Cloud Computing 201: Key Issues and Practical Guidance for Negotiating Cloud Contracts

Janet Stiven  
Vice President & General Counsel  
Moody Bible Institute  
+1 312 329 4123  
janet.stiven@moody.edu

Ed Paddock  
Senior Counsel, Data & Technology Practice Group  
McDonald's Corporation  
+1 630 623 2547  
edward.paddock@us.mcd.com

Mark Irving  
Senior Counsel, Corporate and Securities  
Thomson Reuters  
+1 617 856 1045  
mark.irving@thomsonreuters.com

Joe Pennell  
Partner, Business & Technology Sourcing Group  
Mayer Brown  
+1 312 701 8354  
jpennell@mayerbrown.com
Overview/Agenda

• Key Issues
• Contract Language Examples
• Range of Outcomes
Key Issues for Cloud Customers

- Audit and Security Standards
- Data Breach
- Data Ownership and Use Rights
- Limitations of Liability
- Indemnities

- Service Level Agreements (SLAs)
- Termination, Exit Rights, and Data Portability
- Identifying all Contract Documents
Audit and Security Standards

a. Determine what standards are appropriate for the customer’s business

b. Address plan for ongoing assessment and scope of monitoring of Provider during term of contract
Recognized audit and security standards include:
a. Service Organization Controls (SOC) reports:
   i. SOC 1/SSAE 16/ISAE 3402 (formerly SAS70)
   ii. SOC 2
   iii. SOC 3
b. ISO 27001
c. Sarbanes–Oxley Act of 2002
d. PCI DSS
e. HIPAA
f. FedRAMP
g. CSA
Audit and Security Standards – SOC 1 and SOC 2 Reports

SOC 2 Report

a. Detailed report for Provider’s customers and business partners

b. Focus is evaluation of non-financial internal controls relative to five trust services principals (Security, Availability, Confidentiality, Processing Integrity, Privacy)

c. Utilizes AT Section 101 professional standard (not SSAE 16)

d. **Note** SOC 1 and SOC 2 both utilize Type 1 and Type 2 reports:
   
i. Type 1 reports involve limited testing to validate the existence of controls
   
ii. Type 2 reports involve extensive testing on the effectiveness of controls
Audit and Security Standards – SOC 3 Reports

SOC 3 Report

a. Short report for marketing purposes
b. Simpler version of SOC 2 with very little testing
c. Details not disclosed
d. Permits Providers to obtain certification seal
ISO 27001:2013 is a security management standard that specifies security management best practices and comprehensive security controls following the ISO 27002 best practice guidance. This is a widely-recognized international security standard.

Certification in the standard requires:

a. Systematic evaluation of information security risks, taking into account the impact of threats to and vulnerabilities of Provider
b. Design and implementation of comprehensive information security controls and other forms of risk management to address Provider and architecture security risks
c. Adoption of an enterprise management process to ensure that the information security controls meet ongoing information security standards
Audit and Security Standards – US Regulations and Standards

A number of US regulations contain provisions relating to the storage, protection, or transfer of data and require that the relevant data and/or operations be auditable. Examples include:

a. Sarbanes–Oxley Act of 2002 (SOX), Pub. L. 107-204. This applies to public companies and contains provisions related to e-mail retention, data security and integrity, and oversight — all of which must be considered when using cloud services.

b. Payment Card Industry Data Security Standard (PCI DSS). These are requirements for payment account data security, containing specific requirements related to security management, policies, and procedures.


d. Federal Risk and Authorization Management Program (FedRAMP). Government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
Cloud Security Alliance – some tools:

a. Cloud Controls Matrix (CCM)
b. Consensus Assessments Initiative Questionnaire
c. Cloud Trust Protocol
d. Cloud Audit
"Audit Rights

Customer may audit [Provider]’s compliance with the terms of the Agreement and this Data Processing Agreement up to once per year. Customer may perform more frequent audits of the Cloud Service computer systems that Process Personal Data to the extent required by laws applicable to Customer. If a third party is to conduct the audit, the third party must be mutually agreed to by Customer and [Provider] and must execute a written confidentiality agreement acceptable to [Provider] before conducting the audit.

To request an audit, Customer must submit a detailed audit plan at least two weeks in advance of the proposed audit date to [Provider] Corporation’s Global Information Security organization (“GIS”) describing the proposed scope, duration, and start date of the audit. [Provider] will review the audit plan and provide Customer with any concerns or questions (for example, any request for information that could compromise [Provider] security, privacy, employment or other relevant policies). [Provider] will work cooperatively with Customer to agree on a final audit plan. If the requested audit scope is addressed in a SSAE 16/ISAE 3402 Type 2, ISO, NIST, PCI DSS, HIPAA or similar audit report performed by a qualified third party auditor within the prior twelve months and [Provider] confirms there are no known material changes in the controls audited, Customer agrees to accept those findings in lieu of requesting an audit of the controls covered by the report.
The audit must be conducted during regular business hours at the applicable facility, subject to [Provider] policies, and may not unreasonably interfere with [Provider] business activities.

Customer will provide GIS any audit reports generated in connection with any audit under this section, unless prohibited by law. Customer may use the audit reports only for the purposes of meeting its regulatory audit requirements and/or confirming compliance with the requirements of the Agreement and this Data Processing Agreement. The audit reports are Confidential Information of the parties under the terms of the Agreement.

Any audits are at the Customer's expense. Any request for [Provider] to provide assistance with an audit is considered a separate service if such audit assistance requires the use of resources different from or in addition to those required for the provision of the Cloud Services. [Provider] will seek the Customer's written approval and agreement to pay any related fees before performing such audit assistance.”
Data Breach Notification (Overview)

a. Specific breach notification sections

b. Traditional “Confidential Information” sections
Data Breach Notification Considerations

a. Trigger of notification obligation
b. Timing of notification
   i. When is a provider required to notify customer?
   ii. When does the clock start ticking for a customer to notify data subjects?
c. Responsibility for breach-related activities – Who sends notifications and receives inquiries?
d. Control of communications – Do the parties have duties to coordinate their public responses?
e. Liability for costs
f. Breach preparedness activities
Data Breach – Common Breach-Related Activities and Damages

a. Forensic investigations
b. Out-bound communication (e.g., notification letters)
c. In-bound communication (e.g., call center staffing)
d. Credit monitoring for affected person
e. PR/crisis communications
f. Lost profits
g. Brand reputation
h. Third party claims
Data Breach – Common Strategies

a. Carve-out to qualitative LOL
b. Carve-out to quantitative LOL
c. Defining certain damages as direct damages
d. Right to terminate - Termination without penalty regardless of fault
Data Breach – Example (Traditional Confidential Information Provision)

Example:
Security of Confidential Information. Neither Party shall disclose to any third party during or after the Term and each Party shall keep strictly confidential all Confidential Information of the other, protecting the confidentiality thereof with the same level of efforts that it employs to protect the confidentiality of its own proprietary and confidential information of like importance to it and in any event, by reasonable means. Each party agrees to give notice to the other party immediately after determining that a disclosure of Confidential Information has occurred in violation of this Agreement.

Some concerns:
• Does the definition of “Confidential Information” include customer data?
  o e.g., one-way confidentiality?
  o e.g., personal data is publicly known?
  o e.g., explicit marking requirement?
• “immediately after determining” → “upon having reason to suspect that”
• “disclosure” → “disclosure or use”
Data Breach – Example (Specific Breach Notification Provision)

Notification of Unauthorized Use. In the event that Vendor determines that a Security Breach has occurred, Vendor shall inform Customer within three business days of Security Breach. Vendor will provide Customer with a description of the Security Breach and any other information Customer may reasonably request. Vendor and Customer shall coordinate in good faith on developing any required notices for individuals affected by the Security Breach. “Security Breach” means any unauthorized access or use of Customer’s personal data located on Vendor’s systems and for which notification is required by law.

Some concerns:
- “within three business days” → when does Customer’s clock start ticking for notification?
- “shall coordinate in good faith” → Right to review and approve communications?
- “located on Vendor’s systems” → in-transit?
- “for which notification is required by law” → User IDs? IP addresses?
Data Breach – Potential Traps for Removing Liability

a. Customer’s data ownership
b. Customer’s security obligations
c. Data back-up
All Customer Data submitted by Customer to Vendor, will remain the sole property of Customer. Customer will be solely responsible for the accuracy, quality, integrity, and availability of the Customer Data. Vendor shall only use the Customer Data for the purpose of providing the Services to Customer. Vendor will use commercially reasonable security measures to protect Customer Data against unauthorized disclosure or use.
Customer is responsible for adding authorized users to its account, for maintaining the confidentiality of all account passwords, for ensuring that each account password is used only by the authorized user, for ensuring that accounts and passwords are not shared, and for maintaining the security of its account and of the equipment needed to connect to, access or use the SaaS and the Connected Services. Customer shall limit access to the Services only to authorized persons.
The Services are not intended to replace the need for Customer to maintain regular data back-ups or redundant data archives. VENDOR WILL HAVE NO LIABILITY FOR LOSS OR RECOVERY OF DATA OR PROGRAMS or loss of use of system(s) arising out of the Services.
Data Ownership and Use Rights

Data Ownership

• Don’t assume that you maintain ownership of the data simply because you’re the one that put it in the cloud to begin with

• Read the terms of service to see if you retain ownership of your data

• Avoid cloud contract provisions that allow the provider to maintain flexibility to change those terms and conditions without your approval
Data Ownership and Use Rights

Data Insights

• Review contract templates and standards to protect your interests in data and insights and to guard against value leakage
• Value may be generated in a form that is not protected by traditional contract clauses
• For example:
  • Designate your data as trade secret and as Confidential Information and as Customer Data
  • Remove, narrow, or apply royalty rates to exceptions such as:
    • Secondary use of your data
    • Use “to improve our services”
    • Use of “anonymized” data or data consolidated across customers
"Customer Data" means, other than Resultant Data, information, data and other content, in any form or medium, that is collected, downloaded or otherwise received, directly or indirectly from Customer or an Authorized User by or through the Services.

"Resultant Data" means information, data and other content that is derived by or through the Services from processing Customer Data and is sufficiently different from such Customer Data that such Customer Data cannot be reverse engineered or otherwise identified from the inspection, analysis or further processing of such information, data or content.

vs.

Get the SciTech Edge...
"Customer Data" means any and all information, data, materials, works, expressions or other content, including any that are (a) uploaded, submitted, posted, transferred, transmitted or otherwise provided or made available by or on behalf of Customer or any Authorized User for Processing by or through the Hosted Services, or (b) collected, downloaded or otherwise received by Provider or the Hosted Services for Customer or any Authorized User pursuant to this Agreement or any Service Order or at the written request or instruction of Customer or such Authorized User. All output, copies, reproductions, improvements, modifications, adaptations, translations and other derivative works of, based on, derived from or otherwise using any Customer Data are themselves also Customer Data.
Limitations of Liability – Issue Explanation

a. Limit or alter by agreement the measure of damages otherwise available under the law
b. Part of an integrated risk allocation system that includes:
   i. Indemnification provisions
   ii. Consequential damages provisions
   iii. Contractual caps on liabilities
   iv. Representations and warranties of the parties, including disclaimers, exclusions and limitations
   v. Contractual statutes of limitation
   vi. Insurance
c. Identify and rate the materiality of the risks
d. Classifying data helps in assessing and mitigating risks
a. Identify what business asset will be placed in the cloud (i.e., data, application, function, process)
b. Evaluate the asset: How would the business be harmed or impacted if:
   i. The data became widely public and distributed?
   ii. The Provider accessed the data?
   iii. The data or function were manipulated by an outsider?
   iv. The function failed to provide expected results?
   v. The data were unexpectedly changed?
   vi. The data or function were unavailable?
Limitations of Liability – Analyzing the Provisions

a. Analyze limitation of liability provisions carefully

b. Consider the following:
   i. Mutual protection
   ii. Appropriate carve-outs (e.g., confidentiality, data security, indemnity, IP infringement, data loss)
   iii. A financial cap for direct damages
   iv. Exclusion of certain types of loss (e.g., indirect loss and/or data loss) and causes;
   v. Exclusion of liability for downtime
“Disclaimers and Limitation of Liability

a. While [Provider] makes reasonable efforts to provide the Service continuously, it does not guarantee such service. The Service will be interrupted on occasion for planned and unscheduled maintenance, without notice to [Customer]. The Service is provided AS-IS and AS-AVAILABLE. [PROVIDER] DOES NOT WARRANT THAT THE SERVICE WILL BE AVAILABLE AT ANY TIME NOR THAT ANY TEXT MESSAGE WILL BE DELIVERED.

b. [PROVIDER] SPECIFICALLY DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, REGARDING THE SERVICE INCLUDING ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

c. [Provider] disclaims all liability arising from any action or omission of any third party providing hardware, software, networking, storage, or other technology required to run the Service.

d. In no event will [PROVIDER] be liable for any incidental, consequential, or punitive damages of [Customer], User, or [Customer’s customer], regardless of the form of action or claim by [Customer] or User.”
“LIMITATION OF LIABILITY

NEITHER PARTY SHALL BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, OR ANY LOSS OF REVENUE OR PROFITS (EXCLUDING FEES UNDER THIS AGREEMENT), DATA, OR DATA USE. [PROVIDER]’S AGGREGATE LIABILITY FOR ALL DAMAGES ARISING OUT OF OR RELATED TO THIS AGREEMENT OR YOUR ORDER, WHETHER IN CONTRACT OR TORT, OR OTHERWISE, SHALL BE LIMITED TO THE TOTAL AMOUNTS ACTUALLY PAID TO [PROVIDER] FOR THE SERVICES UNDER THE ORDER GIVING RISE TO THE LIABILITY IN THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO SUCH LIABILITY LESS ANY REFUNDS OR CREDITS RECEIVED BY YOU FROM [PROVIDER] UNDER SUCH ORDER.”
“LIMITATION OF LIABILITY. EXCEPT AS SET FORTH IN THIS SECTION 10 TO THE EXTENT PERMITTED BY LAW, IN NO EVENT SHALL [PROVIDER] OR CUSTOMER BE LIABLE FOR SPECIAL, INCIDENTAL, CONSEQUENTIAL OR PUNITIVE DAMAGES OR LOST PROFITS IN ANY WAY RELATING TO THIS AGREEMENT. IN NO EVENT SHALL [PROVIDER]’S OR CUSTOMER’S AGGREGATE, CUMULATIVE LIABILITY IN ANY WAY RELATING TO THIS AGREEMENT EXCEED THE AMOUNT OF FEES ACTUALLY RECEIVED BY [PROVIDER] FROM CUSTOMER DURING THE TWELVE (12) MONTHS PRECEDING THE CLAIM. THE FOREGOING LIMITATIONS SHALL NOT APPLY TO PAYMENT, CONFIDENTIALITY AND INDEMNITY OBLIGATIONS, OR CLAIMS OF MISAPPROPRIATION OF INTELLECTUAL PROPERTY. THE PARTIES WOULD NOT HAVE ENTERED INTO THIS AGREEMENT BUT FOR SUCH LIMITATIONS.”
“WARRANTIES, DISCLAIMERS AND EXCLUSIVE REMEDIES

“[PROVIDER] DOES NOT GUARANTEE THAT (A) THE SERVICES WILL BE PERFORMED ERROR-FREE OR UNINTERRUPTED, OR THAT [PROVIDER] WILL CORRECT ALL SERVICES ERRORS, (B) THE SERVICES WILL OperATE IN COMBINATION WITH YOUR CONTENT OR YOUR APPLICATIONS, OR WITH ANY OTHER HARDWARE, SOFTWARE, SYSTEMS, SERVICES OR DATA NOT PROVIDED BY [PROVIDER], AND (C) THE SERVICES WILL MEET YOUR REQUIREMENTS, SPECIFICATIONS OR EXPECTATIONS. YOU ACKNOWLEDGE THAT [PROVIDER] DOES NOT CONTROL THE TRANSFER OF DATA OVER COMMUNICATIONS FACILITIES, INCLUDING THE INTERNET, AND THAT THE SERVICES MAY BE SUBJECT TO LIMITATIONS, DELAYS, AND OTHER PROBLEMS INHERENT IN THE USE OF SUCH COMMUNICATIONS FACILITIES. [PROVIDER] IS NOT RESPONSIBLE FOR ANY DELAYS, DELIVERY FAILURES, OR OTHER DAMAGE RESULTING FROM SUCH PROBLEMS. [PROVIDER] IS NOT RESPONSIBLE FOR ANY ISSUES RELATED TO THE PERFORMANCE, OPERATION OR SECURITY OF THE SERVICES THAT ARISE FROM YOUR CONTENT, YOUR APPLICATIONS OR THIRD PARTY CONTENT.


“TO THE EXTENT NOT PROHIBITED BY LAW, THESE WARRANTIES ARE EXCLUSIVE AND THERE ARE NO OTHER EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS INCLUDING FOR SOFTWARE, HARDWARE, SYSTEMS, NETWORKS OR ENVIRONMENTS OR FOR MERCHANTABILITY, SATISFACTORY QUALITY AND FITNESS FOR A PARTICULAR PURPOSE.”
Limitations of Liability – Consequential Damages Limitations

a. Limitation on consequential damages for commercial losses between contracting business entities is enforceable

b. Must coordinate any exclusion under the indemnification clause with any general consequential damages exclusion clause

c. An indemnification clause covering “any and all claims, damages and losses” can be deemed to include consequential damages incurred by the indemnitee or third party claimant, unless such damages are expressly excluded from the indemnified claims

d. Determine whether third party claims representing consequential damages are to be excluded from indemnification provision
Indemnity – Issue Explanation

a. Critical area to negotiate to ensure that risk is properly allocated
b. Consider the type of cloud services being provided and the information being stored
c. In particular, as a customer, you are looking for protection from claims related to:
   i. The provider's breach of its confidentiality or data security obligations.
   ii. Any authorized use of the services that infringes a third party's IP rights.
d. Be on the lookout for limits on indemnification:
   i. Costs finally awarded by a court.
   ii. Only IP infringement in limited jurisdictions (e.g., U.S. only).
Indemnity – Issue Explanation (Continued)

a. Be aware that the Provider may also look for indemnification related to:
   i. Confidentiality/Data Protection
   ii. IP Infringement
   iii. Illegal Content

b. Other market sectors
   i. Any rules specifically applicable to the sector in which the services are being provided.

c. Consider additional representations and warranties.
IP Indemnity – Examples

Proprietary Rights Indemnification. Provider agrees to indemnify, defend and hold Indemnitees harmless from and against any and all [third party] Claims that may be suffered by any Indemnitee and that allege the Services infringe or misappropriate any United States [or foreign] patent, copyright, trade secret, trademark or other proprietary right. If Provider is enjoined from delivering the Services to Customer, the Services and such injunction is not dissolved within thirty (30) days, or in the event that Customer is adjudged, in any final order of a court of competent jurisdiction from which no appeal is taken, to have infringed upon or misappropriated any patent, copyright, trade secret, trademark or other proprietary right in the use of the Services, then Provider shall, at its expense: (a) obtain for Customer the right to continue using such Services; (b) replace or modify such Services so that it does not infringe upon or misappropriate such proprietary right and is free to be delivered to and used by Customer; or (c) in the event that Provider is unable or determines, in its reasonable judgment, that it is commercially unreasonable to do either of the aforementioned, Provider shall refund to Customer any prepaid fees for the Services that were to be provided after the effective date of such injunction or order.
General Indemnity. Provider agrees to indemnify, defend, and hold the Customer Indemnitees harmless from and against any and all [third party] Claims that may be suffered by, any Customer Indemnitee and that arise out of [any act or omission of Service Provider in connection with its performance under this Agreement, including without limitation, Claims arising out of]:

(a) death or bodily injury
(c) property damage [to the extent arising out of Service Provider’s negligence or breach of this Agreement];
(d) fraud, willful misconduct, gross negligence, or criminal acts; or,
(e) breaches of [any representation, warranty, or covenant under this Agreement] or [key provisions related to Provider’s compliance with applicable laws, viruses/malicious or disabling code, etc.].
a. Service Level Agreements (SLAs) = targets by which to measure the performance of the service

b. Some solutions can offer higher SLA targets (often priced in); others offer SLAs on a take-it or leave-it basis (because their SLAs are standardized for all clients)

c. Meant to incentivize the vendor’s performance vs. compensation for inadequate performance

d. Credits are the key to meaningful SLAs

e. Someone has to monitor
Service Level Agreements – Most Common Types of SLAs

I. Two most common SLAs for Saas:
   a. Service desk – response and resolution time
   b. Availability – Expressed as percentage (excluding permitted downtime)

II. Some other SLAs:
   a. Performance
   b. Security
   c. RPO/RTO
Service Level Agreements – Support/Service Desk (Overview)

a. Response time – How quickly the Vendor acknowledges the problem

b. Resolution time – How quickly the vendor resolves the problem

c. Severity/definitions – A trigger for different response/resolution times

d. Hours of operation – The hours during which the SLA is counted

e. Measurement – Generally expressed as an average across a period of time
Vendor will use **commercially reasonable efforts** to provide support to Customer comprised of (i) on-line access to the Vendor support portal generally available twenty-four (24) hours a day, seven (7) days a week **(subject to circumstances outside of Vendor’s control)**; and (ii) Vendor’s telephone support line **(currently 9am-5pm US PT Monday through Friday)**. Vendor will use **commercially reasonable efforts** to respond to Customer’s inability to access the SaaS within eight (8) hours of the Problem being reported by Customer to the Vendor support team through one of the methods identified above.
Some comments:

- Who has right to define severity level?
- Who has right to determine resolution?
- What is mechanism for reporting on tickets?
a. Uptime
   i. 99.9% uptime = 8.76 hours down per year
   ii. 99% uptime = 87 hours down per year
   iii. 98% uptime = 175 hours down per year
   iv. 97% uptime = 262 hours down per year
b. Permitted Downtime / Other Exceptions
Provider shall make the SaaS Available at least **99.5%** (the “Availability Commitment”). “Availability” or “Available” means the time during each calendar month that the SaaS is available for use by Customer. “Downtime” means the time that the SaaS is not Available, but excluding Excused Unavailability. “Excused Unavailability” means: 

(i) **scheduled maintenance** (currently 12:30am US ET Sunday to 3:30am US ET Sunday, or such other alternative time outside of 9:00am US ET through 9:00pm US ET Monday through Friday, **upon notice to Customer**); 
(ii) unavailability caused by acts or omissions of Customer or its agents or caused by any breach by Customer of this Agreement; 
(iii) unavailability caused by network unavailability or bandwidth limitations outside of the Provider network; 
(iv) issues arising from bugs or other problems in the software, firmware or hardware of Provider’s suppliers; 
(v) hacks, malicious introduction of viruses, disabling devices, and other forms of attacks that disrupt access to the SaaS; 
(vi) power outages or other telecommunications or Internet failures; and 
(vii) events outside of Provider’s control.
Credits meant to incentivize performance
• Not an adequate remedy for breach
• Not a “penalty”
• Mechanism for payment needs to be considered
In the event that the Service fails to be available 99.5% in a given month, Provider will tender a credit to Customer in the amount of fifteen percent (15%) of net monthly fees for the applicable services for the month in which the service level violation occurred. The credit will apply only to outstanding amounts owed under future invoices, and the availability of such credit represents Provider’s sole liability and Customer’s exclusive remedy for all service level violations under the Agreement.
Recurring SLA Violations. If Provider fails to meet the Availability Commitment for two (2) consecutive calendar months or fails to meet the Availability Commitment for any three (3) calendar months within any twelve (12) month period, then by notice given within thirty (30) days after the end of the month which triggered Customer’s right of termination, Customer may terminate this Agreement effective thirty (30) days after receipt of the notice, and receive a refund of any pre-paid Fees for periods after the effective date of termination. The provisions of this SLA state Customer’s sole and exclusive remedy for any service level deficiencies of any kind.

Some comments:

• “Customer may terminate” → Is this considered a termination for breach or termination for convenience?
• Sole and exclusive remedy → Other damages?
Service Level Agreements – Other Considerations

a. Reporting – Define agreed upon reporting. What is the point of measurement? Whose reports govern in a dispute?

b. Monitoring – Someone needs to actually read the reports.

c. Deemed failures – For undelivered reports? For poor performance?

d. Advanced concepts:
   i. Burn-in period
   ii. Calculating/capping credits for multiple SLA violations
   iii. Earn backs
Termination/Exit Rights/Data Portability – Issue Explanation

a. Termination Rights
   i. When can you terminate the agreement?
   ii. When can the cloud provider terminate?
   iii. Termination costs?

b. Termination Assistance/Data Portability
   i. Agree to assistance pricing for a period pre- and post-termination
   ii. What are provider’s obligations to return your data?
   iii. What format will they return your data in?
   iv. How long do they have to return your data?
Upon any expiration or termination of the Agreement, Provider shall, upon Customer’s request, continue to provide the Service to Customer pursuant to the terms of this Agreement for a transitional period of up to [twelve (12)] months (the “Transition Period”). Services during the Transition Period will be subject to the fees set out in the applicable Service Order(s), prorated on a monthly basis and payable in advance, based on the annual fees charged to Customer for the Services during the six (6) month period immediately preceding the termination date. During the applicable Transition Period, Provider will provide cooperation and assistance as Customer may reasonably request to support an orderly transition to another provider of similar software or services, or to Customer’s internal operations.

Upon request by Customer made within thirty (30) days after any expiration or termination of this Agreement (including any Transition Period), Provider will make Customer Data available to Customer or such other provider in [a format reasonably specified by Customer] OR [specific format you want to designate] OR [in an industry-standard, platform agnostic format], on a limited basis solely for purposes of Customer or such other provider retrieving Customer Data for a period of up to sixty (60) days after such request is received by Provider.
Identifying all Contract Documents

a. At Customer's option and upon its written request, all or some portion of a SaaS agreement may be located on the internet.
b. As a result, the contract may not be “fixed” (i.e., it may change at any time and the Provider may not provide notice).
c. Customer should make every effort to “fix” the contract in one document.
d. Attach as exhibit(s) to contract copies of all online portions of the contract.
e. Add language to the contract making clear that any future changes in those elements must not (i) materially decrease the level of data protection, service support, or SaaS performance existing as of the effective date; and (ii) impose any materially new or different obligations on the customer.
f. Provider should also be required to provide notice to customer of any changes to the agreement.
g. Include a termination right in the event a later change materially decreases the level of data protection, service support, SaaS performance, etc., existing as of the effective date.
Other Key Issues

a. European General Data Protection Regulation (GDPR)
b. Safe Harbor / Privacy Shield
c. Subcontracting and flow-down of provisions
d. Electronic discovery issues
e. Record retention issues
f. Government seizure / requests
g. Disaster recovery and business continuity
h. Financial stability of providers / due diligence
i. Export control issues
j. Compliance with laws
k. Force majeure (e.g., impact to SLAs and indemnification)
Questions?

Janet Stiven  
Vice President & General Counsel  
Moody Bible Institute  
+1 312 329 4123  
janet.stiven@moody.edu

Ed Paddock  
Senior Counsel, Data & Technology Practice Group  
McDonald’s Corporation  
+1 630 623 2547  
edward.paddock@us.mcd.com

Mark Irving  
Senior Counsel, Corporate and Securities  
Thomson Reuters  
+1 617 856 1045  
mark.irving@thomsonreuters.com

Joe Pennell  
Partner, Business & Technology Sourcing Group  
Mayer Brown  
+1 312 701 8354  
jpennell@mayerbrown.com
Poll Question

Is your organization a (SELECT ONE):

1. **Cloud Watcher** (organization that is developing cloud strategies and plans but has not yet deployed applications into the cloud)

2. **Cloud Beginner** (organization that is new to cloud computing and working on proofs-of-concept or initial cloud projects.)

3. **Cloud Explorer** (organization with multiple projects or applications already deployed in the cloud and focused on improving and expanding its use of cloud resources)

4. **Cloud Focused** (organization that is heavily using cloud infrastructure and is looking to optimize cloud operations as well as cloud costs)
Poll Question

What type of cloud solution does your organization most frequently use:

a. Public
b. Private
c. Hybrid
Poll Question

What is your biggest challenge in the cloud? (SELECT ONE):

- Security
- Compliance
- Managing cloud services costs
- Operational (e.g., problems integrating with other systems/services, lack of resources/expertise)
- Governance/control
- Trying to keep your business clients from using a company credit card to buy cloud services under standard terms and conditions (without any legal review).