Preparing and Advising Your Clients on Cloud Usage

Janet A. Stiven

Follow this and additional works at: https://via.library.depaul.edu/bclj

Recommended Citation
Available at: https://via.library.depaul.edu/bclj/vol12/iss4/3
Preparing and Advising Your Clients on Cloud Usage

Janet A. Stiven*

DESLINA WILLIAMS: I'm Desalina, and I'm the editor for the Business & Commercial Law Journal. I will be introducing Janet Stiven. She is the vice president and general counsel of The Moody Bible Institute of Chicago. Prior to becoming Moody's vice president and general counsel, for twenty-eight years Ms. Stiven was a member and a business attorney in the Chicago, Illinois office of Dykema Gossett, a national firm with more than 350 lawyers. She has advised clients concerning Cloud services agreements, terms of use, Cloud vendor assessments, and Cloud computing policies and related privacy and data security considerations. Please welcome Janet Stiven.

JANET STIVEN: Good afternoon. It is my pleasure to be back "home" at DePaul. As some of you may know, I am an alum of the DePaul College of Law, and it is exciting to be here to talk to you about a topic that I have focused on for a number of years. The issues surrounding Cloud computing have some different dimensions than those presented when we first started using the Internet to provide services. When contracting or provisioning Cloud services, it is important to think about the big picture. During my twenty-eight years of law firm practice, I gained extensive experience drafting and negotiating contracts. Part of effective contracting requires an understanding of both the contract provision and their context. If you are a lawyer, you have been trained to understand conceptually what the legal provisions mean; but if you do not understand the context, you will not be able to effectively review and comment on the agreement. The context for reviewing Cloud contracts requires knowledge that Catherine Sanders Reach discussed in her presentation. If you are going to be a lawyer practicing in the Cloud, I suggest you invest some time to learn how the technology works.

From my perspective, technology is becoming the platform for business. Whether you work in a law firm or in a company, technology is linked inextricably to everything we are doing; so you have to understand how it works. You need to develop a "road map" to guide you as you go through the process of provisioning for cloud services. Ini-

* Vice President and General Counsel at The Moody Bible Institute of Chicago
tially, you have to consider the duties that your board and management might have related to the company’s use of the Cloud service. The biggest thing to think about from a fiduciary standpoint is the enterprise risk that can be involved in using Cloud services. You also need to consider the due diligence process you are going to use. As for the agreement itself, you will need to think about what the contract provisions mean in the context of the deal that you are working on.

We should distinguish between consumer Cloud services and business enterprise Cloud services. I assume that most of you have used consumer Cloud services, such as those on the list that was displayed on the screen a few minutes ago. Many Cloud services were developed based on the consumer model where many Cloud services were initially provided for free. We now understand that the free model was not so free because of the information that you give up in exchange for the “free” services. But from the business point of view, the consumer Cloud model was not built for enterprise security because the drivers of that platform are different.

Thus, when evaluating business Cloud services, you need to think about the enterprise risks that might be involved. The risks will vary depending on the business. If the risks are significant enough, the board of directors will need to be involved in the decision of whether to deploy a particular process or service to the cloud. Due diligence is a critical part. A due diligence checklist is a valuable tool no matter what business you are representing. Checklists provide a way to standardize your thought process and make sure you do not overlook important risk elements and processes. Lawyers trained in Cloud computing matters can raise appropriate questions and bring good analytics to bear on the process for evaluating use of the Cloud service and weighing the legal and business risks.

As you think about the Cloud model, think of a stack with three layers: infrastructure, platform, and software. You will also need to consider the deployment model since they each have different legal implications. Amazon Web Services, AWS, is probably the infrastructure backbone for many Cloud services. Rackspace is another big provider. The platform layer is where development work is being done. Cloud software, or “SaaS” is the Cloud service with which most people are familiar. Cloud software services are accessed through your browser.

The big picture issue to discuss with your business client about the Cloud is strategy. What is the business problem that the Cloud solution is going to solve? A lot of people are excited by the Cloud be-
cause of many conveniences they have experienced using personal Cloud services. There is a desire to bring similar conveniences and tools to the business arena. Unfortunately, many consumer Cloud services were not built with the kind of protections, efficiencies, and scalability needed for a business enterprise. So you want to make sure that the Cloud service that you are evaluating is designed to solve the business problem or need identified by your client.

So ask the question “What is the business goal and objective and how does this Cloud service solve that problem?” Expertise in this area is important. I understand that the general counsel at a multinational company recently sent to the law firms that serve their companies a technology survey. The survey was directed to the associates, who are the ones who would be most likely to review the contracts for that client. The survey revealed that none of them could answer the technology-related questions correctly. This example underscores the importance for lawyers of all ages and experience to educate themselves on the topic of Cloud computing. In addition to educating yourself on Cloud technology, you will need to ensure that the company’s business team involved in assessing the Cloud services is also educated on this topic; and, to the extent, they need outside resources to make sure that they have access to and use of those other resources to identify and manage risks.

Because the Cloud is still in the early stages of development, many companies lack specific Cloud-use policies, but they may have IT related policies. So you would look at those existing policies as you evaluate how the Cloud service fits in with existing enterprise risk management process and determine whether some other risk mitigation steps would be needed before deploying the service. You will also need to consider the security, privacy, and compliance requirements for the particular business you are representing. For some businesses that may be HIPAA, and for others it may be the PCI standards related to credit card transactions. In the financial services area, you have to meet the GLBA standards.

We will be discussing a wide array of other federal and state laws that implicate the use of Cloud services. It is essential to carefully consider the regulatory landscape. The risk management process includes a risk assessment that identifies the risks to be addressed. Once you have identified the risks, you will need to be certain that the contract provisions address and mitigate those risks. Something often overlooked is vendor management. This is an important management issue. There is a need for vendor due diligence prior to contracting
and also the need for a continuing plan for monitoring the vendor the back end.

The risks in Cloud computing are varied. These include strategic risks, reputational risks and an assortment of other risks. It is interesting to read what large public Cloud providers say about risks—I recommend reviewing the risk factors sections in public company filings for the large cloud companies. Pay attention to what these providers are disclosing. The risks identified include a loss of all your data, security breaches, reliance on third-party technology, an inability to perform the Cloud services without the assistance of other companies in their supply chain, and that they are depending on someone else that you do not know to provide the cloud services to you.

System interruption is another risk. As you likely have experienced, access to the Internet is not available. Since Cloud services are totally dependent on an Internet connection, access and “uptime” are essential. Depending on the nature of the business, an interruption in Internet service may mean that a business may not be operational during the time of that system interruption. Lack of redundancy is another risk. This risk is particularly significant when considering cloud vendors that are also a major part of the Cloud infrastructure, such as, AWS. You will need to consider the implications of an interruption in service involving a Cloud services company that is also the backbone Cloud architecture and the risks of putting important business systems out in that environment.

You also need to consider regulations that affect the company that is considering use of Cloud services. You may have read about some of the litigation in Europe involving major Cloud providers and restrictions that are being placed on them. It is important to evaluate how those restrictions impact the Cloud services that your business client is considering. Unanticipated regulations imposed on a particular Cloud vendor or part of the Cloud delivery system could impact your business client. Consequently, you will need to focus both on regulations that affect your clients, and the things that affect the Cloud vendors.

In evaluating the physical infrastructure of the Cloud provider you will need to determine where the actual physical servers are located. Are they in areas that are prone to earthquakes, floods, fires, and other natural disasters that wipe out the ability for the provider to deliver its services? These are just some of the things that the major Cloud providers have identified as risks of using Cloud services. Depending on the type of business client you are representing and the
nature of the Cloud service, you may have a much longer list of possible risks to consider.

People think of lawyers as sort of the people who are coming to "spoil the party" and advocate against the adoption of Cloud services. I believe, that as a lawyer, you need to work toward providing a solution, a way forward. Lawyers should be risk identifiers and mitigators.

How do we put all these risks in context when making a decision about whether to move forward with a Cloud solution? Some businesses use Cloud services to perform development work and testing of potential applications. That type of process may not have the same degree of risk as other business processes since you may not necessarily be placing the enterprise operations at risk for because it is a testing environment. The scope of risk may be different when a business uses the Cloud service for a critical business process. Catherine Sanders Reach mentioned that smaller law firms, for example, build their whole law firm practice in the Cloud. While this can be helpful to managing expenses because of the economies of scale provided by many Cloud applications, using the Cloud for critical business services places the entire business at risk. Prior to contracting for such Cloud services, you will need to calculate the cost to the business if there is a loss of access to the Cloud service.

It is important to consider some of the bigger picture things that can happen to a business if the data placed into the Cloud is disclosed and becomes widely available although not intended by the business? Lawyers need to be particularly cautious when using the cloud for business purposes since they are entrusted with protecting client information. What happens if the Cloud service does not perform as expected? It is important to consider before contracting for the Cloud service how a potential lack of functionality or poor performance will affect the risk assessment for the Cloud solution. What is the value the asset being placed into the Cloud and what is the consequence if something happens to it in the Cloud? You should think through the "what if" scenarios and help your business clients decide whether they want to take on those risks.

Evaluate the tools that you can use in the risk assessment process. Consider a site visit, when feasible. For example, law firms that are considering use of a Cloud solution for document storage and management are performing site visits and assessing look to see physical security as well as the technical controls. Some clients have been surprised when they have gone on a site visit and found the vendor's facility in an unsecure location. This has led to a decision, based on
the appearance of the facility, not to move forward to procure the Cloud service due to the lack of trust in the vendor's security controls.

There are also third-party issues to consider because so much of the Cloud depends on layers of other resources. Often businesses are unaware that the Cloud provider has contracted with other cloud vendors to provide aspects of the Cloud service. It is important to utilize good supplier due diligence practices, just as you would in a non-Cloud environment. In the Cloud, virtually every situation is likely to involve a third party. You will need to have a plan for investigating the various layers of service providers to understand whether the needed protections are being extended through the supply chain.

Another important issue to consider relates to confidentiality. I think people continue to get more comfortable with the use of Cloud services—comfortable in the sense of a willingness to relinquish privacy rights based on the large amount of data that many consumer Cloud providers have already aggregated. But confidentiality in the Cloud environment is still critically important because of the need for a business to protect its own proprietary information and the duties of confidentiality relating to employee and customer information. For example, employees' or customers' health, benefit, or financial information may be stored in the Cloud. Businesses using Cloud services may still have an obligation under the law, depending on the regulatory framework applicable to their business, to ensure that that information is protected as the regulatory framework might require. So you have to think about confidentiality, integrity, and availability of the information and how it gets impacted when using a Cloud service. One of the things that we will talk about in a minute are some of the changing laws in connection with privacy and how sharing that information with a third party might adversely impact the protections for that information. Some people have no expectation of privacy when sharing information, such as when information is shared with a third party without a confidentiality agreement. So as you negotiate contract terms with a Cloud provider, make sure that you build confidentiality requirements into the agreement and extend them through the business supply chain to help mitigate against the risks that using a third party to provide the service results in a waiver of the confidentiality.

With respect to risk assessments, unfortunately, as Catherine Sanders Reach mentioned, there is not any one set of standards that has been adopted regarding the risk assessment process. This means that attorneys must tailor the risk assessment process to the particular situation, regulatory requirements, and business needs of that client.
I recognize that the process I am describing may sound like a lot of work for what might be a small dollar value contract. However, while the cost of the service might be low, the long-term financial and business implications could be far greater. So you need to be considering those longer range perspectives and help your client decide how much time and money to invest on the risk assessment process. From the perspective of an in-house general counsel, it is a very fast paced environment and there is often resistant to a due diligence or risk assessment process as many businesses lack the time and financial resources to invest in this.

As lawyers in these situations, you should develop the tools that help to streamline the process. That is part of the reason for coming to a symposium like this, to develop an analytical framework for evaluating the Cloud provider and Cloud services agreement and accessing tools and resources for effectively navigating this process. This will help you bring value to the table as an attorney in this area. It is important. Do not skip over it because you can end up putting yourself in a situation with problems at the back-end because you did not take time to understand the technology and it is implications at the front-end.

When assessing, it is important to think about information security in the Cloud from three perspectives as you review the provisions of the Cloud services contract to make sure that appropriate controls are included: a business, technical, and administrative security perspective. Technical and administrative security requires consideration of questions such as the following: Are the systems and information going to remain available to you? Are you going to be able to control access and confidentiality? Are you going to be able to protect people from unauthorized use or disclosure of information or from loss of your data?

What makes this area difficult to navigate is the lack of a central location to access an inventory or laundry list of all the things to consider before using the Cloud. You will have to do a little research prior to negotiating each Cloud services agreement in order to understand the legal framework that is involved. A good starting place is with your client’s industry and check for any industry-specific legislation.

Jurisdictional issues continue to be a concern when using Cloud services. You will need to consider jurisdiction from both a U.S. and non-U.S. perspective. Be aware that once you go outside the U.S. the same protections and rules do not necessarily apply to the information and services. So understanding the location from which the Cloud
provider will deliver the services is important. Be certain to ask the Cloud provider during the risk assessment about the locations from which they provision their services and whether they will be handling your client's business information from locations outside the U.S. in order to determine whether that works for your client's regulatory framework. There are laws that relate to data disposal, destruction, security breach and encryption.

Encryption is an increasingly important topic in the Cloud arena because it helps to solve some security compliance. Encryption for HIPAA-related compliance has received a lot of attention in the health area because of the concern about health information being inappropriately or unexpectedly distributed, and encryption is considered an effective means of addressing that concern. Note that many Cloud providers are not yet offering encryption because of the difficulty in handling the encryption keys. Technology and the law are not keeping in sync with many laws written before current technology was developed. Duties relative to information security are changing such that defining and responding to information security threats may differ as time moves forward, and what may be reasonable security for one company may not be reasonable security for another.

The duties of care are relative to the information and our obligation. Another aspect of information security relates to contractual promises that your client has made to its employees, customers, or other parties that have set an expectation or created an obligation by your client about information handling that may be impacted by the Cloud service. Such promises are often found in privacy policies or other contracts. These undertakings must be considered to ensure that these obligations are passed through to the Cloud vendor in the Cloud services agreement. This is an important but often overlooked due diligence item. You can find information on privacy policy enforcement actions on the FTC's website. Many privacy policies are prepared by company personnel based on privacy policies for other companies without realizing that one size does not fit all. This results in unintended obligations concerning privacy and security. So do take time to think about whether your client has made privacy and security commitments before proceeding to use a Cloud service.

Due diligence concerning cloud services can be divided into two main aspects: due diligence related to the handling of the data itself and due diligence concerning the cloud service provider. There are different analytical approaches to each. From the data side, you will want to determine the information type, such as personally identifiable information, credit card information, or personal health information.
tion, and then classify the data. Classifying the data involves consideration of whether it is sensitive information, mission critical to your client’s business operation, or a trade secret. I would not place trade secrets into the Cloud.

Data segregation is another issue. Due diligence involves determining whether the data is going to be in a co-tenant Cloud service. Many Cloud services are offered in shared environments in which one server is used to create many virtual servers that can be used concurrently by a number of different companies. There is the opportunity for data leakage and the potential for other tenants on that server to inadvertently or deliberately access another company’s data. Companies concerned about access to their data sometimes prefer to maintain control over their server environment and choose to use a private Cloud or a private Cloud layered in a public Cloud. These decisions highlight the importance of understanding the potential technology solutions and the risks associated with using a shared cloud environment.

Recoverability of information is another key due diligence item. Cloud vendors should be questioned about their process for handling requests for access to data in the cloud when needed by the company. This is particularly relevant in the case of litigation. We found that clients have employee self-provisioning Cloud services. I have been surprised to learn that employees have placed company data in the Cloud without first securing approval from the legal or compliance departments in their companies or investigating the applicable regulations. Some of the self-provisioning results in company data being placed in the employee’s personal cloud service account. Thus, when it comes time to respond to a subpoena or to gather that information in connection with litigation and there is no easy means to retrieve that information.

Topics to address with the Cloud service provider (CSP) include ownership rights. This topic was a big concern in early Cloud service agreements because of the consumer orientation to those contracts. Often, the agreements stated that the CSP owned all the data provided by the customer. Based upon the concerns raised by business customers, there is now greater clarity from service providers about ownership. While the issue has been resolved to some degree, you still need to ask the question. If you plan to represent clients in Cloud computing contracts, you will need to educate your clients about reading all the fine print in the online terms and conditions associated with many cloud services before contracting to use the services. Personally, I sometimes choose not to use a Cloud service if there is ambigu-
ity about the ownership of the information that I might share with the CSP.

The issue of deletion is another topic to consider. You will need to assist your client in determining how to handle the deletion of the data when your client ceases use of that service. Depending on the service provider, if you have not made those arrangements up front, your data may remain in a Cloud environment in which you have no control, such as when you terminate the Cloud service and no longer have a contractual relationship with that provider. So if arrangements are not made up front at the time of signing the Cloud service agreement, a business may be left in an awkward situation of having its information out in the Cloud without any sort of control placed on it.

As you perform due diligence on a CSP, keep in mind that a number of them have only been in business for less than five years and that the failure rate of such businesses is 80 percent. You can develop a list of due diligence questions by consulting supply chain management materials and other legal resources. Some of the questions about the Cloud service providers to include on your due diligence list: What is the CSPs operating history and financial strength? What sort of procedures do they have? What internal controls do they apply? Do they use the strategies that Catherine Sanders Reach outlined in her presentation? What sort of timing accuracy and management information do they have? Is it an environment where there is a lot of acquisition activity? Are large service companies buying up smaller companies?

Acquisitions in the Cloud area regularly occur as companies seek the latest and greatest technology and are willing to paying a lot of money for it. What happens if your provider suddenly becomes part of another provider? Also, think about how they manage their system and the fact that your client is going to be interfacing with them in some way. If the CSP makes changes to its system architecture, it may impact your client's operations.

While part of the appeal of using Cloud services for some businesses is the fact that the CSP is handling the system management, your business client will still be responsible for managing access to the system. You do have to get granular in your analysis of the Cloud service and the CSP. Is there someone in the IT group at your client who is willing to invest the time for the necessary due diligence and ongoing responsibilities related to monitoring the Cloud service? Since Cloud technology is still relatively new, many companies lack personnel with expertise in this area. This means that you will need to help your client determine if it has the right resources to be able to
probe these system-related issues to make sure that the provider is able to interact with the company in a way that allows for appropriate management and maintenance of the system. Sources of information about the Cloud provider include financial statements and news reports. It has been surprising to me how frequently I find companies that have undertaken no due diligence concerning the cloud provider.

Certifications present another area of inquiry in due diligence. Some Cloud providers indicate on their websites that they are HIPAA or SAS 70 certified. This is misleading, as there are no such certifications. Although internal audit standards were developed for use with review of financial statements, they are frequently used in analyzing CSPs due to a lack of other standards. Other internal control standards used in the Cloud area include SOC-1, SOC-2, and SOC-3. These self-assessments are popular because they allow for standardization of analysis and comparison among CSPs. It allows you more of an apples-to-apples comparison. Remember, some of the standards are criteria that the company itself establishes. So depending on the criteria used one company’s assessment may not really be the same as another company’s if the other company used different self-assessment criteria. HIPAA has specific requirements that do not vary from company to company. Thus, a statement that a company is HIPAA compliant allows for a shared understanding of what that means.

Other standards that are commonly used by Cloud providers include PCI and ISO 27001. ISO standards are frequently used in the manufacturing area because of their global acceptance and understanding. The Cloud Security Alliance is considered one of the leading standard setting bodies in the Cloud. I suggest you visit their website regularly to stay abreast of standard initiatives and analytics you should be applying as you evaluate the internal controls. There are numerous and complex issues to consider when contracting for Cloud services. Do not practice in the Cloud area if you are not willing to invest the time to understand these components.

Once you have completed the due diligence and determined to proceed with use of the Cloud service, you will need to turn your attention to the Cloud services contract. Many Cloud providers still use click-wrap contracts which are accessed using the Cloud provider’s website. Do not let the fact that the contract is a web-based one deter you from requesting those contract modifications needed by your client. As is the case with many form contracts, the vendor’s goal is to discourage negotiations by presenting the contract in a manner that makes negotiating difficult. Realize that you are going to have to pay attention for hyperlinks within the Cloud terms and conditions of ser-
vices in order to ensure that you have reviewed all parts of the service agreement. Cloud contract components often include the CSPs privacy policy, use policy, and service level agreement. You want to make sure that you have identified all the components of the contract and reviewed them with your client. Otherwise, your client may end up not having the rights that they expected.

You will need to evaluate whether the Cloud service agreement addresses your client's business and security needs. You will need to prioritize the provisions of the Cloud services agreement that are most important to your client. This will be guided, in part, by your client's regulatory compliance obligations. Many Cloud contracts include provisions, which permit the CSP to make unilateral changes to the terms and conditions. These provisions are enforceable so carefully consider whether to accept such provisions as changes could result in functionality of the services.

Pricing is an important provision. Many businesses are finding Cloud solutions appealing, in part, because of convenience and cost effectiveness. Consider carefully the pricing provisions to ensure that your client ends up with services that meet its budgeting and cost savings goals. Part of the pricing is determined by what service you receive, how much, for how long and how fast, and the unit cost. You will need to ensure that your client is satisfied with the price structure for the Cloud service and that that pricing stays firm for the term of the agreement. Cloud services are attractive to businesses because they can be quickly provisioned. Provisioning quickly means that there are times when the business is using a lot more resources so costs will fluctuate depending on the level of usage. It can be beneficial to negotiate up front for X number of resources in exchange for a volume discount. Most companies, however, prefer to "pay as you go," which is a more typical model but may result in pricing spikes.

Ask for the right to audit the CSP although recognize that the CSP may resist this right because of burdens to the CSPs business operations. Some CSPs have instead started to use self-certifications based on standards established by industry groups. The coalescence around some of the current industry standards provides businesses with some comfort about the CSP internal controls. Large companies often are able to obtain the right to audit usually under a confidential agreement because of the security concerns of the Cloud provider not wanting to expose their security structure to anybody because that makes them vulnerable to attack. Depending on the leverage of your client, you should explore the opportunity to for a site visit and audit those
aspects of the CSP's operations that are important to the security program for your client.

Governing law, jurisdiction, and forum selection are obviously incredibly important. If you are going to have a dispute, where is the battle going to be fought? So pay attention to jurisdiction issues that might arise. Particularly if you are dealing with somebody providing the service from an international platform, you want to make sure you understand the laws of those jurisdictions or you may decide not work with a particular provider if they are outside the U.S. So just be attentive to that as you should be with every contract.

Service level agreements are important components of the Cloud services agreement as they go to the heart of the functionality and the service for which your client is bargaining. You should be aware that many CSPs subcontract some components of the Cloud service. This means that you will need to ensure that your client's Cloud services agreement contains appropriate protections related to this subcontracting of services and that the subcontractors expressly assume responsibility for any regulatory compliance related to the subcontracted services. The difficulty for companies provisioning for Cloud services is the fact that there is no have contractual privity with your CSP subcontractors. Mergers and acquisitions is a rapidly evolving area, and a company could be acquired and sometimes not every service is maintained. A company gets acquired because it has one service and a particular interest to the industry but maybe the others are not as appealing, and you could suddenly find the Cloud service that you are using is no longer available. Catherine Sanders Reach gave you an example of the attorneys who used a Cloud-based time-keeping system, which suddenly was not available anymore. Similarly, two years ago, the Department of Justice shut down a major Cloud provider and suddenly the customers were without access to the Cloud services and, more importantly, their data. You will need to address in the Cloud services agreement what happens if your client's information and cloud service is suddenly unavailable.

Law firms are being asked by their clients about the firm's disaster recovery plan because so much client information is held by law firms. You will need to make the same inquiry of the Cloud provider and include in the contract a plan for ensuring the return of your client's data. Liability is a big area of focus in all contracts, and the Cloud environment is no different. You have to pick your battles. Depending on your leverage, if you are a large company, you may have market leverage. Be certain to link together the warranty disclaimers, indemnities, and limitations on liability. The typical warranty dis-
claimer disclaims any and all warranties, so you will need to specifically negotiate the warranties that your client needs. You should include warranties that apply to the service level. You will need to avoid any inconsistency between the warranty disclaimers and the service level agreement. Limitation of damage provisions should be carefully considered. Some limitation is probably appropriate. You will need to consider the facts and circumstances of each Cloud service arrangement in order to determine what limitations, if any, are appropriate.

Be sure to investigate insurance coverage related to Cloud service use by your client. There is an insurance product being developed for these types of losses that companies might experience relative to use of Cloud services. Make sure you coordinate indemnification and limitation of liability provisions. I see frequently that those provisions are not correctly linked. Check the contract for provisions related to the destruction and loss or alteration of data. Evaluate provisions in the contract related to data breach. The laws in this area vary from state to state. There are a few states that impose front-end obligations, which could impact companies using cloud services. You want to think about the fact that many contracts only provide a notification of the breach and do not address the costs and expenses associated with addressing the breach. Be certain that the contract addresses the indemnity needs that you have relative to infringement claims. Typically in any technology contract, you want to make sure that the CSP is providing an indemnity for any intellectual property infringement. The CSP should indemnify your client for claims arising out of the use of the CSP’s technology.

Service level agreements can seem a little daunting for the non-technology lawyer. Understanding up time is important. Up time is when the services are expected to be available. Often the standard is set at 99.9 percent. Since the standard is not 100 percent, this means that there is a percentage of time the service might not be available. That might or might not be consequential to your business. If your client’s business model depends on a Cloud service being up and running, the percentage of down time is a key consideration. Typically a 99.9 percent commitment is related to sort of normal delivery and it excludes regular maintenance by the cloud provider. When you aggregate down time for regular maintenance and down time for regular upgrades and realize that that down time does not count toward the up time commitment, you actually have more down time than may be expected. You need to ask the provider about how fre-
quently they are doing those updates, and think about how they affect your client.

Think about the CSP's communication network and accessibility and how your client can communicate if about a problem or need to rapidly obtain information. You want to talk about how you escalate things. You should also think about resolution time. Most providers will offer some basic service levels about resolution of issues. You will need to determine whether those response times are adequate for your particular client. This is where the lawyer needs to take time to probe and understand and to ask questions about availability and performance expectations. Redundancy is also important. Discuss with your client the need to build back-up and redundancy so if that Cloud service is interrupted, there is a plan for system fail. Periodic return of the information is important and often is not requested. Be sure to agree up front about at what time and in what format the data will be returned to your client. Make sure the format is one useable by our client.

Most cloud agreements allow the cloud service provider to suspend access to the service if the provider is not paid. This can result in the customer's information disappearing immediately following any failure to timely pay. This may be a surprising result but can occur unless you properly draft the cloud services agreement. So you will want to make sure that you understand what their rights are. Request that notice be provided to your client before any suspension of service for non-payment. A payment might get lost in processing. You want to make sure to build in some kind of notice before any suspension of access to the service, and make sure you have an appropriate balance of responsibility.

We talked about third-party terms and just making sure as you negotiate these the terms are covered appropriately. The term of Cloud services is something to think about. Keep in mind that unlike the traditional software license, which permits you to install the software on your own computer and, typically, use forever, Cloud services typically will discontinue as soon as the customer ceases payments for the service. Be sensitive to this in planning any transition to a different service—your client might have to keep paying for two services while it transitions so that there is not interruption in access to the data from the other service.

Make sure you understand the costs that might be involved and the kinds of termination fees the CSP may impose. You want to avoid having to pay to leave a provider. Pay attention to hidden costs that
could affect the business deal. You want to negotiate receipt of advance notice of changes in services to avoid surprise.

Oversight and monitoring is important. Once you have negotiated the Cloud services agreement your client will have an ongoing relationship with the CSP and will need to ensure there is plan to monitor the CSP’s fulfilling all the contract obligations. Such a continuous monitoring plan is required for many financial institutions. You want to make sure that you are following the processes and making any changes that might be necessary.

I hope that this overview helped provide a framework for understanding the context for the contract and how to effectively tailor a Cloud services contract.

AUDIENCE MEMBER: We recently negotiated a Cloud service agreement that had a vendor subcontract with Rack Space. We are somewhat at a loss at finding what is the best deal so you can deal with a vendor you are working with as well as Rack Space. Are there any organizations that are sort of monitoring or saying what a particular Cloud vendor does so that it prevents each of us from having to go to a particular vendor and labor our SOA or our provisions?

JANET STIVEN: I do not know of any one industry source. Technology publications, like Information Week Periodically, publish such comparatives. Not necessarily across every point, but looking at some of the bigger picture issues will help you have a perspective of what to market. What is going on in the industry is important to understand. You want to be savvy and know what is customary in the marketplace.

AUDIENCE MEMBER: Because practically none of us would be here if we did it day in and day out. We would be teaching it.

JANET STIVEN: Spend time reading information published by large Cloud providers, such as Amazon Web Services and Rack Space. They have white papers that provide a lot of good background information. They are also starting to offer their own analytics. Watching what the bigger industry players are doing will help you have some perspective. You may find that the Cloud is not the solution for your client because you are unable to gain needed assurances.

AARON COOPER: Thank you, Ms. Stiven. We are going to take a short break.