Due Diligence Considerations for Lawyers Evaluating Cloud Computing Service Providers

THE FLORIDA BAR STANDING COMMITTEE ON TECHNOLOGY

MARCH 2017
(Formatting Update July 2018)

THE FLORIDA BAR
651 E JEFFERSON ST, TALLAHASSEE, FL 32399

Due Diligence Considerations for Lawyers Evaluating Cloud Computing Service Providers

Prepared by The Florida Bar Standing Committee on Technology

INTRODUCTION

The Legal Cloud Computing Association (LCCA) has developed standards for lawyers to consider when conducting due diligence of a cloud service provider (CSP) as required by Florida Bar Ethics Opinion 06-1 and 12-3. The Florida Bar's Standing Committee on Technology has annotated these standards with questions lawyers should ask their CSPs, and commentary on why the standard and questions are important. The Florida Bar takes no position on whether these standards define a lawyer's ethical or legal obligations to meet their duties to adopt reasonable security safeguards to protect client information and personally identifiable information. The Committee, however, strongly encourages lawyers considering the adoption of cloud computing to review Florida Bar Ethics Opinion 06-1 and 12-3. Additionally, reliance on the proposed questions for CSPs alone is not recommended. The lawyer considering the use of the cloud should consult with an information security and cloud computing expert who can tailor these questions and identify additional issues when conducting due diligence of a cloud service provider. Finally, The Florida Bar Member Benefits website lists CSPs that have met most or all the LCCA's standards.

I. PHYSICAL AND ENVIRONMENTAL MEASURES

A. Location of Data

CSPs should disclose where data housed in their systems is being stored geographically and can restrict its movement so that it remains within a country.

Questions Lawyers Should Ask Their CSP:

1. **Where is my data physically stored (country, city, facility)? Is it in more than one location? What controls are in place to assure data is kept there?**
2. **What physical security measures are in place at the location where the provider's systems are housed?**
3. **Is my data backed up? How often?**
4. **Who owns the servers on which my data is stored? (Is it the company itself or do they outsource to a vendor?)**
5. **How and when will I be notified if the data is going to be moved or replicated elsewhere?**

Commentary:

Certain laws (like data localization and data transfer laws) and contractual provisions (like client engagement agreements and business associate agreements) may prohibit a lawyer from transferring sensitive information (personal information, proprietary information, and other client information) outside the jurisdiction where the information is collected. Accordingly, a lawyer should assess where data will be physically stored.

Lawyers have ethical and legal obligations to ensure that reasonable physical security safeguards are in place to protect sensitive information. Lawyers should inquire about physical security measures and

location information to provide information on how the provider protects its facility ("data center") against theft as well as natural disasters.

Disaster plans are a crucial part of ensuring business continuity, and backup is necessary to protect one's data and minimize potential data loss and downtime in the event of a disaster or other event impacting access to one's data. Having a fulsome backup of your data can also provide relief in the event of a ransomware attack.

Lawyers have legal and ethical obligations to understand what happens to the client information they share with service providers (like CSPs): who will the CSP share the information with, who may have access to it, and who owns that data in the event the CSP goes out of business or the relationship is terminated.

B. Certifications

CSPs should host on reputable cloud services that have obtained one of the following certifications or met similar indicia. All the certifications listed are used to gain confidence and place trust in a service organization's systems.

a. Type 2 SOC 2 certification A Service Organization Controls ("SOC") 2 report evaluates an organization's information systems as they relate to security, availability, processing integrity, confidentiality, and privacy of a system.

b. ISO 27001 certification ISO 27001 is an international standard published by the International Standardization Organization (ISO), and it provides a framework of how to manage information security in a company. The main philosophy of ISO 27001 is based on managing risks: find out where the risks are, and then systematically treat them.

c. ISO 27018 certification ISO 27018 is the first International code of practice that focuses on protection of personal data in the cloud. It specifies guidelines based on ISO/IEC 27002, taking into consideration the regulatory requirements for the protection of Personally Identifiable Information ("PII") which might be applicable within the context of the information security risk environment(s) of a provider of public cloud services.

d. The Legal Cloud Computing Association's Standards on Cloud Computing.

Questions Lawyers Should Ask Their CSP:

1. **Have you obtained (and maintained) any of these certifications? If not, please list/describe any similar certifications.**
2. **With which federal, state, and industry-based security and privacy legal frameworks are you compliant? For example:**
    a. **The Payment Card Industry's Data Security Standards;**
    b. **The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Privacy Rule, Security Rule, and Breach Notification Rule under HIPAA;**
    c. **Gramm Leach Bliley;**
    d. **The Sarbanes-Oxley Act (SOX); or,**
    e. **other potentially relevant regulations?**
3. **Will you agree to sign a business associate agreement under HIPAA, if I represent healthcare providers or other HIPAA Covered Entities?**

Commentary:

These certifications are sometimes requested by clients and afford you the ability to demonstrate to a third-party that your firm's CSP has received an independent evaluation that determined the CSP met

a certain standardized level of security. Additionally, if you are storing in the cloud information for a client governed by HIPAA, GLBA or other federal/state laws that require specific security and privacy procedures and protections, or if you believe you may at some point represent such a company, then you must ensure that the CSP is compliant with those laws. If you represent healthcare providers, for example, you may be governed by HIPAA and may need to obtain a business associate agreement from the CSP.

C. Geographic Redundancy

CSPs must have their data centers in multiple geographic locations in the event of a natural disaster. The impact of an outage at one data center can be minimized by automatic backup and redundancy provided by additional data centers.

Questions Lawyers Should Ask Their CSP:

1. **Are the cloud-based applications and data stored in more than one geographically separated data centers? If so, how many and in which countries?**

Commentary:

Lawyers can minimize the risk of data unavailability by ensuring that their CSP has "geographic redundancy" (i.e., the same data located in more than one location). Initially, it is important to point out that most CSPs provide these geographic redundancies, but the lawyer should inquire as to where all his/her data may be housed, as there may be privacy or data security laws (data localization laws) or contractual obligations with certain clients that limit where the data may be maintained.

II. DATA INTEGRITY MEASURES

A. Encryption[1]

CSPs should maintain data encryption protocols covering: (1) data stored at the data center, and (2) data transmitted to and from the data center. Strong encryption may protect data from unauthorized access, copy, modification or other attacks to the integrity and security of the data.

Questions Lawyers Should Ask Their CSP:

1. **Is my data encrypted at rest? Is it encrypted in motion?**
2. **What data, if any, is NOT encrypted? At what point in time? Why?**
3. **Do you have encryption keys that would allow you to decrypt my data? Who has access to those keys? What is your policy regarding the sharing of those keys with any third parties such as law enforcement, regulatory authorities, court orders, etc.?**
4. **Who within your organization has access to my encryption keys? And why?**
5. **What if I "lose" the encryption keys?**

1 "Encryption" is essentially the process of making data unreadable to an unauthorized individual. There are primarily two types of encryption: (1) "encryption at rest" where data that resides on a hard drive is rendered unreadable; and (2) "encryption in motion" which ensures that when data is transmitted from one place to another (e.g., email) the data is encrypted. For a more in depth explanation of encryption, review this resource.

Commentary:

An attorney has an ethical obligation to investigate the online data storage provider's security measures, policies, recoverability methods, and other procedures to determine if they are adequate under the circumstances. Encryption is one of the most powerful technical safeguards that may be used to minimize the risk of unauthorized access to sensitive information; however, it is important that access to the encryption key (which can be used to unlock and read the encrypted data) is limited. Whether a CSP keeps a copy of the key or shares it with third-parties, is an important factor to consider in evaluating the security of sensitive information stored with those providers.

B. Testing

CSPs should disclose if and how frequently data testing (auditing) and/or ethical hacking services are being performed on their systems. Some of the testing methods are listed below.

a. Vulnerability Scans - A vulnerability scan is the process of identifying and quantifying security vulnerabilities in an environment. It identifies security flaws based on a database of known flaws, tests a system for the occurrence of these flaws, and provides a report of exposures and the associated level of risk for each confirmed vulnerability.

b. Penetration Testing is a simulation of an internal or external attack with the intention of gaining unauthorized access to systems and the data stored within the network.

c. Static Code Reviews - Static analysis code testing provides an understanding of security issues within program code. It is a systematic review of the software source code without executing the code. The main objective of this testing is to find errors in the early stages of the development cycle.

d. Dynamic Code Reviews - A Dynamic Code analysis relies on studying how the code behaves during execution. It monitors system memory, functional behavior, response time and overall performance of the system. The main objective of this testing is to find and fix any defects.

Questions Lawyers Should Ask Their CSP:

1. **What security measures and testing do you have in place?**
2. **How often is the testing administered and how or by whom?**

Commentary:

Lawyers should choose cloud-based service providers with a proven record on security and should conduct due diligence or consult with a technology expert who can make recommendations.

Assessment and verification of a provider's security measures by a third-party is one aspect of establishing trust in a cloud provider and its reputation. Regular audits and testing by reputable third-party assessors promote transparency and an assessment of the quality of the provider's measures.

C. Limitations on Third-Party Access

CSPs should disclose their policies relating to restricting and allowing 3rd party access to confidential client data by their cloud service provider and its representatives.

Questions Lawyers Should Ask Their CSP:

1. **Do you allow third-party access to client data? If so, to which third parties? Law enforcement? Regulators? Requests via court subpoena?**
2. **Do your service providers have access to client data? If so, which ones and why?**

3. **What protection and assurance will you give me that no third parties will have access to data I store with your service?**
4. **Please identify all functionality / services that is outsourced and name the third party.**
5. **Do these third-party vendors abide by the same security policies and procedures that apply to the cloud vendor's employees?**
6. **Are there business or function continuity plans if the third-party vendor fails?**
7. **Will you give me notice if subcontract out to other cloud service providers?**

Commentary:

Third-party access to client information presents a risk of unauthorized access, misuse, destruction, or theft of that information. It is therefore imperative that only those with a legitimate business need have access to the data. Given the sensitive nature of the data (client information, personal information, and proprietary information) it is reasonable to request that no third-party have access to your data or encryption keys for the data, and that the CSP provide notice if it changes who has access to the data.

D. Data Retention Policy

CSPs should disclose their data retention policies (i.e., how long they retain their customers' data). Additionally, the CSPs should take reasonable steps to ensure that when data is deleted from the cloud provider's environment, the cloud provider has measures in place to ensure the data is no longer available to any entity.

Questions Lawyers Should Ask Their CSP:

1. **Will you return my data when the relationship is terminated?**
2. **How long will you retain my data if the relationship is terminated?**
3. **Will you provide transition support if the service is terminated?**
4. **Will you securely and permanently destroy my data upon my request? How do you remove and delete my data? What documentation will you provide verifying that the destruction and return of data are complete?**
5. **Will any of my data in the possession of your vendors be permanently and securely deleted upon the termination of our agreement?**
6. **How do you send my data to me when the agreement is terminated?**

Commentary:

It is important that you have ownership rights in your data. When one of the parties wants to terminate the relationship, you should be able to request a copy of all your data and require that the CSP permanently and securely delete your data.2 If you cannot obtain these representations from the CSP, you may be obligated to inform your client of the possibility that the client's data "may linger on the cloud provider's servers for a period after representation has ended."[3]

[2] N.H. Bar Assn Ethics Comm. Op. 2012-13/4 (2013), available at New Hampshire Bar Association Ethics Committee Advisory Opinion 2012-13/4.

[3] The Ethical Implications of Cloud Computing for Lawyers, 31 J. Marshall J. Info. Tech. & Privacy L. 71 (2014)

III. USERS AND ACCESS CONTROL

A. End User Authentication[4]

CSPs should provide appropriate authentication protocols based on the needs of their customers. Examples include multi-factor authentication,5 strength of password requirements, certificate-based protocols,6 device authentication7.

Questions Lawyers Should Ask Their CSP:

1. **What methods and controls are available to ensure that the users who log in to access the data are who they say they are?**
2. **Does your service automatically time-out after a certain period of inactivity?**
3. **Are similar authentication requirements in place for mobile versions of your service?**

Commentary:

"End User Authentication" is the way the CSP determines you are who you say you are when you try to access data. This can be by using simple login credentials (username and password) or it could be a stronger safeguard like two-factor authentication (e.g., receive a text message with a pin) or biometrics (e.g., fingerprints or facial recognition through your mobile device).

B. Addition or Suspension of a User

CSPs should provide admin users8 the ability to add users and suspend users, as well as create certain limitations on users' access to information.

Questions Lawyers Should Ask Their CSP:

1. **Do I have exclusive control over who is added/removed to the service? If not, who else has this ability?**
2. **Can I can suspend a user's access to the service?**
3. **If an employee leaves my firm, what controls do I (or another administrator on my account) have available to terminate their access to my account?**

Commentary:

It is important that access to the law firm's sensitive information is controlled. Therefore, the law firm should ensure that it can manage, add, suspend, and delete user access to the information stored in the CSP. Similarly, the law firm should ensure that when employees depart the firm (or the IT service provider supporting the firm) their access to the CSP is immediately terminated.

---

[4] "End-user authentication" is a method by which the service verifies that the person trying to log in is who they say they are.
[5] "Multi-factor authentication" requires a user to provide at least two different methods of authentication (e.g., logging in username/password, plus responding to a text message).
[6] "Certificate-based protocols" build certain certificates into your device so that the service knows that the device belongs to a legitimate user.
[7] An example of "device authentication" may mean that when a device logs in from a different IP address than usual, additional security questions are presented to the user.
[8] An "admin (or administrative) user" is someone who has the highest level of control and access to the system. Typically, admin users are high level information security professionals within a company.

C. Tracking

CSPs should enable the ability to generate detailed audit logs[9] of user activities within their services and disclose the period they keep such logs.

Questions Lawyers Should Ask Their CSP:

1. **How is activity in my account monitored & documented in log files?**
2. **What do those log files show?**
3. **Does your service provide an easy-to-use/access/understand log of account / end-user activities such as log on and off time, downloads, uploads, etc.?**
4. **What reporting options and audit support are available?**
5. **How far back will the logs go, and how long do you keep the logs?**

Commentary:

Should a data incident or the need to investigate access to the firm's CSP arise, it may be important to know who accessed the data, what data they accessed, and when. Logs from the CSP will help to accomplish these goals while providing an ongoing ability to audit access to the CSP.

D. Addition or Deletion of Data

CSPs should enable the end user to add and delete data.

Questions Lawyers Should Ask Their CSP:

1. **What are my limitations for adding data and what data am I able to delete?**

Commentary:

Lawyers should be able to control the data in their account to ensure the proper retention and ultimately the secure deletion of sensitive information.

E. Retrieving Data

CSPs should provide functionality to enable users to be able to retrieve data in a usable non-proprietary format, and restore data inadvertently deleted within a reasonable period.

Questions Lawyers Should Ask Their CSP:

1. **If I choose to leave your service or need a copy of my data outside your system, what are my options for doing that?**
2. **What format(s) is my data stored in and exportable in?**
3. **If my data is inadvertently deleted, can it be restored? How?**

Commentary:

There may come a time when the lawyer decides to use a different CSP, or otherwise terminate the relationship. This transition/termination usually requires the transfer of data from the old CSP to the new one. There may also be third-party requests for data (e.g., pursuant to a lawful subpoena or other

[9] "Audit logs" track a user's activity in the CSP – when they logged in, for how long, what they accessed, etc.

court order). It is therefore important that the lawyer can immediately retrieve the data in a format that allows the data to be read and used easily.

IV. SERVICE AGREEMENT

A. Terms of Service

CSPs should present a clear and understandable Terms of Service. The Service Agreement should define the CSP's performance obligations with clear terms and definitions, demonstrate how performance is being measured and what enforcement mechanisms are in place to ensure the terms are being met.

Questions Lawyers Should Ask Their CSPs:

1. **Do you offer a Service Level Agreement (SLA)10 for your services? If yes, how many 9's does it have (look for 99.9% to 99.999% uptime guarantee)?**
2. **What incident response time does the provider offer in the SLA?**
3. **Are there penalties in place when SLA obligations are missed?**
4. **What are your limitations on:**
5. **My use of the service?**
6. **Indemnification if you lose or destroy my data? Limitations of liability?**
7. **Automatic renewal and cancellation of account by user?**
8. **Notification of any changes in the terms of service?**
9. **Payment details?**

Commentary:

The Service Level Agreement measures the period the CSP must be operable and provide your law firm the service it is purchasing. Maintenance and other technical issues can make your data temporarily inaccessible. So, it is important to limit that unavailability and ensure that any maintenance is performed during off-peak hours.

Other terms of service should also be reviewed to determine if there are limitations on how you can use the CSP, whether you will be indemnified if the CSP accidentally destroys or alters your data, and whether the payment terms are consistent with your expectations.

B. Privacy Policy

CSPs should provide a clear and accessible Privacy Policy. The Privacy Policy should disclose how information supplied to the service is housed, protected, shared, manipulated, or disposed of. In general, all user information entered into a CSP application should be treated as confidential, private information that cannot be used by the CSP for any purposes other than support of system integrity and usability objectives. Furthermore, the CSP should only be permitted to view your information when they have your explicit consent.

[10] A "Service Level Agreement" defines the service a customer can expect to receive from the provider. Examples include the amount of time the service will be available, how quickly the provider will respond to inquiries, and whether any the provider will be subject to fines/penalties if it fails to comply with these commitments.

Questions Lawyers Should Ask Their CSPs:

1. **What is your privacy policy?**
2. **Do you use customer data to promote your organization through advertisements?**
3. **Do you share customer behavior or other customer information with third parties? If so, with whom and why?**
4. **Does your privacy policy require that you give me notice if there are any material changes to the policy? Is my consent required for you to make any material changes to your privacy practices? If not, what recourse do I have so that I am not opted into those privacy practices automatically?**

Commentary:

A lawyer is obligated to know where his client's information is stored, with whom, and what that entity does with the client's data. A good CSP privacy policy should explain that information to the lawyer who may then want to share that information with her clients. The CSP's privacy practices may change over time (e.g., it may decide it wishes to share information with third-parties), so it is important that the lawyer be immediately informed of any such material changes so she can determine whether a change in CSP is necessary.

C. Uptime Guarantee

CSPs should clearly state their uptime guarantee and the metrics upon which it is based. Uptime is the amount of time that a server has stayed up and running. The guarantee must clearly state how uptime is defined and what is the compensation if the uptime promise is not met.

Questions Lawyers Should Ask Their CSPs:

1. **What uptime and performance SLAs does the provider offer?**
2. **Are there penalties in place when SLA obligations are missed? / Do you offer compensation commensurate with any potential financial loss if my organization suffers due to lack of availability? Will you compensate me automatically or do I need to ask for it?**
3. **Do you have a transparent, public site where you publish any system issues or outages for everyone to see?**
4. **What is your downtime history?**

Commentary:

As discussed in the section on Service Level Agreements above, lawyers should ensure that a quantifiable amount of uptime/downtime is set forth in the agreement with the CSP. Downtime occurs when a provider is inaccessible to customers for a period. Because downtime (or cloud outages) can be disruptive and costly for your law practice, it's wise to review a provider's track record of downtime and select a provider with as few (or no) downtime incidents as possible.

D. Confidentiality

CSPs should include terms to abide by the duties of confidentiality in the Privacy Policy, thereby ensuring that the online data storage provider has an enforceable obligation to preserve users' confidentiality and security of user data.

Questions Lawyers Should Ask Their CSP:

1. **How is my data isolated and protected from your other customers' data?**
2. **Do your Terms of Service, Privacy Policy, or Service Agreement address confidentiality and security?**

Commentary:

The confidentiality of data you store in the cloud is a primary concern for lawyers who incorporate CSPs into their practice. Lawyers have an ethical obligation to maintain as confidential all information that relates to a client's representation, regardless of the source. A lawyer may not voluntarily disclose any information relating to a client's representation without either application of an exception to the confidentiality rule or the client's informed consent. Additionally, a lawyer has the obligation to ensure that confidentiality of information is maintained by nonlawyers under the lawyer's supervision, including nonlawyers that are third parties used by the lawyer in the provision of legal services.

Enforcing these ethical obligations may require limitations on the nonlawyer's (CSP's) ability to share your client's information with third parties (e.g., requests from third-parties in private civil litigation, informal requests from law enforcement, or the provision of sensitive information in response to a subpoena without first notifying you).

E. Ownership of Data

CSPs should provide an explicit recognition of the user's ownership of the data. It should be clearly stated that the provider cannot acquire any rights or licenses, including intellectual property rights, to the user's data.

Questions Lawyers Should Ask Their CSP:

1. **Who owns the data (including any copies) we store in your service?**
2. **Do you believe you have any rights of ownership in my data?**
3. **What assurance will you provide, if our relationship is terminated, that all data is returned to me and that you will securely destroy all copies of my data?**
4. **What language is built into our agreement with your service that memorializes your position on data ownership?**
5. **Do you use my data for statistical or other proprietary purposes? If so, do you anonymize the data? Will you give me the option to opt out of this use of my data?**

Commentary:

Information lawyers store in the cloud belongs to the lawyer and her client. The CSP should not hold any ownership rights in that data. To allow a CSP to have ownership rights in the data or copies of the data creates a risk that the data will be shared or moved without your control, and that it may not be securely returned and destroyed at the end of the relationship.

F. Requests for Data

CSPs must notify users of demands for their information by 3rd parties as soon as possible, unless the provider is specifically prohibited from doing so by law.

Questions Lawyers Should Ask Their CSP:

1. **Do you have a formal policy or procedure, incorporated into my agreement with you, that memorializes your position on how you respond to requests from third**

parties for access to or copies of my data? If there is no formal policy or procedure, is there an informal one?

2. **How do you respond to informal requests for data from law enforcement or any other third-parties?**
3. **If a third-party presents a warrant or subpoena requesting my data, how will you respond? Will I be notified and given an opportunity to formally object or move to quash the request before you produce my information?**
4. **Will your procedures change if we no longer have a contractual relationship but you still have a copy of my data in your possession (though I hope you will have destroyed all such copies)?**
5. **Will you provide me with an option where I am the only person/entity with the encryption keys to unlock my data stored with your CSP (i.e., you will not store a copy of that key)?**

Commentary:

How a CSP responds to third-party requests for data goes to the heard of a lawyer's ethical obligation to maintain the confidentiality of his client's data. The CSP should not provide any of your data to a third-party without a lawful subpoena or warrant. Even then, the data should not be provided without first notifying you of the request and providing an opportunity to object to the request or move to quash the request. Ideally, the data will be encrypted and only you will have a copy of the encryption key, so the third-party will not be able to read the contents of your data.

G. Data Breach

CSPs must immediately notify users of any unauthorized access of the user's information. The CSP's policy covering time and method of notification should be clearly stated as well as the standard policies and practices for responding to such data breaches. To the extent, the lawyer incurs costs investigating the CSP's data breach, or any third-parties bring claims against the lawyer because of the CSP's breach, the CSP should agree to indemnify the lawyer for those costs and claims.

Questions Lawyers Should Ask Their CSP:

1. **Is there a provision in the service agreement requiring the CSP to give me immediate notice (preferably within 48 hours of discovery of the incident) of any suspected unauthorized access to my data?**
2. **Will the CSP agree to provide as part of the above notification, the following information:**
3. **The date, estimated date, or estimated date range of the breach;**
4. **A description of the information that was accessed or reasonably believed to have been accessed as a part of the breach of security; and,**
5. **The number of individuals who were or potentially have been affected by the breach.**
6. **Is there a provision in the service agreement that will require the CSP to cooperate with me to investigate the data breach and, to the extent I incur any costs investigating a CSP data breach, the CSP will indemnify me for those costs?**
7. **Will the CSP agree to indemnify me for any claims brought against me by third-parties because of the CSP data breach?**
8. **Does the CSP's service agreement have a mandatory arbitration provision that requires any claim or lawsuit that you bring against the CSP for a CSP breach require arbitration or other alternative dispute resolution process?**

9. **Does the CSP carry cyber insurance? If so, what does the insurance cover/exclude? What are the coverage limits?**

Commentary:

State and federal data breach notification laws, contractual obligations between lawyers and their clients, and ethical obligations all may require lawyers to notify their clients if their clients' data stored with the CSP has been accessed by an unauthorized third-party. Under these same laws, a service provider with whom the lawyer has shared certain client information is often legally required to notify the lawyer of any unauthorized access of that information. It is important that a process is in place at the beginning of the relationship between the lawyer and the CSP that ensures a lawyer is immediately notified of a potential compromise of his/her client's data.

The cost of responding to such an incident and notifying affected clients and other third-parties may be expensive. It is therefore important that the lawyer-CSP service agreement explain who will bear the financial burden of investigating data breach, notifying affected third-parties, and any claims made against the lawyer based on the CSP's breach. The CSP may carry cyber liability insurance that will cover these costs and may even make you an additional insured under their policy. [11]

H. Disaster Recovery

CSPs have an obligation to maintain an accurate, up-to-date and regularly tested process for recovery and continuity plans in the event of a natural disaster or business disruption.

Questions Lawyers Should Ask Their CSP:

1. **How will our data be protected in the event of a power outage, facility disaster, local disaster and regional disaster?**
2. **How quickly can operations be restored if the main system goes down?**
3. **How do you protect your data center(s) from natural disasters, including fires, floods, hurricanes, and earthquakes?**
4. **Can your service scale up to meet my business needs as my law firm grows?**
5. **Does the contract include terms that limit data access by the vendor's employees to only those situations where you request assistance?**
6. **If the provider goes out of business, what is the process to retrieve your data and how long will it take?**

Commentary:

If a lawyer is not able to move his or her data to another cloud service provider, this may render the data unusable. If the lawyer's practice is largely cloud-dependent, it may also impact a lawyer's ability to maintain the systems necessary to remain in uninterrupted practice. Additionally, lawyers have record retention obligations, and depending on the type of client or matter, these files may have to be retained for different time periods. As your firm grows, so will your cloud storage needs. To ensure that you're choosing a flexible cloud provider, find out what additional storage capacity and other services can be offered over time and for how much.

[11] Protect your firm: Invest in cyber liability insurance, ABA, (July 2013).