KEEPING YOUR HEAD IN THE CLOUDS

(Contracting with Cloud-Based Service Providers)

May 20, 2014

CCPA Compliance Forum
Rocky Hill, Connecticut

David Benoit, Esq.
Aeton Law Partners, LLP
Origin of Cloud Computing

- In the 1960s Ross Perot rented idle computing power from one company to carry out processing needs of another (mostly during the night)

- Bartering of Computer power: Win-Win
  - Company that owned the computers monetized its downtime
  - Company that needed computing power did not have to outlay capital for equipment
Types of Cloud-Based Services

- Broad Definition: Scalable provisioning of IT as a service using the Internet or a network.

Three main cloud computing models:
- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)
IaaS

What do you want to be when you grow up - a *cumulonimbus*?

Data Storage.

© D. Fletcher for CloudTweaks.com
IaaS

- Client outsources equipment used to support operations, typically on a pay-per-use basis
  - Storage
  - Hardware
  - Servers
  - Networking Components
- Service Provider owns equipment and is responsible for housing, running and maintenance.

aetonlaw.com
PaaS

- A way to “rent” hardware, operating systems, storage and network capacity over the Internet
- Allows clients to rent virtualized servers for running applications or developing and testing new ones
- Adds vendor management of the operating system, middleware and runtime database to an IaaS service
- Often used by developers to build applications on top of the computing infrastructure
SaaS

- Provider delivers software (typically based on a single set of common code and data definitions) that are consumed in a one-to-many model
- Software is licensed on a pay-for-use, per-user or a term basis
- Adds data management and application management to a PaaS environment
Why Move to the Cloud?

- Speed and Flexibility
- Heightened Security
- Easier Collaboration and Integration
- Cost Reduction
- Greater Connectivity and Mobility
Why Move to the Cloud?

Thanks to cloud technology, Nigel can not only work from home, but he can work from other people’s homes as well.
Contract Differences: Traditional vs Cloud

- **Right to Use**
  - Perpetual licensing vs subscription use
  - License fees + support/maintenance vs bundled

- **Payment Terms**
  - Withhold license fees until acceptance vs due once service becomes available

- **Overall Loss of Direct Control – What does that mean to your organization?**
Factors to Consider

- The application you are using (e.g. what use purpose does it support?)
- How critical the application is to your business to help determine the necessary availability levels that will be demanded (e.g. is it customer facing and/or does it provide a key business function?)
- The data that will be exchanged, stored and maintained by the provider (e.g. how sensitive is the data, where will it will be stored and who will have access to it?)
Fee Structures

- Ensure that the right to use the software is clear and that there are no hidden fees.
- For example, if the pricing metric for the service is determined by the number of users, is the metric per unique/seat user, concurrent or only active users?
- Does the provider also charge for technical support to users who are not really using the software application but need ad hoc access to it?
Functionality

- Clearly identify all of the functionality you are paying for from the provider to ensure they do not degrade this functionality over time.

- One good way to memorialize this in the contract is to attach a functionality matrix with screenshots of the software application as an appendix to the contract.

- Also, list all additional and optional fees in the contract, such as additional storage fees, custom reports, etc.
Ownership

- Clearly identify who owns any customizations or enhancements, especially if your organization pays for them as “work product” developed solely for your organization and they provide a competitive advantage.

  (e.g. an individual branch of the provider’s standard base code that is unique to your organization and for which you paid for the development effort).
Data Rights and Responsibilities

- Include language that states who owns data during all of its lifecycle, including when data is transferred or exchanged (data in transit) and during storage (data at rest).

- Include language regarding who bears the risk for loss of data in transit.

- Depending on the nature of your data and how it is processed, you should negotiate language to affirm your ownership of the results of any processing of data that occurs on the provider’s systems.
“I liked it better before big data and metadata when we just had good old regular data.”
Data Rights and Responsibilities

- Consider including a process that allows for regular backup of your data on your premises.
- Need for on-premises data backup is situational, depending on the criticality and comfort level of your organization with each SaaS engagement.
- Possibly no on-premises backup is needed, but this should be considered.
Data Rights and Responsibilities

- Define the provider’s responsibilities in the event of:
  1) A security breach (e.g. ensure they provide an immediate notice if your data may be compromised);
  2) An outage; and
  3) Termination of the agreement (e.g. ensure the provider will cooperate with the return of your data in a format and manner previously agreed, and with no additional fees for the return of data).
Security and Disaster Recovery

- Obtain detailed information about the provider’s security processes and procedures, including data flow diagrams.
- One way to obtain this information is to leverage a questionnaire approach.
- Draft these minimum security conditions into the contract and obligate the provider to maintain them throughout the term of the agreement.
Security and Disaster Recovery

MY DOCTOR SAYS MY HAIR LOSS IS CAUSED BY ME WORRYING ABOUT DATA LOSS!
Include language confirming the provider’s:

- Data storage period and data destruction policy;
- Business continuity plan (specifying redundancy requirements to include data backup and recovery methods/processes).
- Participation in disaster recovery testing at specific time intervals (e.g. once every two years) without charge.
Termination

- Even though a provider may lock your organization in for a specific contract term and minimum number of users, ensure the ability to terminate for cause, including a continued lack of uptime and availability.

- Ensure payment terms are clear and confirm that the provider cannot immediately shut off services for late or disputed invoices.
Key components should contain specific, measurable and enforceable terms that the provider must adhere to for each component of the service provided.

If the provider fails to meet an obligation, the SLA must have the “teeth” to help mitigate such failure from happening again.

The “teeth” are specific remedies that apply when the provider’s obligations are not met.

Remedies usually take the form of monetary damages for specific failures and/or credits for future services.
SLAs: Key Contact Information

- List all account management and technical support contact information including phone numbers.
- Contact information should be reviewed several times during the year to ensure it is up to date.
- Identify the provider’s regular hours of operation and support, and identify where their support centers are located.
- This is useful to know if their support centers are located off-shore or in different time zones.
SLAs: Response and Resolution Times

“Thank you for calling Customer Service.
If you’re calm and rational, press 1.
If you’re a whiner, press 2.
If you’re a hot head, press 3....”

© Randy Glasbergen
glasbergen.com
SLAs: Response and Resolution Times

- Include a matrix that identifies
  1) Priority levels for different software modules and the diverse technical issues that can arise;
  2) Provider’s response times; and
  3) Provider’s expected resolution times for each.
    - Resolution times may not be guaranteed by the provider, but response times should be.
- Ensure your organization has the final say in determining the severity level for each potential issue.
SLAs: Response and Resolution Times

DOGBERT’S TECH SUPPORT

HELLO, I...

SHUT UP AND REBOOT.

HEY, IT WORK...

SHUT UP AND HANG UP.

MY AVERAGE CALL TIME IS IMPROVING.
Identify the uptime and application performance metrics needed for each software service component.

Ensure uptime and performance calculations are listed in the SLA and that they can be objectively and easily measured on a rolling basis (not per calendar month).
SLAs: Uptime and Performance

- Quantify the downtime allowed in terms of hours or days so you can truly understand the impact of downtime business needs.
  - For example, a 99.7% uptime would mean that there is approximately 11 allowable days of unplanned downtime in one year.
  - A recommended approach would be to negotiate at least a 99.9% uptime, allowing for less than four days of downtime in one year.
Hold the provider accountable for things within its control.

A provider cannot control the public network or the Internet, but it should be able to provide reports regarding the time it takes your data to be processed and actionable steps on its side for the specific service you are using affected by unplanned downtime.

A provider can share risk with its counterparts and ensure that the network providers its chooses also have contingency plans in place to ensure uptime.
SLAs: Uptime and Performance

- Identify the provider’s standard maintenance windows.
- Define what “planned maintenance” means and confirm that the provider will provide a reasonable notice in advance to be considered “planned maintenance.”
- Define the calculations to be used for credits if uptime or application performance guarantees are not met.
- Explain the process to obtain a credit, including the notice period needed for requesting the compensation and when and how the compensation will be provided.
SLAs: Uptime and Performance

- Include the ability to terminate the entire agreement without further liability if uptime fails over a particular period of time (e.g. if uptime drops x amount over x number of rolling days).
- Most cloud providers will want you to commit to at least a year of service (usually paid monthly).
- What if you sign a one-year deal and the service is down for five days straight upon the start date?
- Do you still want to be committed to that provider for the next 360 days?
SLAs: Maintenance and Support

- Identify how many major and minor versions of the software are allowable compared to the provider’s most recent generally available (GA) version.
- Ask about the frequency of releases and upgrades (both minor and major) upgrades upfront.
- Codify the notification process for releases and ensure that you can opt out of releases or upgrades (assuming that your instance is not too many versions behind their most recent GA version).
SLAs: Maintenance and Support

- Identify the ongoing support expectations for any customizations and enhancements.

- This includes identification of turnaround times if custom reports that you cannot create on your own are needed (e.g. reports that require the provider’s help or third-party professional services).
Cloud Questions?

aetonlaw.com
David Benoit
Aeton Law Partners LLP
aetonlaw.com
860.724.2162
101 Centerpoint Drive
Middletown, CT 06457
dbb@aetonlaw.com