

SECURITY



Legal Considerations in Migrating to the Cloud

BY H. WARD CLASSEN AND WALTER S. DELACRUZ

Clients are increasingly asking law firms and corporate legal departments to review cloud computing service agreements, which service providers often propose following an RFP process. This may be a cost-cutting initiative. By migrating to the cloud, businesses can reduce information technology related expenses and often secure a wider array of services and improved service levels.¹ The move to a cloud services provider, however, should only be undertaken after the company has reviewed the data and processes it seeks to outsource to the cloud, and the controls it desires to maintain over those data and processes.

What is cloud computing?

Cloud computing allows a company to outsource its IT infrastructure and move to a subscription model to receive software and information technology related services. The National Institute of Standards and Technology has defined cloud computing as “a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned with minimal management effort or services provider interaction.”

Under this model, a customer’s software and data are located on the vendor’s servers and other infrastructure, and the customer accesses it over the public internet via a web browser. A customer often experiences immediate advantages including:

- improved server deployment time² (the time to go through a click-through agreement);
- a financially flexible pay-as-you-go utility model to use critical technology infrastructure and software;³ and
- the ability to quickly increase the scale of the customer’s information technology infrastructure.

Definition

Most definitions of cloud computing, including that of the National Institute of Standards and Technology (NIST),⁴ describe cloud computing’s critical characteristics as including:

- self service by a customer;
- on-demand access (allowing a business, for example, to sign up for email services for a certain number of employees during one week and then for additional numbers of employees at later time periods, all on a pay-as-you-go basis);
- broad access to the provider’s services via any number of customer devices (including handheld devices, desktop PC, laptop, tablet); and
- resource pooling, allowing “spikes” in any individual business’s usage to be covered by the overall capacity of the system.

Service models

Cloud-based service offerings are generally considered to fall into one of three areas: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). These classifications are general marketing concepts, however, so a business contemplating a migration to a cloud environment must carefully review



H. WARD CLASSEN is deputy general counsel for Computer Sciences Corporation (CSC), and the author of *A Practical Guide to Software Licensing for Licensees and Licensors* (ABA Press). Classen can be contacted at hclassen@csc.com.



WALTER S. DELACRUZ is of counsel in Moses & Singer LLP’s Intellectual Property and Global Outsourcing and Procurement practices. He has extensive experience in IP counseling, and transactions in the telecommunications and financial services industries. Delacruz can be contacted at wdelacruz@mosessinger.com.

the service descriptions to ensure the business receives the services it desires.

SaaS is the most common service model, providing fully functional software applications through the web. The user is accessing third-party software on another party’s infrastructure. The software is updated and the data backed up by the third party. Examples of SaaS offerings include *Salesforce.com*’s Customer Relationship Management tools, Facebook and Google’s Gmail.

PaaS provides application-virtual hardware and middleware systems, allowing customers to build their own software applications. Customers can utilize as many virtual machines as they need, creating increased flexibility and rapid elasticity. Examples of PaaS offerings include Microsoft’s Azure platform and Rackspace Cloud’s Cloud Sites platform.

IaaS provides a complete virtual platform (servers, storage space, network devices, etc.) for a customer to undertake all of its computing activities using its own applications and operating systems. Customers have the ability to provision and configure the vendor’s virtual machines. Examples of IaaS include Amazon’s Elastic Compute Cloud and Rackspace’s Cloud Servers service offerings.

Delivery models

There are four standard delivery models for cloud computing: a private cloud, a public cloud, a hybrid cloud and a community cloud.

Private cloud. A private cloud is dedicated to a single user, with dedicated physical infrastructure and dedicated staff. A private cloud is most appropriate for heavily regulated industries, including financial services and health-related services, where financial, personally identifiable, or other private or sensitive data is handled and/or stored by the customer.

Public cloud. A public cloud has many users, without an infrastructure dedicated to any particular user. Public clouds are the most common form of cloud computing and are what most people think of when they think of cloud computing.

Hybrid cloud. A hybrid cloud consists of two or more clouds bound together by standardized or proprietary technology that allows data and application portability. As an example, a company using a hybrid cloud can move usage from their private cloud to the other cloud in the event of capacity spikes, or for backup or other purposes.

Community cloud. Community clouds are developed to address the needs of certain industries, with technical specifications tailored to meet regulatory or other business requirements. An example of a community cloud is the Capital Markets Community Platform, launched on July 1, 2011, by NYSE Technologies. This platform provides cloud computing services to broker dealers, institutional investors and hedge funds with latency sensitive operations requirements.⁵

The identification of processes and data appropriate for cloud computing

At the outset, a company contemplating a move to the cloud needs to have a good understanding of the data it collects, and understand the different kinds of processes that are applied, or will be applied, against that data. The company would also need to assess the sensitivity of the data, including its proprietary or confidential nature, and determine whether the data includes personally identifiable information. The processing of certain kinds of data (e.g., financial or consumer credit data, or health-related data) is subject to regulatory oversight including federal and state law.

Also, as part of the analysis, the company needs to map its data flows, from generation or collection, to processing and storage. In the event that processing protocols move data between different legal jurisdictions, more than one state's privacy and data protection law will attach. The company will need to be aware of the corresponding legal requirements and potential cost implications.

After the company has completed a data census, mapped its data flow, and determined the sensitivity of its data and processes — including determining (if applicable) the regulatory requirements corresponding to personally identifiable information and other confidential and proprietary information — it will be better able to assess the offerings among cloud providers. The company may also determine that mission-critical processes, or proprietary or confidential information, may not be appropriate for migration to anything other than a private cloud.

Legal and regulatory implications of cloud computing in the United States and Europe

United States

In considering a migration to the cloud, companies need to be mindful of the specific regulatory requirements covering their industry. For example, in the United States, financial services companies need to comply with Gramm-Leach-Bliley,⁶ which holds companies responsible for developing, implementing and maintaining a comprehensive information security program to protect nonpublic customer information. For financial services companies with broker dealer operations, FINRA's proposed Rule 3190⁷ may limit the use of

A public cloud has many users, without an infrastructure dedicated to any particular user.

cloud computing in this activity because of the limits on outsourcing placed on broker dealer operations. The proposed FINRA rule clarifies obligations and supervisory responsibilities regarding outsourcing arrangements, and imposes additional requirements, including establishing and maintaining a supervisory system and written procedures for any functions performed by a services provider that are reasonably designed to comply with applicable requirements. The Rule makes clear that a firm's delegation of a function or activity related to a firm's business as a regulated broker dealer to a third party (including a corporate affiliate) does not relieve the firm of the ultimate responsibility for compliance with applicable securities laws and regulations, and FINRA and Municipal Securities Rulemaking Board (MSRB) rules. In addition, a firm may not delegate its responsibilities for, or control over, any outsourced functions or activities.

Companies that process or store non-financial personally identifiable information or other sensitive data, including health services-related information, or that provide services accessed or used by minors under the age of 13, need to comply with the federal law treating such information.⁸ Other federal laws that apply to the storage or processing of information, and the accessing of such data by government or law enforcement authorities, are the Electronic Communications Privacy Act and the United States Patriot Act.⁹ The array of applicable federal laws that attach depends upon the kinds of data processed and compels well-advised companies to understand their data flows. Companies need to be clear about what data they are capturing, what processes are being applied against such data, and where the data are being transported for processing or storage.

In addition to the federal rules, 46 states plus Puerto Rico, the Virgin Islands and the District of Columbia have laws that attach in connection with data governance, breach notification, and stored and moving data encryption requirements.¹⁰

Europe

In Europe, rules regarding the use of cloud computing are similarly layered. The EU Data Protection Directive (Directive 95/46/EC) provides that transfers of personal data originating in any one of the 27 member states of the

Things Can Go Wrong

Companies contemplating a migration to a cloud or data center virtualization services provider would do well to consider the move carefully. An example of where things can go very wrong, even for large, sophisticated customers and large, sophisticated services providers, is presented by the case of the Texas Department of Information Resources (DIR) and IBM Corporation. On March 31, 2006, the Texas DIR issued a Request for Offer (RFO) to outsource the consolidation of 27 separate state agency data centers, into two.

IBM was the successful bidder, and on Nov. 22, 2006, the parties entered into a seven-year agreement for IBM to complete the project within 24 months. The contract was worth \$863 million. Problems consolidating the data centers developed, with charges by the Texas DIR that IBM was not investing sufficient resources into the project,¹ and by IBM that the Texas DIR was not doing enough to improve its commitment to improve the governance of the project, and to compel state agencies to move control of their IT environments to a centralized, common system.²

On July 16, 2010, the Texas DIR issued a Thirty Day Notice to Cure Breaches³, and then, a second letter on Aug. 16, 2010, providing notice to IBM of DIR's intent to terminate the agreement for cause. At the time of the first DIR letter, the project was considered to be only 12 percent completed, with only five state agencies having been migrated, and with no schedules in place to migrate the remaining 22 agencies. In the second DIR letter to IBM, DIR further indicated that it would rebid the contract.⁴ During the months following the notice letters, the parties failed to reach agreement regarding remedies. In November 2010, the Texas DIR published a call for new bids from other suppliers to finish the data center consolidation project. The new procurement process

will be done as two separate projects, one for infrastructure support and one for services.⁵

The Texas DIR/IBM experience underscores the need for careful planning regarding the migration of data and information management services to a services provider. Key factors for a successful migration include understanding the scope of the project, and confirming that there is agreement regarding basic assumptions and each party's obligations under the agreement. In addition, the data, its sensitivity (whether it is personally identifiable information or proprietary information) and data flows need to be understood by the parties in order to plan for its appropriate treatment under the agreement.

ENDNOTES

- 1 Letter from Karen Robinson, executive director, Texas Department of Information Resources, to Cynthia McLean, vice president and global project executive (July 16, 2010), available online at <http://alt.coxnewsweb.com/stateman/pdf/08/0818ibmletter.pdf>.
- 2 Lee, Justin, "IBM Blames Texas' DIR in Data Center Contract Dispute." *Webhostindustryreview.com*, posted on Aug. 23, 2010, accessed on Aug. 30, 2011, available online at http://thewhir.com/web-hosting-news/082310-IBM_Blames_Texas_DIR_in_Data_Center_Contract_Dispute.
- 3 Karen Robinson Letter of July 16, 2010.
- 4 Towns, Steve, "Texas Warns IBM of Outsourcing Contract Failures," *Governmenttechnology.com*. Posted on July 16, 2010, accessed on Aug. 30, 2011, available online at www.govtech.com/pcio/Texas-Warns-IBM-of-Outsourcing-Contract.html.
- 5 Pariseau, Beth and Carl Brooks, "Texas rebids IBM data center consolidation project," *Searchdatacenter.com*. Posted on Jan. 31, 2011, accessed on Aug. 30, 2011, available online at <http://searchdatacenter.techtarget.com/news/2240031466/Texas-rebids-IBM-data-center-consolidation-project>.

European Union¹¹ may be made only to member states and to jurisdictions that have been determined by the European Union to have adequate data security standards.¹² The United States is not among those states deemed to have adequate data security standards. To meet the EU adequacy test, US companies moving personal information and data from Europe to the United States can do so lawfully by:

1. the Safe Harbor provision,¹³
2. Model Contractual Clauses,¹⁴ and
3. Binding Corporate Rules.¹⁵

Because of the strong privacy rights reserved to European citizens under European privacy laws, there may be a general presumption against the legitimacy of cloud comput-

ing in Europe. On June 18, 2010, it was reported that the Data Protection Authority of Schleswig-Holstein, one of the 16 German states, issued a legal opinion that clouds located outside of the European Union that are used in connection with a European data subject are unlawful per se, even if the EU Commission had issued an adequacy determination in favor of the foreign country in question, or if the company moving the data had self-certified to the Department of Commerce's Safe Harbor framework.¹⁶ Under this ruling, for example, it would be illegal for a European company to use a Canadian cloud services provider, or Amazon Web Services (AWS) (which has certified that it complies with the US Safe Harbor data security requirements) to process, transport or store data belonging to a European data subject.

An opening for legal use of the cloud in Europe is provided by the European Commission's Public Consultation on Cloud Computing for the purpose of determining a road map for use of cloud computing in Europe.¹⁷ The EU Digital Agenda Commissioner initiated a public request for comment period seeking discussion from users and developers regarding cross-border data protection and liability, standards and operability, uptake of cloud services, and ways to promote research and innovation. The comment period closed on Aug. 31, 2011, and the Commission's strategy on cloud computing will be released in 2012.

Significant issues in negotiating cloud computing agreements

Cloud services were originally considered to be commodities, resulting in the use of non-negotiable form agreements by vendors. As cloud services have matured and increased in complexity, customers are able to negotiate their agreements instead of being forced to accept the vendor's standard terms. The use of negotiated contracts rather than click-through agreements is changing the nature of cloud computing.

Because a company may be migrating mission-critical functions or data to the cloud, success will require management's commitment to a strategic plan and the adoption of a process to ensure the selection of an optimally qualified services provider. It will also be necessary to negotiate a sound agreement with the selected services provider, and to ensure the ongoing oversight and management of the services provider. Set forth below is a brief discussion of some of the important contractual issues, as well as potential resolutions to the parties' competing interests.

Contract term

Companies and their counsel should carefully consider the optimal length of the term of the agreement, especially because technology can change very rapidly, and there may be concern about locking into an agreement for too long a time with the services provider. The counter-balancing point is that the services provider does not want to commit to too short a time, especially if there is a long investment in learning and the provider doesn't reap the benefits until later in the contract. A mechanism for periodic benchmarking and adjustment may be appropriate.

Availability

Availability is also extremely important to the customer as network outage seriously impacts a corporation's operations. "Availability" should be carefully defined and negotiated. The failure to do so may leave the customer with little recourse in the event of an outage. Similarly, the parties should carefully define "force majeure" to prevent the vendor from claiming all outages were because of an event of force

majeure. A prudent customer should tie availability to the agreement's service levels, which will financially incentivize the vendor to meet its obligations. Network outages can occur in any organization, as illustrated by recent outages at Amazon, Microsoft's Hotmail, Skype and Google's Gmail.

Outages reported earlier this year underscore the risks presented to businesses that want to move to cloud computing. When AWS experienced an outage in April 2011, hundreds of its business customers were unable to conduct business for four days. The affected companies included Twitter, Hootsuite, Reddit, Quora and Foursquare, but also many smaller, lesser known ecommerce companies that conduct their businesses only over the Internet, and would not have been able to get started or operate their businesses without AWS. Other major outages include Microsoft's Hotmail outage in December 2010, which temporarily deleted user inboxes for more than 17,000 users, and the March 2011 outage in which 150,000 Google Gmail users had their mailboxes erased.¹⁸

Data security and confidentiality

From the customer's perspective, data security is paramount. Failure to protect the customer's data and its client data can have far-reaching consequences. In addition to the financial consequences, the customer faces significant reputational risk. Customers who have experienced breach of data security are likely to be less attractive to potential clients than their competitors.

A prudent customer should thoroughly understand how its data will be protected. It should scrutinize the vendor's security standards, practices and procedures. These practices and procedures should be subject to periodic audit by the customer. In addition, to further ensure that the vendor has robust data security practices, the cloud services provider should be contractually obligated to provide the customer with an SSAE/16 certification on an annual basis. The SSAE/16 process was designed by the Auditing Standards Board of the American Institute of Certified Public Accountants to assist companies that have outsourced functions and activities to third-party service providers. Such companies would engage a CPA organization to audit the services provider's systems to determine whether they are adequately described by its management as of the specific date, and whether the controls related to the control objectives stated in the management description were suitably designed to achieve those control objectives as of the specified date.

In addition, the services provider should indemnify the customer for all losses suffered in the event of a data breach. This indemnification should be carved out from any limitation of liability contained on the underlying agreement.

Hacking does not usually result in a breach of the service provider's confidentiality obligations. As such,

Public Sector Entities See Increase in Cloud Computing

Public sector entities are driven by the same incentives as private companies to cloud computing. The US federal government's "Cloud First Strategy" directs federal agencies to look first to cloud solutions to meet IT infrastructure needs.¹ A driver of the federal government's initiative is to reduce the number of federal data centers by 39 percent by 2015.² The strategy document has estimated that up to \$20 billion of the US federal government's annual \$80 billion IT budget should be directed to cloud computing solutions.³ One of the first federal agencies to adopt a cloud solution is the General Services Administration (GSA), which on July 27, 2011, completed a move of more than 17,000 employees and contractors to the Google Apps for Government platform.⁴ The GSA estimates that email operation costs will be reduced by 50 percent over the next five years, and savings will be \$15.2 million, attributable to the decreased use of data centers requiring hardware, software licenses, maintenance and contractor support.

State and local governments are also turning to cloud providers for projected cost savings and improved provisioning of services to consumers. City government agencies in Andover, Minnesota; Boulder, Colorado; Carlsbad, California; Chicago, Illinois; Miami, Florida; New Hanover County, North Carolina; New York, New York; Plano, Texas; and Virginia Beach, Virginia have signed up for a Microsoft cloud services solution.⁵

In New York City, in connection with the deal announced on Oct. 20, 2010, New York City government projected that it would save \$50 million over a five-year period by migrating 100,000 New York City government workers to the messaging and collaboration applications of Microsoft's Business Productivity Online Suite (BPOS). The move consolidates more than 40 separate city agency license agreements into a single one.⁶ For the New York City transaction, the parties anticipated that the application services would be upgraded and superseded by Microsoft's Office 365.⁷ In early 2010, Microsoft had announced that it already had 40 million paying users of its various online services, including 500 governmental entities.

In San Francisco, the city and county government announced on May 18, 2011, that it was moving from multiple email systems to Microsoft's cloud-based offering.⁸ Email services for more than 23,000 employees across 60 departments and agencies will be provided. The service will cost \$1.2 million per year and help the city achieve a mandated 20 percent budget reduction.

On June 22, 2011, the state of Wyoming announced that it had completed transitioning its 10,000 state government employees to Google's Apps for Government Platform. The solution chosen by Wyoming includes email, documents, calendar and video, disaster recovery, and Federal Information Security Management Act (FISMA) certification. In connection with the migration, the state projects that it will save \$1 million annually.⁹

ENDNOTES

- 1 The Cloud First Strategy announced in November 2010 directs federal agencies to identify and migrate three IP capabilities into the cloud within 18 months. See *Federal Cloud Computing Strategy*, available online at www.cio.gov/documents/federal-cloud-computing-strategy.pdf.
- 2 See *Bloomberg Government Briefing, Federal Cloud Computing and Data Center Consolidation*, by Afzal Bari, March 2011. The number of federal data centers would be reduced from 2094, to 1286.
- 3 *Federal Cloud Computing Strategy*, p.1.
- 4 Johnson, Martha, "GSA Is In The Cloud," *The GSA Blog*. Posted on July 26, 2011, accessed on Aug. 22, 2011, available online at <http://gsablogs.gsa.gov/gsablog/2011/07/26/gsa-is-in-the-cloud>.
- 5 "Cloud Computing in State and Local Government, Who's in the cloud? Your Peers, That's Who" available online at http://microsoft.com/Industry/government/guides/cloud_computing/slg/default.aspx.
- 6 Jackson, Joab, "Microsoft Signs Cloud Deals with California, New York City," *PCWorld.com*. Posted on Oct. 20, 2010, accessed on Aug. 30, 2011, available online at www.pcworld.com/businesscenter/article/208332/microsoft_signs_cloud_deals_with_california_new_york_city.html.
- 7 Johnston, Stuart, "New York City Workers Going to Microsoft's Cloud," *internet.com*. Posted on Oct. 21, 2010, accessed on August 29, 2011, available online at <http://itmanagement.earthweb.com/netsys/article.php/3909276/new-york-city-workers-going-to-microsofts-cloud.htm>.
- 8 Gaudin, Sharon, "San Francisco moves onto the cloud with Microsoft," *Computerworld.com*. posted on May 18, 2011, accessed on Aug. 29, 2011, available online at www.computerworld.com/s/article/9216832/san_francisco_moves_onto_the_cloud_with_microsoft.
- 9 "Wyoming spurns Microsoft, chooses Google Apps. State completes migration to Google Cloud Platform," *Electronista.com*, updated on June 22, 2011, accessed Aug. 30, 2011, available online at <http://electronista.com/articles/11/06/22/state.completes.migration.to.google.cloud.platform>.

the customer should carefully negotiate the terms of any underlying non-disclosure agreement to ensure it is protected in the event its data and confidential information is compromised by a successful hacking event. The services provider should be obligated to notify the customer of any attempted hacking and any known security breaches affecting the confidentiality of the customer's information or the security of the customer's data.

The major network data breach experienced by the Sony PlayStation Network in April 2011 underscores risks created by data in the cloud. Between April 17 and April 19, 2011, Sony Network Entertainment America PlayStation was hacked, reportedly by the hacking group Anonymous.¹⁹ Sony did not acknowledge the breach until April 26, 2011, almost 10 days after it occurred. Sony shut down the network and Qriocity, its media streaming service, for 25 days. It was reported that personal information for more than 77 accounts and 12 million credit card numbers was compromised. A number of class action lawsuits were subsequently filed against Sony, alleging Sony failed to take reasonable care to protect, encrypt and secure the private and sensitive data of its users, and seeking monetary compensation for data loss, credit monitoring and other relief.²⁰

There have been other major data breaches in 2011, including at Lockheed Martin in which over 100,000 network users were affected,²¹ and the Epsilon data breach in March 2011,²² which affected companies that outsource their marketing and email communications to Epsilon. Epsilon's affected customers included Target, Kroger, TiVo, JP Morgan Chase, CapitalOne, Citibank, Home-shopping Network and Ameriprise Financial.

Compliance

A customer cannot delegate its compliance obligations. As such, although the contract between a company and a services provider may state that the provider must comply with flow down requirements imposed on the company, the provider should also indemnify the company for any breach of its obligations to comply with the company's compliance obligations, or failure to comply with any applicable laws. The most common compliance obligations, which a company should flow down to the services provider, are Sarbanes-Oxley (SOX) and privacy obligations such as the Health Insurance Portability and Accounting Act and Gramm-Leach-Bliley.

Service levels

Service levels are an important means of ensuring a services provider meets its obligations. Service levels should be negotiated for all important aspects of service delivery, including availability, error corrections and issue

resolution, user support and service upgrades/technology upgrades. Service-level credits should be attached to each of these metrics. Service-level credits should apply after an initial "burn in" period during which the services provider can bring the company's systems online without worrying about financial penalties. The "burn in" period should be no longer than 60 days from the start of the delivery of services. Service-level credits should not be the company's sole remedy for the services provider's breach of the service levels. At some point, the company should have the right to terminate the agreement for cause if the services provider's failure to meet the service-level metrics becomes excessive.

Technology determination

One way that cloud services providers achieve economies of scale to provide lower cost, is to require all customers to use a common technology and architecture platform. A common platform has many benefits but also has drawbacks. Customers usually have no control over upgrades and changes in technology. Thus, there may be an unforeseen impact on a customer's technology systems. For example, an upgrade may not be compatible with other software solutions within the customer's IT network. Thus, the customer should carefully consider any mandatory obligation to upgrade as well as any impact it may have on its systems. In addition, the customer may also lack the flexibility to add additional functionality to its system.

Use of subcontractors

Companies considering migrating to the cloud should generally not be concerned with the services provider's use of subcontractors, provided that the services provider contracts directly with the third-party subcontractor and is responsible for the subcontractor's performance. Companies should ensure that the cloud services provider directly provides all services. The company should not be required to contract with a third-party vendor for ancillary services. For example, in the process of switching to a new cloud services provider, if a company's data must be reformatted to avoid potential accountability issues in the event problems should arise, the incumbent or new cloud services provider, and not a third party, should be responsible for such reformatting. The company should avoid being caught up in finger-pointing and disagreements between the cloud services provider and the third-party subcontractor.

Termination

From the company's perspective, the agreement's termination provisions are among the most important provisions in the agreement. The company should ensure

Well-advised companies should ensure that the cloud services provider is contractually required to provide transition services for an agreed-upon period of time.

that, regardless of the reason for termination, the cloud services provider will promptly return the company's data in a pre-agreed format. The cloud services provider should not have the ability to withhold the company's data for any reason including, but not limited to, any payment obligation. Of course, from the service provider's perspective, withholding the company's data is one of the few leverage points it has for ensuring the company's prompt payment.

Well-advised companies should ensure that the cloud services provider is contractually required to provide transition services for an agreed-upon period of time. From the company's perspective, it should be no less than 90 days. Most services providers seek to limit the time period so that they can focus their resources on other customers. Cloud services providers do not want to be committed to providing termination services for a significant period of time.

A cloud services provider will usually negotiate to charge a premium rate and require payment in advance if it terminates the agreement because of the company's breach. If the agreement is terminated for the services provider's breach, the provider should be obligated to provide the services at the rates in effect at the time of termination. Finally, the services provider should be contractually required to cooperate with the company and with the company's new provider to ensure a smooth transition.

Other issues for consideration

Other issues the parties should consider are which party's privacy policy will govern the provision of the services; the backup processes for data storage, including where and how often the data will be backed up; and restrictions on data location and dispute resolution. In the case of disputes, triggers for beginning the dispute-resolution process and the method for resolving the dispute (i.e., mediation, arbitration, litigation etc.) should be agreed upon.

Public sector contracts

Governmental entities are increasingly negotiating cloud contracts. One of the largest public entity negotiated contracts is the City of Los Angeles/Google Apps agreement executed in October 2009.²³ The agreement was negotiated with Computer Sciences Corporation as a reseller using Google, SADA and Appirio as subcontractors, and provided for the migration from Groupwise Novell to Google Apps for 40 government departments involving up to 30,000 users. The total value of the transaction was announced at \$25 million, with the first year valued at approximately \$6 million.²⁴

Also in California, the city and county of San Francisco negotiated a cloud service agreement to migrate to the Microsoft Office Suite email system. Email services for more than 23,000 employees across 60 departments and agencies will be provided. The service will cost \$1.2 million per year and will help the city achieve a mandated 20 percent budget reduction.²⁵

In public sector contracts, limitation of liability, warranty and indemnification are usually the most difficult issues to resolve. Cloud services providers usually seek to limit their liability to a multiple of the agreement's monthly fees charged by them. Most services providers resist indemnifying a company customer for third-party liability arising from the service provider's actions or from breach of the contract.

Another significant issue for governmental entities and companies with sensitive data is the location where the data will be stored. Most are concerned with data being moved outside of the United States, and with security issues if the data is from sensitive public service departments, such as fire and police departments. Other issues relate to accepting government "flow downs," including local government regulations, which may significantly increase the cost of providing cloud services, especially when these additional costs may be applicable to only a single customer.

User groups


User groups, which are not industry specific, have come together to drive developments in cloud computing. In October 2010, the Open Data Center Alliance (the Alliance), an independent IT consortium, was formed to coordinate standards for the development of data centers that would be fulfilled by cloud computing. The stated mission of the Alliance is to: identify the customer requirements for corporate adoption and deployment of cloud computing; define usage models that outline expected delivery of these requirements based on open, industry-standard and multi-vendor solutions towards a vision of secure federation, automation, common management and transparency; influence industry innova-

ACC Extras on... Migrating to the Cloud

InfoPAKSM

- *Cloud-Based vs. On-Premise eDiscovery and Information Governance (Aug. 2011).*
www.acc.com/infopaks/cloud-ediscovery_aug11

QuickCounsel

- *Cloud Computing: Considerations for Data Safety (Sept. 2010).* www.acc.com/cc-data-safety_sep10 

Presentations

- *Legal Aspects of Cloud Computing (May 2011).*
www.acc.com/legal-aspects-cc_may11
- *Reducing Risk for Your Company Through Cloud Computing (Oct. 2010).* www.acc.com/reducing-risk-cc_oct10

Top Ten

- *Top Ten Considerations When Using Cloud Computing (Sept. 2011).* www.acc.com/topten/cloud-computing_sep11

Think Tank

- *Cloud Computing and Social Media (May 2010).*
www.acc.com/thinktanks/cloud-computing_may10

Article

- *Cloud Computing (Dec. 2009).*
www.acc.com/cloudcomp_dec09

Alliance

- More than a million professionals depend on the easy-to-use, cloud-based solutions from IntraLinks, an ACC Alliance partner. IntraLinks lets you collaborate more effectively, manage risk more efficiently and share information more securely. ACC members receive a 20 percent discount on all new subscription contracts. Find out more at www.acc.com/alliance.

ACC has more material on this subject on our website. Visit www.acc.com, where you can browse our resources by practice area or search by keyword.



The new GLD button lets you click to copy, print or email a checklist from certain ACC online resources.


tion focus with a collective membership commitment to utilize Alliance Usage Models to guide corporate planning and purchasing of data center resources coupled with Solutions Provider member commitment to prioritize solution delivery based on Alliance Usage Model requirements; and collaborate with industry standards bodies to define required industry standard development aligned with Alliance priorities.

Members of the Alliance include more than 150 enterprise-level corporations in financial services, energy, telecom, industrial manufacturing and media from the United States, Europe and China. The Alliance is said to represent more than \$100 billion in annual IT spending. The Alliance is guided by a 12-member steering committee.

In June 2011, the Alliance published a list of eight standards (Usage Models) documenting user requirements for fostering cloud adoption by Alliance members. The standards are intended to:

- assure levels of security and enable security compliance monitoring;
- allow interoperability and interfacing between proprietary clouds; and
- provide a common service catalog so customers can compare services, features and pricing among the providers.²⁶

Protecting your investment

Cloud computing offers a cost-efficient and effective means for customers to manage their information technology needs. Like any technology, however, cloud computing is not without its limitations. As such, a prudent customer should carefully consider and negotiate the terms of the underlying agreement to ensure it is protected from both a legal and business perspective. 

Have a comment on this article? Visit ACC's blog at www.inhouseaccess.com/articles/acc-docket.

NOTES

- 1 Five-nines reliability (i.e., 99.999 percent) of uptime is being marketed by some cloud services providers. See *Computerworld.com*, article posted on April 26, 2011, by Patrick Thibodeau. Available online at www.computerworld.com/s/article/9216160/who_gets_blame_for_amazon_outage.
- 2 See "A Tale of Two Clouds" by Bill Ahlstrom. Posted May 11, 2009. Available online at www.tmforum.org/community/blogs/cloud_computing_blog/archive/2009/05/11/a-tale-of-two-clouds.aspx.

- 3 The pay-as-you-go model is particularly attractive to companies where the alternative has been investment in infrastructure software, which is severely underutilized. In a report of a study conducted by Sun Microsystems, *Take Your Business to a Higher Level* (2009), it was reported that server and storage utilization rates in enterprise data centers typically average less than 12 percent. Report available online at www.anja.it/opencms/export/sites/default/documenti/55d915d2-93d9-11de-a31d-f3c446ddbba06_cloud_computing_primer.pdf.
- 4 "Cloud Computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned with minimal management effort or services provider interaction. This cloud model consists of five essential characteristics, three service models and four deployment modes." The National Institute of Standards and Technology (US Department of Commerce).
- 5 www.automatedtrader.net/headlines/78807/nyse-technologies-unveils-cloud-platform.
- 6 15 USC §§6801-6809 (1999).
- 7 FINRA's proposed rule was announced on April 29, 2011. The initial comment period expired on May 13, 2011.
- 8 Respectively, HIPAA and the HITECH Act of 2009; and the Children's Online Privacy Protection Act of 15 USC §§6501-6506 (1998) (COPPA).
- 9 For The Electronic Communications Privacy Act, see 18 USC §§ 2510-2522 (1986); for the USA Patriot Act, see 115 Stat 272 (2001).
- 10 As of October 2011, the States that had not yet passed data breach notification legislation were Alabama, Kentucky, New Mexico and South Dakota. www.claa.org/documents/breach.
- 11 Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the United Kingdom.
- 12 Argentina, Andorra, Canada, Iceland, Liechtenstein, Norway, Guernsey Island, Faroe Islands, Isle of Man, Israel, Jersey Island and Switzerland.
- 13 Safe Harbor requires annual self-certification to the US Department of Commerce. The Safe Harbor certification provision is not available to US financial services companies.
- 14 The European Union provided the Model Contractual Clauses to service agreements between a services provider and a company. The Model Contractual Clauses were updated in 2010 to provide that subprocessors of data are to be held to the same standards of confidentiality and security as a data importer.
- 15 Binding Corporate Rules allow multinational corporations to transfer data across borders provided that the Data Protection Authority in each country from which data are to be transferred approve of such transfer. The Binding Corporate Rules must also be otherwise in accordance with the Article 29 Working Party requirements.
- 16 See "German DPA Issues Legal Opinion on Cloud Computing" by Hunton Williams LLP, July 1, 2010. Available online at www.martindale.com/computer-data-services/article_hunton-williams-llp_1071518.htm.
- 17 [Ec.europa.eu/information-society](http://ec.europa.eu/information-society). The description of the comment period provides that, "The European Commission is seeking views from citizens, businesses, public administrations and other interested parties on how to fully benefit from cloud computing."
- 18 For the AWS Outage see http://money.cnn.com/2011/04/21/technology/amazon_server_outage/index.htm. For Google's 2011 outage see www.eweek.com/c/a/Cloud-Computing/Gmail-Outage-Highlights_Googles-Restoration-Response-858387/.
- 19 See www.pcmag.com/article2/0,2817.2384919.00.asp. Anonymous is a loosely organized computer hacking and activist group. See [http://en.wikipedia.org/wiki/anonymous_\(group\)](http://en.wikipedia.org/wiki/anonymous_(group)).
- 20 See, e.g., *Johns v. Sony Computer Entertainment America LLC et. al.* (complaint available online at <http://www.techfirm.com/storage/johnsvsony-complaint-final.pdf>); *Maksimovik v. Sony Japan, Sony USA, Sony Canada et.al.* (Toronto Canada).
- 21 See <http://reflectionsonsecurity.wordpress.com/2011/05/30/lockheed-martin-cyber-attack-linked-to-rsa-data-breach>.
- 22 See www.eweek.com/c/a/Security/Epsilon-Data-Breach-Hits-Banks-Retail-Giants-154971.
- 23 See www.info.apps.gov/content/city-los-angeles-california.
- 24 For an outline of the deal see David Huber, "CSC, Google join forces on LA cloud computing project," *Washington Technology*, May 18, 2010. Available online at <http://washingtontechnology.com/articles/2010/05/03/state-and-local-csc-google-la-cloud.aspx?page=1>.
- 25 Sharon Gaudin, "San Francisco moves onto the cloud with Microsoft," May 18, 2011. Available online at www.computerworld.com/s/article/9216852/san_francisco_moves_onto_the_cloud_with_microsoft.
- 26 www.opendatacenteralliance.org.

"Legal Considerations in Migrating to the Cloud." Copyright © 2011 the Association of Corporate Counsel. All rights reserved. If you are interested in joining ACC, please go to www.acc.com, call 202.293.4103, ext. 360, or email membership@acc.com.

MOSES & SINGER LLP

Disclaimer

Viewing this or contacting Moses & Singer LLP does not create an attorney-client relationship.

This is intended as a general comment on certain developments in the law. It does not contain a complete legal analysis or constitute an opinion of Moses & Singer LLP or any member of the firm on the legal issues herein described. This contains information that may be modified or rendered incorrect by future legislative or judicial developments. It is recommended that readers not rely on this general guide in structuring or analyzing individual transactions or matters but that professional advice be sought in connection with any such transaction or matter.

Attorney Advertising

It is possible that under the laws, rules or regulations of certain jurisdictions, this may be construed as an advertisement or solicitation.

Copyright © 2011 Moses & Singer LLP
All Rights Reserved