Transactions in the Cloud: A User's Guide

Presented By:
Kemal Hawa and Emily Naughton of Greenberg Traurig, LLP
and Amber Lester of CyrusOne, Inc.

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

PART I

CLOUD SERVICES 101

WHAT IS THE CLOUD?

- The “Cloud” consists of a physical network of data centers, equipment, fiber optic cable infrastructure, and submarine cable systems, interconnected globally
- Data centers are the heart of the Cloud
  - Data centers are secure buildings containing racks/cabinets of servers for data storage
  - Data centers can be large hub sites, or can be smaller edge sites located closer to the end user
- Data centers are connected by telecommunications and broadband networks

CLOUD PROCUREMENT

- Cloud technology is central to most business operations today
- Cloud contracts are first and foremost about procuring performance at specified levels
  - Of course, the standard legal protections are also addressed
- To ensure performance, one must have a basic understanding of Cloud technology
  - Different types of agreements can be used depending on the services provided
  - Pricing, performance metrics and remedies for failure to meet performance standards vary depending on the services provided and the customer’s business needs

CLOUD-BASED SERVICES

- IaaS (Infrastructure as a Service)
  - Storage and retrieval, disaster recovery, virtual equipment, firewalls, etc.
- SaaS (Software as a Service)
  - Delivery of software centrally hosted on the Cloud, e.g., O365, Salesforce, security software
- PaaS (Platform as a Service)
  - Provision of networks, servers, storage, applications, and other services that are required to support or host the user's application
  - The user creates customized software using the Cloud platform

TYPES OF CLOUD OFFERINGS

> Public Cloud

- Involves shared servers owned and operated by a third party
- Primary benefits are scalability and the ability to pay only for servers utilized

> Private Cloud

- Involves dedicated servers typically housed in a data center, but can also be hosted on premises
- Primary benefits are control, customization and security

> Hybrid Cloud

- Simply a combination of the features of public and private Cloud, e.g., the utilization of public Cloud for non-sensitive applications, and private Cloud for mission critical and sensitive items

DATA CENTER CAPACITY PROCUREMENT

- End users enter into data center leases, licenses, and services agreements directly with data center operators
  - For space and power (retail colocation)
  - For managed services (essentially retail colocation with more services)
- End users procure data center capacity from Cloud providers (such as Microsoft, AWS, and Google)
- End users enter into agreements with OTTs (over-the-top) providers (such as Netflix, Hulu, Apple TV/iTunes) to procure services such as streaming video and other content
  - OTTs, in turn, lease capacity from data center operators
  - Many OTTs partner with Cloud providers; many Cloud providers are OTTs

DATA CENTER SALE LEASEBACKS

- Large enterprise customers with cumbersome IT infrastructure footprints are increasingly selling their data centers to data center operators and leasing back space within those data centers
- Key benefits to seller:
  - Seller can remain in the data center and continue its operations without interruption
  - Opportunity for seller to gradually reduce its footprint at the property
  - Allows seller to pass operational responsibility for the data center to a buyer that is in the business of operating data centers
  - Access to cash from the sale of the property, which can then be used to improve seller’s balance sheet or invest in new business
- Key benefit to buyer:
  - Acquires an asset that has a long-term lease with steady revenue

PART II

KEY ISSUES IN NEGOTIATING CLOUD CONTRACTS

QUESTIONS TO CONSIDER BEFORE NEGOTIATING A CLOUD CONTRACT

- What goods and services are being provided?
- How will the goods and services be used?
- How critical are the goods and services to your business?
- What data is implicated?
  - Data Security and Compliance
  - Data Loss Tolerance
- Are there any downstream considerations or contingencies?
  - Internal Use Only
  - Integration into an External Product or Service
- Who is the provider?
  - A well written contract is no substitute for adequate diligence

PRICING

- Wholesale and retail data center contracts are priced based on power (in kilowatts)
  - Retail customers generally pay for power on a per-circuit basis, irrespective of utilization
  - Wholesale customers typically have separately metered power
  - Cloud contracts have all-inclusive service fees
- The line between when it makes economic sense to enter into a wholesale or retail data center contract or a Cloud contract is blurring
  - End users are requiring many of the same rights and services under each type of contract

SERVICE LEVELS AND CREDITS

- Service level agreements (SLAs) are critical
  - Power, temperature, humidity and security are most common in data center contracts
  - Service availability and connectivity are most common in Cloud contracts
- Credits are intended to incentivize the provider to perform, and not to make the customer whole
  - For example, if a retailer loses service for an hour, it will incur significant business losses, but SLA credits will only offset a small amount of such losses
  - Providers seek exclusions from payment of credits and caps on credits

EXAMPLES OF SERVICE LEVEL AGREEMENTS

Section 1. Service Levels and Service Credits. In the event Supplier fails to achieve a Service Level set forth below in any given calendar month during the applicable Service Term (but in all cases subject to the exclusions set forth in **Section 2 (Exclusions)** below), Customer may claim the Service Credit corresponding to the applicable failure (as set forth in the table below) by providing Supplier with a written request for such Service Credit within thirty (30) days after receipt of an invoice from Supplier for the period in which the Service Level was not achieved. Supplier's records and data shall be the basis for all Service Level calculations and determinations. Service Credits are Customer's sole and exclusive remedy and Supplier's sole and exclusive liability under the Agreement with respect to any deficiencies, interruptions or failures with respect to the Services. Service Credits shall not have any cash value at the end of the Service Term or otherwise. Unless otherwise stated in the table below, Service Credits are calculated based on the total MRC paid by Customer that is (a) attributed to use of the Colocation Space with respect to which the Service Level failure occurred and (b) the calendar month in which such Service Level failure occurred ("**SLA Credit Baseline**"). Notwithstanding anything to the contrary, the maximum amount of Service Credits in any calendar month under the SLA shall not exceed fifteen percent (15%) of the SLA Credit Baseline. If Customer is in multiple Colocation Spaces, Service Credits are calculated on a space-by-space basis such that a Service Credit shall be given only for a failure in the particular Colocation Space that is the subject of the Service Level failure. For any multiple Service Level event with the same root cause, only the Service Level with the highest Service Credit available shall apply (*i.e.*, multiple Service Credits for the same event will not be given).

EXAMPLES OF SERVICE LEVEL AGREEMENTS (CONT.)

Section 2. Exclusions. For purposes of determining the percentage of availability, stability or other measure for any Service Level under this SLA, the following causes will be excluded from the calculation (*e.g.*, if unavailability or instability are due to any of the causes listed below, such unavailable or unstable time shall be included as “available” or “stable” for purposes of calculating the percentage of availability or stability):

(a) Customer not utilizing or implementing the redundancy components of the infrastructure provided by Supplier including without limitation Customer’s failure to purchase or properly utilize an “A” and “B” power whip to the Power Demarc;

(b) scheduled maintenance during a maintenance window communicated to Customer;

(c) acts or omissions of Customer or its employees, agents, customers, contractors, representatives, or a third party acting at the direction of Customer;

(d) Supplier following or implementing instructions or procedures issued by Customer;

(e) a Force Majeure Event; and

(f) any other exclusions set forth in the Agreement.

EXAMPLES OF SERVICE LEVEL AGREEMENTS (CONT.)

Service Level	Description	Percentage	Service Credit
Power Availability	The power availability SLA shall become effective only once Customer has purchased and is properly utilizing an "A" and "B" power whip to the Power Demarc. The "Power Demarc" is the receptacle at the end of the power whip attached to each Customer power distribution unit or power strip. Supplier will provide power to the Power Demarc ("Power Availability"). Power shall be deemed unavailable if the electricity feeds in both power whips "A" and "B" fail simultaneously, for any amount of time, on the Supplier side of the Power Demarc. Power Availability shall be provided by Supplier to Customer at 100% uptime per month ("Power Availability Service Level"). For purposes of determining whether the Power Availability Service Level has been achieved, the percentage of availability shall be calculated each month during the Service Term as follows: (Total minutes of Power Availability per month) / (Total minutes per month). Customer shall be entitled to a Service Credit as set forth in this Section in the event the Power Availability Service Level is not achieved. The Service Credit is expressed as a percentage of Customer's MRC in a Colocation Space for the month in which the Power Availability Service Level is not achieved.	100%	No Credit
		<100% ≥99.5%	3% of SLA Credit Baseline
		<99.5% ≥99.0%	5% of SLA Credit Baseline
		<99.0 % ≥98.5%	10% of SLA Credit Baseline
		<98.5%	15% of SLA Credit Baseline

EXAMPLES OF SERVICE LEVEL AGREEMENTS (CONT.)

Downtime: Any period of time when [service] applications are put into reduced functionality mode due to an issue with the [service] activation.

> "**Downtime**" is defined for each Service in the Services Specific Terms below. Downtime does not include Scheduled Downtime. Downtime does not include unavailability of a Service due to limitations described below and in the Services Specific Terms.

> "**Scheduled Downtime**" means periods of Downtime related to network, hardware, or Service maintenance or upgrades. We will publish notice or notify you at least five (5) days prior to the commencement of such Downtime.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{User\ Minutes\ \ - Downtime}{User\ Minutes} x\ 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Monthly Uptime Percentage	Service Credit
<99.9%	25%
<90%	50%

DELIVERY OF SERVICES

- Timely delivery of service is often crucial to end users
  - Late delivery penalties and termination rights for late delivery incentivize providers to deliver services on time
- The migration of equipment and data from an on-premises site to a data center is time consuming
  - Early access rights to set up equipment and conduct testing may alleviate some timing concerns
- The time to migrate out of the facility should be considered when negotiating the term of the contract
  - It is common to negotiate transition assistance and/or a transition period to ensure the seamless migration of services at the end of the term

EXAMPLES OF TERMINATION EXTENSION AND ASSISTANCE

> **Example 1: Termination Extension**

Prior to the expiration or termination of an Order Form, and separate from and in addition to any other extension rights or options provided for herein, Customer may extend the effective date of expiration or termination of such Order Form up to [two (2)] times each for a period of [ninety (90)] days (unless otherwise stated in the applicable Order Form) and, upon at least [sixty (60)] days' advance written notice to Supplier, provided that the total of all such extensions under this Section [XX] shall be no more than [one hundred eighty (180)] additional days from the effective date of termination of such Order Form. Notwithstanding the foregoing, the rights set forth in this Section do not apply in the event of a termination by Supplier for Customer's [breach/default] pursuant to Section [XX].

> **Example 2: Termination Assistance**

(a) During the Termination Assistance Period (defined below) and regardless of the basis for termination, Supplier shall provide, in accordance with the provisions of this Section [__], reasonable assistance to Customer and any third parties reasonably designated by Customer with regard to the winding down of the Services and the transition from Supplier to Customer or another provider. Upon Customer's written request prior to the effective date of termination and subject to subsection (b) below and Customer's continuing payment of the fees for the terminated Services, such assistance includes continuation of the Services during the Termination Assistance Period. The "Termination Assistance Period" is the period of twelve (12) months following the effective date of termination of the affected Services, provided such period does not extend beyond the Service Term then in effect with respect to such terminated Services. Customer may terminate the Termination Assistance Period early upon no less than ninety (90) calendar days' written notice to Supplier.

(b) Any resources that Supplier is required to expend in providing such cooperation or assistance and that are in addition to those resources otherwise provided under the Agreement for the terminated Services shall be chargeable to Customer at Supplier's then-current rates. If Supplier has terminated the Services for Customer's failure to pay undisputed amounts owed to Supplier, Supplier may condition the provision of the termination assistance on (i) payment in full of all outstanding undisputed amounts owed to Supplier and (ii) payment of fees in advance of each month for the provision of assistance during the Termination Assistance Period. Under no circumstances shall Supplier be required to (nor shall Customer) share Confidential Information of Supplier with, nor provide access to a Facility to, any third party that competes with Supplier.

BILLING AND AUDITS

- Billing
  - Customers seek to time bar late billing (e.g. bill invalid if not issued within a certain period after the service is rendered)
    - 90 – 180 days is common
  - Providers seek to time bar customers' ability to dispute invoices – often the timing is tied to the time bar imposed on provider to issue bills
- Audit rights
  - Customers seek the right (often annually) to audit invoices and test facilities and systems to ensure compliance and accuracy
    - The timing of audits and the time limit on disputing invoices must be reconciled
  - Providers often seek to recover the cost of audits from customers

EXAMPLES OF AUDIT PROVISIONS

> **Example 1: Compliance and Supplier Audits**

During the Service Term, Supplier shall maintain (or, if the applicable Facility is a new Facility, implement controls at the Facility necessary to obtain) the industry-standard information technology security assessments or their equivalents for the Facility listed below; provided, that certification for new Facilities will not be maintained until after the first audit cycle for the applicable Facility. Upon request, Supplier shall make available for Customer's review (e.g., onsite at the applicable Facility or via web conference) reasonable documentation demonstrating its assessments and certifications. Subject to Customer's obligations of confidentiality hereunder, Customer may provide such documentation to its End Users, so long as any such End Users are required to sign a Customer confidentiality agreement which contains confidentiality provisions at least as protective as those contained herein:

(a) SSAE 18 SOC 1, Type II or equivalent;

(b) AT 101/SOC 2, Type II or equivalent;

(c) ISO27001 certification;

(d) PCI DSS assessment as Level 1 Supplier validating controls of Section 9 and 12

(e) HIPAA/HITECH assessed as required by colocation providers with regard to physical infrastructure and control to protect electronic protected health information (ePHI);

(f) Federal Information Security Management Act (FISMA) assessed to ensure compliance with the applicable controls from NIST 800-53;

(g) Federal Financial Institutions Examination Council (FFIEC);

(h) CSA Security, Trust and Assurance Registry (CSA STAR); and

(i) The Health Information Trust Alliance (HITRUST) Common Security Framework (CSF).

EXAMPLES OF AUDIT PROVISIONS (CONT.)

- **Example 2: Customer Audits**

During the applicable Service Term, Customer, Customer’s internal and external auditors and any government authority or regulatory agency having jurisdiction over Customer’s business (collectively, “**Auditors**”) may conduct onsite audits of Supplier’s operations, books and records, procedures and practices as reasonably necessary for Customer to verify Supplier’s compliance with the Agreement and, in each case, to the extent applicable to the Services and the Colocation Space at which the Services are delivered. Each such audit shall be conducted during Supplier’s regular business hours for its headquarters office, for a reasonable duration and upon reasonable advance written notice to Supplier. Customer shall not conduct more than one (1) audit per 12-month period, unless Customer’s request is required by a government authority or regulatory agency. Supplier will be responsible for Supplier’s own costs to support audits, while Customer will be responsible for audit expenses incurred by Customer and any Auditors provided, however, that if Customer exceeds one (1) voluntary audit per year (the “**Audit Cap**”), then Customer will reimburse Supplier for reasonable costs associated with any voluntary audits in excess of the Audit Cap as follows: [________________________]. Supplier shall have no obligation to participate in more than [___] audits per year. For clarity, audits conducted in response to a breach of the Agreement and any audit to follow up on issues identified in a previous Audit shall not count toward the Audit Cap. All audits shall be conducted in accordance with Supplier Policies, including its physical access policy and audit policy, and shall be subject to the confidentiality obligations set forth in the Agreement. In no event shall an Auditor include a Supplier competitor nor shall an Auditor have the right to audit any areas or systems used by customers of Supplier (other than Customer), any of the internal cost information comprising Supplier pricing nor any fees that are charged on a fixed-cost basis. ”All audits shall be conducted in accordance with Supplier Policies, including its physical access policy and audit policy, and shall be subject to the confidentiality obligations set forth in the Agreement. In no event shall an Auditor include a Supplier competitor nor shall an Auditor have the right to audit any areas or systems used by customers of Supplier (other than Customer), any of the internal cost information comprising Supplier pricing nor any fees that are charged on a fixed-cost basis. If an operational audit reveals that Supplier is not in material non-compliance with Applicable Law or any term of the Agreement, Supplier shall be responsible for and liable for, at its sole cost and expense, taking all necessary actions necessary to comply with such Applicable Law or term of the Agreement. In addition, if any such audit reveals an overcharge of more than five percent (5%) of the audited Charges in any Charges category, Supplier shall promptly reimburse Customer for the actual cost of such audit.

EXPANSION RIGHTS

- Wholesale and retail customers should diligence whether there is sufficient available space and capacity in the data center to accommodate future growth (this is less of an issue for Cloud)
  - Reservations of space and electrical capacity
    - When growth is likely, customer may reserve space and power (usually adjacent space), frequently for a fee
  - Rights of first refusal
  - Right of first offer
- Providers prefer ROFOs to ROFRs or reservations

EXTENSION AND EARLY TERMINATION RIGHTS

- It is difficult and costly to relocate once deployed
- Rights to extend the term should be considered
  - Providers seek maximum flexibility upon expiration of the term and significant advance notice of a customer's election to extend the term
  - Customers seek to cap price increases upon extension of the term (at a pre-negotiated percentage, at CPI, etc.)
- Early termination fees (ETFs) can often be negotiated
  - A basic ETF is simply a reduced schedule of fees due on termination that is less than monthly fees times the remainder of the term
  - A portability right can result in little or no ETFs, provided that the customer migrates to another location within provider's footprint

REPORTING

- The substance and timing of reports on maintenance and service level compliance should be negotiated
- SLA reporting is particularly important
  - Providers generally require that customer report performance failures if customer seeks an SLA credit
  - Customers seek to have provider issue reports identifying performance failures and offering a credit

ASSIGNMENT AND NON-DISTURBANCE

- Assignment or sale by provider/operator
  - Customers often seek restrictions on provider’s ability to assign to an unqualified operator or to a customer competitor
- Assignment and sublease rights of tenant/customer
  - It is a best practice for customers to negotiate in advance permissible assignees (e.g. a financial wherewithal test)
- Non-disturbance and Attornment
  - Superior interest holders (master landlord, property owner and mortgagees) agree to a direct relationship with customer in the event that provider defaults on underlying agreements
  - Customer also seeks to have superior interest holders agree that they will not remove provider until a successor operator is installed

LIMITATIONS OF LIABILITY

- Liability for damage
  - Liability caps are often tied to contract value or to spend (e.g. trailing twelve month spend)
  - Carveouts are key – they can severely expand or restrict recovery
  - Providers generally seek to exclude liability for damage to customer equipment
    - Insurance requirements and waivers of subrogation heavily negotiated
- Indemnification for privacy and data security breaches and for end user content is always hotly contested
  - This is always challenging because in reality neither provider or customer control end user content and third party malicious conduct

EXAMPLES OF LIMITATION OF LIABILITY PROVISIONS

- **Example 1:**

  Limitation of Liability. IN NO EVENT SHALL THE AGGREGATE LIABILITY OF EACH PARTY TOGETHER WITH ALL OF ITS AFFILIATES ARISING OUT OF OR RELATED TO THIS AGREEMENT EXCEED THE TOTAL AMOUNT PAID BY CUSTOMER AND ITS AFFILIATES HEREUNDER FOR THE SERVICES GIVING RISE TO THE LIABILITY IN THE TWELVE MONTHS PRECEDING THE FIRST INCIDENT OUT OF WHICH THE LIABILITY AROSE. THE FOREGOING LIMITATION WILL APPLY WHETHER AN ACTION IS IN CONTRACT OR TORT AND REGARDLESS OF THE THEORY OF LIABILITY, BUT WILL NOT LIMIT CUSTOMER'S AND ITS AFFILIATES' PAYMENT OBLIGATIONS UNDER THE "FEES AND PAYMENT" SECTION ABOVE.

  Exclusion of Consequential and Related Damages. IN NO EVENT WILL EITHER PARTY OR ITS AFFILIATES HAVE ANY LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT FOR ANY LOST PROFITS, REVENUES, GOODWILL, OR INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, COVER, BUSINESS INTERRUPTION OR PUNITIVE DAMAGES, WHETHER AN ACTION IS IN CONTRACT OR TORT AND REGARDLESS OF THE THEORY OF LIABILITY, EVEN IF A PARTY OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR IF A PARTY'S OR ITS AFFILIATES' REMEDY OTHERWISE FAILS OF ITS ESSENTIAL PURPOSE. THE FOREGOING DISCLAIMER WILL NOT APPLY TO THE EXTENT PROHIBITED BY LAW.

EXAMPLES OF LIMITATION OF LIABILITY PROVISIONS (CONT.)

> **Example 2:**

Limitation on Indirect Liability. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, NEITHER PARTY, NOR VENDOR’S SUPPLIERS, WILL BE LIABLE UNDER THIS AGREEMENT FOR LOST REVENUES OR INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY, OR PUNITIVE DAMAGES, EVEN IF THE PARTY KNEW OR SHOULD HAVE KNOWN THAT SUCH DAMAGES WERE POSSIBLE AND EVEN IF DIRECT DAMAGES DO NOT SATISFY A REMEDY.

Limitation on Amount of Liability. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, NEITHER PARTY, NOR VENDOR’S SUPPLIERS, MAY BE HELD LIABLE UNDER THIS AGREEMENT FOR MORE THAN THE AMOUNT PAID BY CUSTOMER TO VENDOR UNDER THIS AGREEMENT DURING THE TWELVE MONTHS PRIOR TO THE EVENT GIVING RISE TO LIABILITY.

Exceptions to Limitations. These limitations of liability do not apply to violations of a party’s Intellectual Property Rights by the other party, indemnification obligations, or Customer's payment obligations.

PERSONNEL ISSUES

- Providers generally seek the right to deny access to anyone who does not meet security requirements, and to anyone who violates its building policies
- Providers and customers often seek to restrict use of subcontractors to pre-approved subcontractors, subcontractors who have passed background checks, etc.

RELATIONSHIP WITH OTHER AGREEMENTS

- Enrollment agreements
  - Initial agreements establishing relationship between the parties sometimes supersede other contracts (e.g. vendor policies)
  - It is critical for customers to ensure that service specific contracts govern over enrollment agreements
- Cross default and IP non-assert clauses may be embedded in contract
  - Because of the mission critical nature of Cloud/data center services, customers try to avoid cross default provisions
  - Customers also resist IP non-assert provisions, which state that the customer waives infringement claims against a provider globally with respect to any services at issue under any other agreement

RELATIONSHIP WITH OTHER AGREEMENTS (CONT.)

- Acceptable use policies
  - Providers typically reserve the right to unilaterally modify policies
  - Changes may be inconsistent with an customer's standard operations, and thus customer may unknowingly be in breach
  - AUPs often have liability shifting provisions that may be different from the negotiated agreement, so customer should ensure that agreement governs
- Policies and Procedures
  - Virtually every provider has facility rules and regulations, access and security rules, and codes of conduct that must be adhered to
  - Customers must ensure that such documents are in fact consistent with their operations, and should carefully negotiate provider's right to modify applicable policies and procedures

END USER CONSIDERATIONS

- In addition to their own use, enterprise customers utilize Cloud/data center capacity in the provision of services to their own customers
  - SLAs given to such customers must be reconciled with SLAs received from the Cloud provider/data center operator
- Resale restrictions
  - Customers often intend to utilize Cloud services as an integral part of their own service offerings, and if so the agreement must allow such use
  - Ability of customer to utilize data center operators and outsource rights to third parties
- Take-or-pay provisions with end users may not be enforceable, which should be factored in when contracting for data center capacity

SECURITY STANDARDS

- Security Standards
  - Financial services and health care industries have specific requirements
  - Certifications
    - SOC (Service Organizational Control) regarding internal controls over financial reporting
      - SSAE (Statement on Standards for Attestation Engagements)
    - ISO (International Standards Organization) for security
    - HIPAA for health care compliance
    - PCI (Payment Card Industry) security standards for credit card processing

GOVERNMENTAL CONSIDERATIONS

- GDPR and other data protection laws must be addressed in Cloud/data center contracts to ensure that customer’s data is stored in the geographic region required by law
- Whether and to what extent customer data must be disclosed to law enforcement is critical
  - Is a subpoena required (in many countries government merely request disclosure)?
  - Does customer have a right to protest disclosure?
  - Should regulators have access to vendor personnel and data center facilities, e.g., in financial services, insurance and health care industries?

PART III

CLOUD CONTRACT CHECKLIST

CLOUD CONTRACT CHECKLIST

- What goods and services are being provided?
  - What applications/programs are being purchased or supported? Is training or ongoing support needed? Will the services be dedicated or shared?
    - Hardware component (buying or leasing hardware)
    - Software component (licensing of software)
    - Service component (engineering, installation, on-going support, maintenance, etc.)
- Where will the services be provided?
  - Will services be provided at multiple sites under a single contract?
  - Have there been issues relating to security or availability of services (including network connections) at the site?

CLOUD CONTRACT CHECKLIST (CONT.)

- Who is providing the services?
- Will any part of the service be provided by any subcontractors or any affiliates? If so, what services will be provided and where are such subcontractors and affiliates located?
- Are employees/ contractors entering the data center or otherwise accessing critical equipment required to sign confidentiality agreements? Are they subject to background checks?
- Is there a mandatory training and awareness program in place for employees to make them aware of the company's security policies, standards and security practices?

CLOUD CONTRACT CHECKLIST (CONT.)

- What are the performance standards for the service?
  - What service levels are provided?
  - What are the customer's remedies in the event of a service level failure?
    - When are credits provided and in what amounts?
    - Will customer have a right to terminate in the event of repeated service level failures?

CLOUD CONTRACT CHECKLIST (CONT.)

- What data is implicated?
  - What data will be stored or generated (flag sensitive or confidential information)?
  - Will the vendor have logical or physical access to data?
    - If the provider will have access to data, does it have a documented information security program? If so, what security precautions and plans are in place to ensure confidentiality, integrity and availability of customer's network, hardware, informational assets, and confidential data?
  - Does the service include data back-up? What is the business impact if all data is lost?
  - Who owns the data? Is there any customization or development anticipated?

CLOUD CONTRACT CHECKLIST (CONT.)

- How critical is the service to the customer’s business?
  - What is the impact to the customer’s business if the service is unavailable for a period of time?
  - What is the work around if the service is unavailable?
  - Does the service/product include any disaster recovery component?
    - If so, what is the process for risk identification/mitigation, what are the recovery time objectives and what are the applications that will support the services?

CLOUD CONTRACT CHECKLIST (CONT.)

- What compliance obligations does the provider have?
  - What certifications will the provider have received for any national or international security or quality standards (e.g. ISO 27001, SOC2, SSAE, ITIL, etc.)?
  - What is the scope and frequency of permissible customer audits?
  - What is the cost associated with the audits and who will bear the cost?

FOR ADDITIONAL INFORMATION:

Kemal Hawa **Shareholder (Partner)** **Greenberg Traurig, LLP** **E-mail: hawak@gtlaw.com** **Phone: 703-749-1379**	**Amber Lester** **Assistant General Counsel** **CyrusOne, Inc.** **E-mail: alester@cyrusone.com** **Phone: 859-468-9803**
Emily Naughton **Shareholder (Partner)** **Greenberg Traurig, LLP** **E-mail: naughtone@gtlaw.com** **Phone: 703-749-1390**	