping cash in the company longer. If a project uses a cloud-based service provider, then the CFO avoids writing a big check upfront."[4]

Key Points:

- ***Do you want to control your eDiscovery processes and implement them in a repeatable and measurable way?***
- ***Does your budget consider the difference between capital expense (Cap Ex) versus operating expense (Op Ex)?***
- ***Do you have many outside parties (outside counsel, contract reviewers, service providers) who need to access case data?***
- ***How quickly do users (outside counsel, expert witnesses, vendors, etc.) need to be able to use the system?***

Public Clouds and Private Clouds: Why public clouds are wrong for eDiscovery

The difference between public and private clouds is very important for those performing eDiscovery. A public cloud uses shared hardware, software and applications that are available to the public. Examples include Amazon EC2, AWS and Google Apps. This approach is very effective when used for consumer-based applications or business applications that do not have the same security and access control requirements or the level of legal and regulatory scrutiny that eDiscovery data has. A private cloud, whether deployed by a company behind the firewall (aka 'internal cloud') or deployed by a provider, uses hardware, software and applications only for subscribing users.

Private clouds have specific advantages over public clouds when it comes to eDiscovery: With a public cloud you don't know where (including what country, state or server) the files are stored, and don't know if you can really control document retention and destruction. And you may not be receiving the level of disaster recovery and business continuity that you require. Clients need to know that they are completely in control of their data, and a private, trusted cloud is the only way to do that.

As recently cited in the *Electronic Commerce & Law Report*, a non-private cloud pools resources to serve multiple clients, which "implies both an increased risk of inadvertent access to data by others in the cloud and an inability to pinpoint with any specificity where data resides at a given moment."

> "The inability to know where one's data is located, of if and when the data may be moved to another state or country, implies a good deal of potential legal risk."[5]

With private clouds, subscribers understand where their data resides, so their information aligns with proper jurisdiction, security and applicable document retention.

Key Points:

- ***Who owns the infrastructure (including disk drives) and where is it located?***
- ***How is access to the infrastructure controlled?***
- ***Can document retention and data destruction be certified?***

What Disaster Recovery and Business Continuity capabilities does your provider have?

System crashes or natural disasters can impact not only cloud computing providers, but also any corporate enterprise or law firm. Many will remember the much-publicized news in October, 2009 when Microsoft lost data for mobile Sidekick phone users. This disaster affected mighty Microsoft and the reason was that there was no disaster recovery or backup plan.

Not all cloud computing providers are created equal. Clients expect their data to be secure and available and the way to do that is to provide enterprise-class disaster recovery (DR) capabilities, business continuity planning (BCP) protocols and client service-level agreements (SLAs).

To provide maximum benefit, ensure that your provider offers enterprise-class disaster recovery (DR), with a SAS-70 Type II certified and replicated datacenter in the event a service gap or power outage occurs.

Providers should also offer Business Continuity Planning (BCP) protocols to ensure that core business processes are preserved and service to clients is maintained, avoiding a "Ghost Ship" scenario where systems may be up but core business processes fail.

Each service provider should clearly outline their Service Level Agreements (SLAs), including Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO). These policies define the maximum outages contractually allowed and ensure that users are in control of that data stored in the cloud.

Some providers offer better disaster recovery, business continuity planning, SLAs, RPOs and RTOs than those of internal corporate or law firm IT departments.

Key Points:

- ***Does the provider have enterprise-class disaster recovery facilities?***
- ***Does the provider maintain defined Business Continuity Protocols?***
- ***Does the provider offer system SLAs? How well have they historically been met?***

What Security and Compliance Certifications does the provider offer?

Security, privacy and control should be the concern of every attorney and litigation support person whether they are using a cloud computing-based application or an on-premise application. However, the notion of security is many-fold and must include data security, physical security and network security.

201.CMR.17, the Massachusetts data protection law, went into effect March 1, 2010. It requires the selection and retention of a third-party service provider who is capable of properly safeguarding personal information. The third party service provider provision in 201 CMR 17.00 is modeled after the third party vendor provision in the FTC's Safeguards Rule. 201.CMR.17 requires each and every service provider to have and provide a written information security program and to encrypt data in transit. Other states are writing, planning to adopt or have already adopted similar legislation.

While you may think of telemarketers in the previous example, you should think about the way that you handle your proprietary and confidential data today and how you send it to service providers, including outside counsel. Today's typical process involves issuing a legal hold and collecting relevant data in electronic, paper or other format. At this point the vast majority of corporations put this collected data on a CD, DVD, hard drive or USB drive and ship it to a vendor, outside counsel or the outside counsel's vendor. And, if the matter is multi-jurisdictional or involves multiple outside counsel, the data is copied many times and shipped to the many recipients who have varying levels of technological sophistication, security and compliance controls. At this point the proprietary and confidential data has been copied potentially many times and has left the confines of the corporation without *any* security or privacy controls.

The ideal solution is a private cloud computing-based eDiscovery software platform that stores only a single copy of a document despite the fact that it may be used in multiple cases with different workflows and designations in each. With such a platform, the data can be centrally managed, controlled and secured regardless of the number of firms or users who need access. And the corporation can audit security once, thereby ensuring compliance to privacy requirements, as opposed to having to audit any number of outside counsel and vendors who receive the data.

Key Points:

- ***Do provider data centers have SAS-70, Type II Certification?***
- ***Does the provider offer International Safe Harbor Certification?***
- ***Do the provider's security management techniques follow ISO 27002 or ISO 27001?***
- ***Can the provider certify where the data is stored and where the servers are?***
- ***Can the provider certify data destruction?***

Does the system offer multi-matter,multi-party and business intelligence capabilities?

While the notion of multi-party and multi-matter support may seem extraneous to that of cloud-based eDiscovery, it is not. In today's world, the vast majority of the applications used for eDiscovery, whether on-premise or cloud-based, only support a single case. When you create another case, another database is created and another copy of your data is created. Duplicate effort occurs across all phases of eDiscovery with such applications. Data is collected multiple times, stored multiple times and reviewed multiple times. This simple reality has many implications, not the least of which are information security, data retention and destruction and cost increases.

The ideal scenario is to use a provider that supports multi-matter, multi-party eDiscovery. Such providers can eliminate duplicate data collections, de-duplicate across cases, and provide single-instance storage so each file only exists once, regardless of the number of matters in which it is included. This design also allows fewer inside resources to manage more service providers with better control. Standards such as chain of custody and production authorization are applied universally. And work product from one case can be re-used in another.

Centralizing cases, documents and parties in a single database of content provides the foundation that is needed to deliver business intelligence that was not previously possible on eDiscovery activities, thereby allowing counsel to control, measure, and monitor matters more efficiently.

The benefits of this are that it enables quantitative eDiscovery process measurement for: budget forecasting; resource governance; risk and cost oversight; managing matter timelines; and production deadlines. Clients can do this on a single matter or, more importantly, across all cases and matters.

Key Points:

- ***Does the system support multiple matters and multiple parties?***
- ***Can the system replicate standards across all cases?***
- ***Is data stored only one-time, regardless of the number of cases involved?***
- ***Can work-product be shared across matters?***
- ***Does the system provide process cost and efficiency metrics across cases and firms for forecasting?***

Footnotes:

[1]"Cloud Computing Confusion Leads to Opportunity," by Gartner, Inc., Daryl C. Plummer, David W. Cearley, David Mitchell Smith, June 19, 2008

[2] "Predicts 2010: Regulatory Changes and Business Demands Will Drive the Long-Delayed Adoption of Legal Discovery Technology," by Gartner, Inc., John Bace, Debra Logan, Whit Andrews, November 17, 2009

[3] "The ROI of Software-as-a-Service," by Forrester Research, Inc., Liz Herbert and Jon Erickson, July 13, 2009

[4] "Talking To Your CFO About Cloud Computing," by Forrester Research, October 29, 2008

[5] Sotto, Lisa J., Bridget C. Treacy, and Melinda L. McLellan. "Privacy and Data Security Risks in Cloud Computing," Electronic Commerce & Law Report, February 3, 2010

CaseCentral is a proud member of the Cloud Security Alliance.