

*Contributor*  
David Gaffaney

## Cloud Computing: What you need to know from your vendor to keep data safe

One of the most comprehensive shifts in information technology over the past decade is the emergence of cloud computing as a strategy for IT systems management. Cloud computing is very broadly defined as location independent, ubiquitous computing and storage on demand. Cloud computing can take the form of pure infrastructure (infrastructure as a service, or IaaS), a computing platform (platform as a service, or PaaS), or a fully supported application (software as a service, or SaaS).

While cloud computing can have many cost consolidation benefits, that is not the focus of this article. Instead, we will explore the concept of data stewardship and the related risks and challenges of which organizations must be aware.

When a commitment is made to a cloud computing model, you are putting your company's mission-critical data and intellectual property in the hands of a third party. Executive leadership will call upon legal or risk management teams to help them better understand the risks and considerations associated with this practice and how the organization may be protected from legal, operational, and compliance perspectives. We will discuss these risks from multiple viewpoints: daily operations and incidents, records management, and e-discovery.

### DAILY OPERATIONS AND INCIDENTS

One of the primary requirements when moving to a cloud model is being able to support day-to-day business operations in a seamless manner. This calls for high-level availability of the applications and data that are being managed, according to a negotiated service legal agreement. From a compliance and risk management perspective, the key attributes to consider when migrating to a cloud environment are data security, location, and transmission.

A shift to a cloud computing model forces organizations to confront new issues in data security as well as familiar issues that have been around for decades. When considering a move to cloud computing, your organization should ask:

- What level of cloud (IaaS, PaaS, or SaaS) best fits your current and future operational structure?
- How do the outsourced components align with your security methods and technology, and can they be synchronized?
- Do you work with or have offices in the EU? If so, you will have data residency rules specific to the country your information must reside in.
- For the United States, does your vendor understand the different state rules for privacy breaches?
- Is your cloud vendor's backup and archive strategy in alignment with yours? Can it be verified?
- Does your vendor fully understand your records management needs, and is it willing to be audited to verify your disposition rules are being followed?
- Can your vendor support identification, collection, preservation and other key aspects of e-discovery, including legal holds? Can they demonstrate their processes for you?

From a security standpoint, it is important to consider the security and authentication architecture being offered by the service provider to ensure that the provider's architecture can be synchronized with your own internal security model. In most cases, organizations are not outsourcing all IT systems to the cloud, but rather a small subset of those systems, such as email or document management. Email is easier to control because there is typically a specific named account per user. However, content management systems or shared drives can be more difficult to synchronize, as access may be given at group or department levels. Maintaining alignment with on-site systems as well as synchronization with your on/off-boarding process will be important. Documenting the specifics of this synchronization is essential for showing process predictability and compliance, something that is also valuable for e-discovery.

The location of data is the most complex aspect of the cloud computing model, especially when international data is included. Data privacy laws and regulations are complex. Data related to citizens of one country may not be stored in another or may require specific conditions to be met before leaving its country of origin. Therefore, it is important to understand where your data will physically reside in a cloud environment and any implications of the geography on the regulatory or legal requirements to which it is subject.

Basic data management and operation should be the easiest part of the equation in the cloud relationship. Where your risk management and compliance framework will be tested is with incident response: the anomalies that expose your organization to the highest risk. For example, there are likely to be reporting and actions required for security breaches applicable to U.S.-based data. Forty-six states have their own unique variation on what is considered private information, how it must be managed and protected (including commentary on encryption), and what actions must be taken when there is a breach. While there may be no residency of data requirement for U.S. states, several have rules about the disposal of certain personal information and its treatment as records. The key point to keep in mind is to make certain you know the rules about your own data and that your cloud provider has the capabilities to deal with these nuances.

A second critical aspect of daily operations relates to the backup and archival of information. A cloud vendor will have a backup schedule and disaster recovery plan for any data it is hosting. The consideration for you, as the owner of that data, is to understand the concepts of archive versus backup and apply them accordingly. For an infrastructure or platform cloud model, the primary activity will be a cycle of rotating backups. For a software as a service deployment, you will need to be more concerned about the targeted archival of information, which is application specific. Whether the methods for archival are governed by you or the cloud vendor it



will be important to understand the parameters and the eventual resting place for the backed-up and archived data. For better control or management, this material should be managed in a separate, dedicated manner and not commingled (e.g. on a shared media, such as disk array) with data from other clients of the cloud vendor. Additionally, because IT staff are often called to testify as 30(b)(6) witnesses as to the specific procedures for backups and recycling of tapes, making sure you know where this responsibility lies in the vendor relationship is crucial.

Finally, it is critical to have an exit strategy with your cloud vendor. For large organizations, you may be discussing scale in tens or hundreds of terabytes. Negotiate the termination provisions with your vendor. This includes items such as (1) causes for termination (e.g. convenience vs. breach), (2) lead time required for notifying the vendor of the desire to terminate the relationship, and importantly, (3) the method to be used by the vendor to return your data to ensure a smooth and secure transition.

#### **RECORDS MANAGEMENT**

A good records management program requires the controls described above plus adherence to a retention schedule. This is not an issue unique to cloud computing; good records management has been a challenge for decades. However, verifying that your provider is actually deleting and digitally shredding when required by a retention schedule is increasingly important, given the massive volumes of electronic information under management. There have been numerous incidents where hosted data that should have been destroyed was not, leading to additional costs and potential legal exposure. It is critical to set up an audit process to validate not only the contractual arrangement but also the vendor's processes for disposition of information.

The level of these audits will depend upon what kind of arrangement you have with your cloud vendors. If you are in a SaaS relationship, then some responsibility may fall under the control of the provider. For IaaS/PaaS arrangements, your organization is typically in charge and executing controls at an application level. Therefore, your IT experts may be the ones setting these parameters.

### **E-DISCOVERY**

All of the previously mentioned considerations lead to discussions of e-discovery practices and how those practices are handled by cloud computing providers. A cloud computing provider is involved in the information management stage of the discovery process. However, controls and processes that are set upfront affect the stages that follow, including identification, preservation, and collection.

During identification, a primary consideration is having access to appropriate search tools that will allow you to locate information in cloud storage based on your desired criteria, such as keywords or topics. It will be important to understand the cloud provider's capabilities in this area before moving to a hosted model. Will these tools be available from the provider, and at what cost? There may be basic search available at no cost, with additional charges for using a more robust tool like Autonomy or Google Enterprise Search. If you have such tools already licensed, can you use them on cloud-based data sets? Are there custom data types that require additional capabilities (e.g. searching into image text with OCR)? Logically, your search tools should be able to work in coordination with your cloud computing model; however it is important to understand the capabilities and limitations in advance of a discovery request so that you're not hunting for answers later.

During preservation and collection, it is important to understand the provider's legal hold capabilities. You may have well-trained staff who understand their obligations from functional and business perspectives, but do these employees (and your IT staff) have the ability to lock down content in place and manage complexities such as multiple overlapping holds? Your legal hold capabilities must also complement your records management technology, making sure that disposition schedules do not override legal holds. It is critical that your cloud environment supports this interaction, or, at the very least, does not interfere with it. If this is not the case, then this may be the point in the lifecycle where you bring the collection set into a fully-controlled repository.

A second consideration during the preservation and collection stages of discovery is the security concept of delegated authority. Many organizations will have a third party perform collections and review. In these cases, you may need to give access to the third party from a geographically separate location. Such capability should be part of the "access anywhere" definition of cloud computing, but the administration is not always straightforward.

### **CONCLUSION**

In summary, cloud computing brings together, under a single umbrella, a number of technology strategies that have been in place for some time. The evolution is in the flexibility of location-independent access and the freedom to extend your virtual data center at will (within the bounds of the contract). With this flexibility comes power, but also risk and questions of control and responsibility. Review the risks and considerations discussed in this article when talking to cloud vendors to be aware of how your information and applications are or will be managed, accessed and controlled.

Experience. **Redefined.**<sup>®</sup>

1-866-229-8700  
www.huronconsultinggroup.com

**Huron**  
CONSULTING GROUP

Huron Consulting Group helps clients in diverse industries improve performance, comply with complex regulations, resolve disputes, recover from distress, leverage technology, and stimulate growth. The Company teams with its clients to deliver sustainable and measurable results. Huron provides services to a wide variety of both financially sound and distressed organizations, including leading academic institutions, healthcare organizations, Fortune 500 companies, medium-sized businesses, and the law firms that represent these various organizations. Learn more at [www.huronconsultinggroup.com](http://www.huronconsultinggroup.com).

© 2010 Huron Consulting Group Inc. All Rights Reserved. Huron is a management consulting firm and not a CPA firm, and does not provide attest services, audits, or other engagements in accordance with the AICPA's Statements on Auditing Standards.