Cloud Computing: Managing the Legal Risks
Mitigating Liabilities When Outsourcing Virtual Storage and Applications

TUESDAY, JUNE 18, 2013

1pm Eastern  |  12pm Central  |  11am Mountain  |  10am Pacific

Today’s faculty features:

Janine Anthony Bowen, Partner, Jack Attorneys & Advisors, Atlanta
Daniel A. Masur, Partner, Mayer Brown, Washington, D.C.
H. Ward Classen, Deputy General Counsel, Computer Sciences, Hanover, Md.

The audio portion of the conference may be accessed via the telephone or by using your computer’s speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact Customer Service at 1-800-926-7926 ext. 10.
**Tips for Optimal Quality**

**Sound Quality**
If you are listening via your computer speakers, please note that the quality of your sound will vary depending on the speed and quality of your internet connection.

If the sound quality is not satisfactory and you are listening via your computer speakers, you may listen via the phone: dial **1-866-570-7602** and enter your PIN when prompted. Otherwise, please **send us a chat** or e-mail **sound@straffordpub.com** immediately so we can address the problem.

If you dialed in and have any difficulties during the call, press *0 for assistance.

**Viewing Quality**
To maximize your screen, press the F11 key on your keyboard. To exit full screen, press the F11 key again.
Continuing Education Credits

For CLE purposes, please let us know how many people are listening at your location by completing each of the following steps:

• In the chat box, type (1) your company name and (2) the number of attendees at your location
• Click the SEND button beside the box

If you have purchased Strafford CLE processing services, you must confirm your participation by completing and submitting an Official Record of Attendance (CLE Form).

You may obtain your CLE form by going to the program page and selecting the appropriate form in the PROGRAM MATERIALS box at the top right corner.

If you’d like to purchase CLE credit processing, it is available for a fee. For additional information about CLE credit processing, go to our website or call us at 1-800-926-7926 ext. 35.
Program Materials

If you have not printed the conference materials for this program, please complete the following steps:

• Click on the + sign next to “Conference Materials” in the middle of the left-hand column on your screen.
• Click on the tab labeled “Handouts” that appears, and there you will see a PDF of the slides for today’s program.
• Double click on the PDF and a separate page will open.
• Print the slides by clicking on the printer icon.
Cloud Computing: Managing the Legal Risks

Primer and Risk Mitigation

Janine Anthony Bowen, Esq., CIPP
jbowen@jack-law.com
(678) 823-6611
June 18, 2013

© 2013 Jack Attorneys & Advisors. All Rights Reserved.
Agenda

• Brief Overview of Cloud Computing

• Later...Minimizing & Mitigating Legal Risk
Cloud computing is a model for enabling ubiquitous, 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 and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

NIST Definition (cont)

• Essential Characteristics
  – On-demand self-service
  – Broad network access
  – Resource pooling
  – Rapid elasticity
  – Measured Service

• Deployment Models
  – Private Cloud
  – Community Cloud
  – Public Cloud
  – Hybrid Cloud

• Service Models
  – Software as a Service
  – Platform as a Service
  – Infrastructure as a Service
Deployment Models: Public Cloud

- The cloud infrastructure is made available to the general public
Deployment Models: Private Cloud

- The cloud infrastructure is operated solely for an organization.
Deployment Models: Hybrid Cloud

- The cloud infrastructure is a combination of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability between environments.

Public Cloud

Private Cloud
Deployment Models: Private Outsourced Cloud

- The cloud infrastructure is operated solely for an organization.
## Three Service Models

### SaaS (Software as a Service)
The consumer uses the provider’s applications running on a cloud infrastructure. (e.g. Google Apps)

### PaaS (Platform as a Service)
The consumer has control over the deployed applications and possibly application hosting environment configurations. (e.g. Force.com)

### IaaS (Infrastructure as a Service)
The consumer is able to deploy and run arbitrary software. (e.g. Amazon EC3)
Contracting for Cloud Services — Key Considerations

Dan Masur
Mayer Brown LLP
Partner
202 263 3329
dmasur@mayerbrown.com

June 18, 2013
Contracting for Cloud Computing Services
The Road to the Cloud!
Breadth of Cloud-Based Offerings

“Nice to have” business tools
Routine, non-sensitive data
Limited scope of business use

Mission critical applications
Regulated or business sensitive data
Enterprise-wide use

Each end of the spectrum presents different legal and contractual challenges, options and trade-offs
Cloud Customers Must Make Informed Tradeoffs

• There is no standard contract “form” that will work for each situation
  – Traditional outsourcing and software licensing terms may be useful, but can not be inflexibly applied to cloud computing

• More robust contractual protection may or may not be the correct answer — it depends

• Prospective cloud customers must take into account
  – Criticality of the software, data and services in question
  – Unique issues associated with cloud computing
  – Public, private or hybrid model
  – Availability and pricing of various alternatives

• For “nice-to-have” business tools or routine data, a low cost solution may outweigh contractual protections

• Requiring robust contractual protections may increase the price and eliminate certain providers altogether
Key Issues/Risks in Cloud Computing
Data security is by far the largest concern as the market has yet to address enterprise security requirements.

Source: TPI

<table>
<thead>
<tr>
<th>Concern</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data security</td>
<td>78%</td>
</tr>
<tr>
<td>Failing regulatory requirements</td>
<td>51%</td>
</tr>
<tr>
<td>Integration risks with legacy systems</td>
<td>49%</td>
</tr>
<tr>
<td>Unclear who has access to my data</td>
<td>49%</td>
</tr>
<tr>
<td>Disaster recovery</td>
<td>48%</td>
</tr>
<tr>
<td>Co-mingling of data</td>
<td>34%</td>
</tr>
<tr>
<td>Up-time availability</td>
<td>33%</td>
</tr>
<tr>
<td>Connectivity / bandwidth</td>
<td>29%</td>
</tr>
<tr>
<td>Service provider viability</td>
<td>27%</td>
</tr>
<tr>
<td>Unclear where data is stored</td>
<td>26%</td>
</tr>
<tr>
<td>Response time</td>
<td>25%</td>
</tr>
<tr>
<td>Migration to different service</td>
<td>25%</td>
</tr>
<tr>
<td>Ill defined business case</td>
<td>11%</td>
</tr>
</tbody>
</table>

n=73
We are at an intersection, with privacy regulation dramatically increasing at the same time cloud computing is increasing exponentially. Enterprises need to understand and prepare for entry into cloud computing – requires assessment, planning (including for regulatory requirements) and careful transformation.
Issues with Privacy and Security: The “Elephant in the Room”

- Data transfer issues (EU and similar jurisdictions)
- Data location issues
- Location of users accessing data
- Movement and storage of data
- Use of subcontractors
- Lack of transparency and control
- Data breach issues
- Data destruction issues
- Ability to impose security and privacy requirements
Issues with Cloud Computing
Privacy and Security — US

- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health (HITECH)
- Fair Credit Reporting Act/FACT Act
- Federal Trade Commission Act (FTCA)
- ID Theft Red Flags
- State Privacy Security Laws (Breach Notification — 45 States and Encryption (MA and NV), use of SSN’s, etc.)
- Industry Standards (PCI)
Issues with Cloud Computing
Privacy and Security — Non-US

In EEA and other jurisdictions where data protection and data transfer regulation is strict, cloud computing challenges and issues increase
Other Critical Contracting Issues for Cloud Customers

### Regulatory and Compliance Challenges

- Auditability
- Lack of transparency and control
- Subcontracting and flow down of provisions
- Electronic discovery issues
- Record retention issues

### Other Key Issues and Challenges

- Service levels
- Disaster recovery and business continuity
- Exit rights
- Financial stability of providers/due diligence
- Export control issues
Cloud Computing
So now what? Can we even do this?
Contracting for Cloud Computing
YES!

• Keep your eye on
  – Criticality of the software, data and services
  – Unique issues associated with cloud computing
  – Public vs. private cloud
  – Availability and pricing of various alternatives

• Leverage outsourcing, software and data use precedent as appropriate
Tier One Enterprise Providers are beginning to get it.....

• Tier One and similar providers are beginning to offer solutions addressing customer concerns, often through private clouds.

• Private clouds offer more protection than public clouds; however private clouds do not magically solve all privacy, security and compliance issues.

• Private clouds cost more than other leveraged solutions.

• They can be dedicated (close to data center services) or leveraged (still some cost savings, but with more limited rights than in a traditional ITO model).

• Some private clouds are not really cloud services (utility model) at all – they are merely custom data center and hosting services.

• Generally, enterprise cloud solutions offer better protections than pure utility cloud solutions.
Public vs. Private Cloud: The Impact on Key Contracting Issues
1. Service Commitments

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Commitment to Contract Terms</td>
<td>Terms may be changed by provider in its discretion</td>
<td>Terms changed only by mutual agreement</td>
<td>Terms changed only by mutual agreement, or a few things may be unilaterally changed by provider, with exit rights with no penalty if changes are not acceptable</td>
</tr>
<tr>
<td>Commitment to Services</td>
<td>High-level definition of standard services, often “AS IS”</td>
<td>Detailed and customized service definition</td>
<td>A detailed, but not customized, definition</td>
</tr>
<tr>
<td>Minimum Term Commitment</td>
<td>Little or no minimum term</td>
<td>Long term commitment early termination charges</td>
<td>May have a short minimum term or long notice period</td>
</tr>
</tbody>
</table>
## 2. Service Quality Protections

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Testing and Acceptance</td>
<td>No testing, no acceptance – perhaps “demo”</td>
<td>Testing built into transition and all deliverables</td>
<td>Testing of key transition milestones and deliverables.</td>
</tr>
<tr>
<td>Commitment to service levels</td>
<td>No meaningful service levels or service level credits and/or unrealistic hurdles to obtaining credits</td>
<td>Detailed and customer-specific service levels with meaningful credits</td>
<td>Service levels built for supplier technology not customer needs, but with meaningful credits</td>
</tr>
</tbody>
</table>
3. Customer Control Rights

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Determine architecture</td>
<td>No right to approve supplier’s architecture</td>
<td>Customer approves architecture</td>
<td>No right to approve supplier’s architecture</td>
</tr>
<tr>
<td>Control changes by provider</td>
<td>Provider may make changes without notice or consent</td>
<td>All changes to services require customer approval</td>
<td>Provider must give notice and customer may terminate if changes have an adverse effect</td>
</tr>
<tr>
<td>Personnel Continuity</td>
<td>No commitment to personnel continuity</td>
<td>Commitments for continuity of key personnel and turnover protections</td>
<td>May have some commitment to continuity of a few key personnel, but with fewer rights</td>
</tr>
</tbody>
</table>
## 4. Compliance Obligations

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Assistance in complying with laws</td>
<td>Standardized offering, no particular assistance, other than standard reports</td>
<td>Compliance with all laws applicable to supplier’s services to customer</td>
<td>Some ability to configure to meet compliance requirements, but often limited solutions</td>
</tr>
<tr>
<td>Audit rights</td>
<td>Typically not available, especially not for subcontractors</td>
<td>Extensive operational and financial audit rights</td>
<td>Some rights available, but may not include physical access</td>
</tr>
<tr>
<td>Other incentives for compliance</td>
<td>Extremely limited liability for breaches or failures of any type</td>
<td>Liability for direct damages up to a cap subject to exclusions</td>
<td>More like dedicated private cloud contracts</td>
</tr>
</tbody>
</table>
## 5. Termination Assistance

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Termination assistance</strong></td>
<td>Return of data if terminated for convenience – no promise of data portability</td>
<td>Extension of services and extensive assistance in transition</td>
<td>Extension of services and reasonable assistance in transition – some terms around data portability</td>
</tr>
<tr>
<td><strong>Post-Termination Rights to Technology</strong></td>
<td>None</td>
<td>Post-termination license, rights subject to exceptions, right to acquire dedicated hardware, and right to make offers to dedicated supplier personnel</td>
<td>Usually none</td>
</tr>
</tbody>
</table>

---

**M A Y E R • B R O W N**
## 6. Fees

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Flexible, Consumption Based Pricing</strong></td>
<td>Consumption-based pricing – by the drink, may be small set up charges</td>
<td>Some fixed or “base” charges, with variable charge component – may not be able to reduce consumption to zero</td>
<td>Lower fixed charges, with high ability to reduce or increase consumption</td>
</tr>
<tr>
<td><strong>Termination Charges</strong></td>
<td>Minimal to none (perhaps small break fee), no wind down expenses (all people and assets are leveraged)</td>
<td>Break fees and wind down expenses, with obligations to cover dedicated stranded assets and dedicated people</td>
<td>Lower break fees, and should be no wind down expenses as assets and people are leveraged</td>
</tr>
</tbody>
</table>
Balancing Privacy, Security and Compliance Requirements with Cloud Offerings
## Balancing Privacy, Security and Compliance Requirements with Current Cloud Offerings

<table>
<thead>
<tr>
<th>Customer Need</th>
<th>Pure Public Cloud Solution</th>
<th>Enterprise Cloud Solution (Leveraged Private Cloud)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Need for diligence due on provider</td>
<td>Physical diligence/inspection not permitted, and not possible if subprocessors used</td>
<td>Basic diligence information is available – certifications, audit reports, etc.</td>
</tr>
<tr>
<td>Know where your data is processed, transferred and stored</td>
<td>Data may be processed, accessed, transferred and stored anywhere</td>
<td>Location of data can be fixed in contract</td>
</tr>
<tr>
<td>Rights to approve subprocessors</td>
<td>Frequent use of subprocessors (scalability, flexibility, variable use)</td>
<td>Notice of subprocessors as necessary for compliance (EU), and approval in some cases</td>
</tr>
<tr>
<td>Controls on data and security standards</td>
<td>Standardized offering with use of cloud provider controls</td>
<td>Customer must review provider standards and determine sufficiency</td>
</tr>
</tbody>
</table>
# Balancing Privacy, Security and Compliance Requirements with Current Cloud Offerings

<table>
<thead>
<tr>
<th>Customer Need</th>
<th>Pure Public Cloud Solution</th>
<th>Enterprise Cloud Solution (Leveraged Private Cloud)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response to data security incidents</td>
<td>Standardized offering, use of sub-processors and other limits may delay discovery of breaches, and ability to provide information regarding extent of breach</td>
<td>Notification of security incidents is offered, although extent of liability remains an item of negotiation</td>
</tr>
<tr>
<td>Proper disposal and destruction of data</td>
<td>No guarantee all data will be found and erased or returned</td>
<td>Data will be returned or destroyed</td>
</tr>
<tr>
<td>Provider has some liability exposure for breaches and non-compliance</td>
<td>Extremely limited liability</td>
<td>More standard (ITO like) liability, although with different caps for security and confidentiality breaches around personal data</td>
</tr>
</tbody>
</table>
Minimizing and Mitigating Risks

• Agenda
  – Understanding the Environment
  – Preliminaries & Readiness Assessment
  – Mitigation Considerations
Technology Convergence

The law erects them...

Technology collapses boundaries...

All trademarks are owned by their respective owners, not Jack Attorneys & Advisors.
What boundaries are collapsing?

- Cost of Computing
- Privacy
- Geography
- Cost of Entry
Preliminaries

- The onus is on the customer to perform extensive evaluation of a cloud provider before entering into the relationship.

- The nature of the cloud relationship drives the requirements of evaluation. Considerations include:
  - The criticality of the cloud implementation
  - The sensitivity of the data/processes being outsourced to the cloud provider
  - The scale of the implementation
4 Immutable Laws of Cloud Security

• “These are things that will always be, things that will never change, and it is a state of being.”

  – First is an understanding that if your data is hosted in the cloud, you no longer directly control its privacy and protection.
  – when your data is burst into the cloud, you no longer directly control where the data resides or is processed.
  – if your security controls are not contractually committed to, then you may not have any legal standing in terms of the control over your data or your assets.
  – if you don't extend your current security policies and controls in the cloud computing platform, you're more than likely going to be compromised

  – Tari Schreider, HP chief architect of HP Technology Consulting and IT Assurance Practice.

“Security and the Cloud: The Great Reconciliation”, eCommerce Times, 14 May 2012  
Why Evaluate the Options?

Who you are drives what you can expect

- Cloud users should clearly understand what they are getting and getting into:
  - Potential costs
  - Best in breed
  - Lock-in

- Where negotiation is possible, needs analysis should drive negotiation of several key provisions (discussed later)
Preliminaries: Decisions to be made before evaluating cloud solutions

- **Why use cloud services?**
  - What are the benefits?
  - Will service quality be better?
  - Is the risk manageable?

- **What’s the scope of the services to be performed?**
  - Are they commonly available via cloud?
  - What requirements must be satisfied?

- **Who can best deliver the services and what’s their track record?**

- **Are there geographic limits on where the services can be delivered from? On where data can be stored?**

- **Does the cloud business case make sense for your business?**
  - Financially
  - From a risk perspective
  - Can the organization deal with the change?
Preliminaries: Checklist for Cloud Readiness

**Business Drivers**
- Do you have staff working remotely?
- Do you have plans to increase your IT infrastructure needs?
- Is your infrastructure reaching end of life?
- Are you constrained in terms of Capital Expenditure?
- Does your organization have a high level of software test/development?
- Does your organization struggle to obtain IT talent internally?
- Is 24*7 support important for your organization?

Source: Appendix in “You Want to Put my Database Where? CloudU
http://www.rackspace.com/knowledge_center/cloudu/curriculum
Preliminaries: Checklist for Cloud Readiness

- **Technical Drivers**
  - Is your application workload highly variable?
  - Do you need automatic infrastructure scaling and provisioning?
  - Do you have a need for complex IT redundancy and resiliency that you struggle to obtain internally?
  - Have you faced issues around IT security?
Quick List of Potential Mitigation Considerations

<table>
<thead>
<tr>
<th>Functionality of solution</th>
<th>Pricing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uptime</td>
<td>Response time</td>
</tr>
<tr>
<td>Quality of service</td>
<td>Data Security/Privacy</td>
</tr>
<tr>
<td>Backup and disaster recovery</td>
<td>Integration with existing systems</td>
</tr>
<tr>
<td>Data access</td>
<td>Customer service/support</td>
</tr>
<tr>
<td>Insurance coverage</td>
<td></td>
</tr>
</tbody>
</table>

Adapted from “Evaluating SaaS Solutions: A Checklist for Small and Mid-sized Enterprises”
Areas of Concern

• Service quality
  – SLAs/Availability
  – Audits/3rd party certifications
• Disaster recovery
• Data security & privacy law compliance
• Provider competence
• Provider Viability
• Role of 3rd Party providers
Mitigation Considerations: SLAs

- **Control-oriented**
  - System availability
  - System response time
  - Fail-over for disaster recovery

- **Operations-oriented**
  - Data retrieval
  - Data integrity
  - Transition assistance

- **Business-oriented**
  - Error resolution time
  - Timeliness re: professional services around cloud solutions
Mitigation Considerations: Backup & Disaster Recovery

• How are backup systems architected?
  – Complete redundancy? Multiple redundancies? Duplicate systems? Real-time backup?

• Where are backup systems located geographically?

• Are third party backup systems utilized (partially/totally)?

• How long would a catastrophic event at a data center affect system availability?

• Concerns for physical assets based on geography (exactly where is that data center located?)

• Ultimately, whose responsibility is it anyway?
We know you are going to do it, so...

• Plan for success and plan for failure.
• Know and mitigate your business and technology risk.
• There are no silver bullets, shortcuts, or easy answers.
Q&A

Contact Me

- Janine Anthony Bowen, Esq., CIPP/US
  jbowen@jack-law.com
  www.linkedin.com/in/jdabowen

- 678-823-6611

- Twitter - @cloudlawyer

- www.jack-law.com
Agenda

I. Significant Risks/Legal Issues
II. Managing the Risks
III. Important Issues to Consider
Significant Risks/Legal Issues

- Data Security
- Confidentiality
- Compliance
- Availability
- Service Levels
- Technology Determination
- Termination
Data Security Risk

How is customer’s data protected?

• The vendor should be willing to disclose security standards as well as practices and procedures.
• These practices and procedures should be subject to audit.
Confidentiality Risk

• Hacking does not usually result in a breach of the vendor’s confidentiality obligations.

• Notification to customer of known security breaches affecting confidentiality/security of customer data.

• Exposes vulnerability of global networked systems

• Examples:
  Sony Play Station
  Lockheed Martin
Regulatory Compliance Risk

- Customers must understand their compliance obligations and recognize that they cannot delegate them to a cloud vendor.
- The most common regulatory obligations are privacy/data security and SOX, but customers in regulated industries have additional obligations.
- Vendors may not have the same compliance obligations as their customers.
- Customers must determine whether and how their use of cloud services affects their ability to comply with applicable regulatory obligations.
Service Availability Risk

Network outages can seriously impact a customer’s operations

- Examples:
  - Amazon
  - Microsoft Hotmail Outage
  - Skype Outage
  - Google Gmail Outage

“Availability” should be carefully defined and negotiated.
Customers should carefully evaluate service levels offered by a vendor for all important aspects of service delivery including:

- Availability (99.95% v 99.99%)
- Error Correction/Issue Resolution
- User Support
- Service Upgrades/Technology Upgrades

- How is vendor performance measured?
- What remedies are available for service level failures?
- How do customers obtain the remedies?
A customer usually has no control over upgrades and changes in technology as all customers are on a common platform to achieve financial economies of scale.

These changes may have an unforeseen impact on a customer’s technology systems and their ability to process data from the cloud, business processes and user training and support infrastructure.
Termination Risk

- Customer should ensure it has the following rights upon termination:
  - Immediate return of customer’s data.
  - Vendor’s assistance in customer’s transition to a new vendor including price protection and commitment to a set transition period.
- Since customers become dependent on cloud services, customers should negotiate limitations on the vendor’s termination rights if possible.
Transaction Preparation: Identify Risks that Affect Customer

- Will the vendor have access to personally identifiable information? Customer’s confidential information?
- With what regulatory obligations must the customer comply?
- What is the customer’s need for service availability (e.g., 24 x 7, 5 x 8)?
- How many business processes will the cloud service affect?
- How difficult will it be to replace the service when the agreement terminates (e.g., availability other similar services; costs of data conversion)?
- What is the cost of the service (will the vendor be motivated to negotiate)?
Evaluate the vendor’s reliability:

• Financial stability

• Cloud service provider experience

• Reputation among existing customers
Transaction Preparation: Prepare to manage the risks

Identify steps a vendor takes to minimize risks or help customers manage them by examining the vendor’s:

• Privacy and data security policies
• Recurring backup processes
• Geo-redundant backup locations
• Litigation hold response capability
• Limits on vendor subcontracting
• Service levels and remedies
• Disaster recovery/business continuity policy
Transaction Preparation: Prepare to manage the risks

Determine the extent to which the customer can manage the risks through the cloud services agreement:

- Agreement format-- Negotiation vs. “I Agree”:
  - Clickwrap
  - Clickwrap with manually signed amendment
  - Full markup of vendor’s form agreement
  - Customer’s agreement

- Negotiate the cloud computing services agreement, to the extent possible, to manage the risks that the cloud service creates.
Important Issues to Consider
Issue 1: What are a customer’s obligations regarding personally identifiable information it uploads to the cloud?

The SAME as customer’s obligations regarding personally identifiable information that remains in facilities owned or controlled by the customer:

- **Due diligence (always):**
  - what customer information will go to the cloud?
  - what are customer’s contractual obligations, if any?
  - what are customer’s statutory (primary examples)?
    - HIPAA/HITECH (privacy and security of medical and health info)
    - Gramm-Leach-Bliley (privacy and security of financial info)
    - FERPA (privacy of education info)
    - PCIDSS (privacy and security of payment card info)
    - FTC (privacy and security of info collected online)
    - State laws (privacy and security of personal info about state residents)
Issue 2: How should a prospective customer evaluate data security risks in a cloud transaction?

• **Due diligence always:**
  - request, review and evaluate the service provider’s:
    - ✓ data backup and archive policies
    - ✓ data retention policy
    - ✓ privacy and data security policy
  - Compare the service provider’s policies with the customer’s own policy and procedures for data processed and stored at customer-controlled facilities

• **Contract when possible:**
  - appropriate obligations:
    - ✓ commercially reasonable efforts
    - ✓ SSAE 16 audits
    - ✓ ISO 27001 certification
  - appropriate remedies:
    - ✓ notification
    - ✓ credit reporting services
    - ✓ call center services
    - ✓ fines and penalties
Issue 3: Why should a customer know where its data will be processed and stored, and by whom?

- Data stored in a jurisdiction different from the customer’s jurisdiction may be subject to:
  - privacy and data security laws in the storage jurisdiction that may be different from, and perhaps inconsistent with, laws in the customer’s jurisdiction
  - access and examination by the government of the storage jurisdiction
- Movement of customer data to a jurisdiction other than the customer’s jurisdiction may violate export laws in the customer’s jurisdiction
- Data processed or stored by a subcontractor of the service provider may not have the same privacy and data security protections
Issue 4: What are a customer’s e-discovery obligations and how can a customer perform those obligations when its data is in the cloud?

- **Obligations**: preserve data and metadata
- **Due diligence always**:
  - identify the format in which the service provider stores data and the procedures for downloading all of customer’s data
  - request, review and evaluate the provider’s e-discovery policy and procedures:
    - compare the provider’s policies and procedures with the customer’s own policy and procedures for data processed and stored at customer controlled facilities
  - Contract when possible:
    - appropriate e-discovery support (at customer’s expense)
Issue 5: What are the purposes of service levels and how should service level provisions be evaluated?

• **Purpose:**
  Identify standards for performance of cloud services that meet the customer’s reasonable needs (always availability—usually 99.9% or higher; sometimes others) and incentives for the service provider to satisfy the standards.

• **Due diligence (always):**
  - What are the customer’s reasonable needs? (mission-critical service or not?)
  - What service levels does the contract offer? (availability? error correction? customer support?)
  - How is performance calculated?
  - Is performance reported? How frequently?
  - What is the remedy for performance failure and how is it calculated?
Issue 6: When should a party be permitted to terminate a cloud computing agreement?

- **Customer:**
  - for breach by service provider
  - for convenience? with a termination fee?
  - for *force majeure* affecting service provider?
  - for change in control of service provider?

- **Service Provider:**
  - for breach by customer?
  - for convenience?
  - for *force majeure* affecting customer?

- **Termination Assistance**
  - fees
  - duration
  - exceptions
Issue 7: How should a customer evaluate a cloud service provider’s force majeure clause?

- Are specified force majeure events appropriate (e.g., power failure for an IT services provider)?
- Are specified events impacted by other obligations of the affected party (e.g., disaster recovery, business continuity)?
- Does the affected party have any consequent obligations?
  - notification
  - mitigation
- Does the other party have a termination right?
Issue 8: What implementation services are customary in cloud computing transactions?

- **Interface development** (technology that allows the customer to transfer data back and forth between the cloud service and technology at one or more customer-controlled facilities and/or other cloud services)
- **Data conversion** (modification of the data structure for use with the service provider’s technology; if so, is the service provider’s data structure proprietary and confidential?)
- **Configuration** (selection between alternative functionalities and capabilities already existing within the service provider’s offering)
- **Customization** (development of new functionality and capability for the service provider’s offering)

Critical issues: time, cost, acceptance procedure
H. Ward Classen

Ward is Deputy General Counsel of Computer Sciences Corporation, a $15B NYSE listed technology company with approximately 93,000 employees in 80 countries throughout the world. He is the author of *A Practical Guide to Software Licensing for Licensees and Licensors* published by the American Bar Association (5th ed. 2013). Contact Ward:

- by telephone at 410.691.6586, or
- by e-mail at ward.classen@gmail.com
Questions?