PERKINSCOIE

COUNSEL TO GREAT COMPANIES

Negotiating SaaS and Cloud Contracts

May 28, 2015

Peter J. Kinsella
303/291-2328

Disclaimer…

The information provided in this presentation does not necessarily reflect the opinions of Perkins Coie LLP, its clients or even the author.

Peter J. Kinsella 303-291-2300

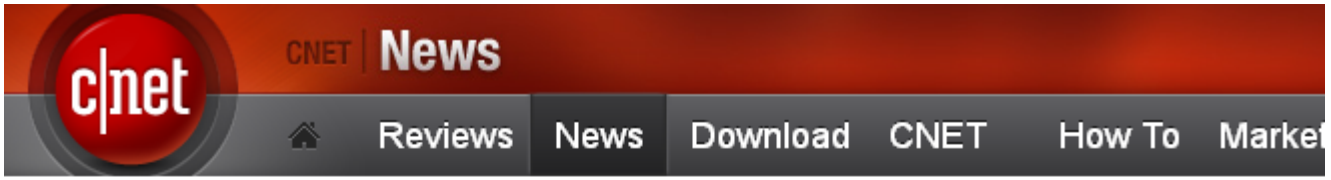
Risk Investigation -1

Customers will often want to consider a variety of financial, data, security and regulatory issues before entering into a cloud services arrangement.

Customers will typically attempt to mitigate risk through a variety of mechanisms:

- Diligence
- Audit pre- and post-contract execution
- Contract risk allocation

Risk Investigation -2



CNET › News › E-Business

October 17, 2000 6:15 PM PDT

Red Gorilla can't survive capital-market jungle

By Stefanie Olsen
Staff Writer, CNET News

Red Gorilla has shut down its site and turned over its current customers to another application service provider, its chief executive told CNET News.com on Tuesday.

"Right now the (Red Gorilla) system is offline, all the employees were let go, and there's no money in the bank," said chief executive John Witchel. "Officetool.com has agreed to continue operating the Web site so that our customers can continue to use our software."

Peter J. Kinsella 303-291-2300

PERKINSCOIE

Risk Investigation -3

Target Boosts Card Security After Data Breach

2 Text

By Richard Davies
@daviesnow

Apr 30, 2014 8:41am

Peter J. Kinsella 303-291-2300

PERKINSCOIE

Common Customer Concerns

- Integration – What is the onboarding process?
- Availability – will the service be available for use?
- Legality – can the customer legally use the service?
  - Privacy – how do I know the provider won't use the data in an unauthorized manner?
  - Security - will the data be secure?
- Integrity - will the data be stored and processed accurately?
- Termination – what happens upon termination?

Contract Negotiations

- Cloud services are often offered to the public as a commodity. Therefore, for small deals involving large providers, there tends to be less ability to negotiate the terms.
- Large providers are willing to negotiate at least some terms of larger deals (in excess of $1M/year)
- Large/sophisticated clients are developing their own form of cloud agreement – some good, some not-so good
- Smaller vendors are willing to deal

Peter J. Kinsella 303-291-2300

Cloud Services Contract Format - 1

- Goods/Software vs. Services Models
  - Many current customer contracts have evolved from a software licensing/UCC model
    - UCC often imposes warranties on delivered software but not on a pure services contract
  - Cloud computing contracts more closely resemble hosting or strategic outsourcing agreements
    - Knowledgeable customers will demand express warranties and remedies to cover services
  - A software license grant clause may cause confusion

Peter J. Kinsella 303-291-2300

Services Contract Format -2

- Compare:
  - Provider hereby grants customer a non-exclusive right to use the software/services.
  - Provider will use commercially reasonable efforts to provide access to the services set forth in Exhibit A.

Peter J. Kinsella 303-291-2300

Onboarding Process

- Typically focused on business issues and procedures
- For more complex arrangements,
  - may be documented in a separate exhibit that details the obligations of the parties in connection with transitioning the customer from its existing service provider
  - may be subject to SLA obligations
  - may need to address how the new provider will work with the existing provider

Pricing/Payment

- Many service providers will seek annual payment in advance (may need to address refund issues for certain breaches and termination issues)
- Pay for use - How is “use” determined?
  - Actual use/number of users/ number of employees
- Price Increases
- Benchmarking
- MFN

Peter J. Kinsella 303-291-2300

Services Description

What is included in the description ?

- Specifications?
- Published materials? FAQs?
- Bug and technical reports?

Common Rule of Thumb: A more detailed description of services is typically better than a description with less detail.

- It reduces arguments about whether a failure has occurred

Peter J. Kinsella 303-291-2300

Service Evolution

What is the process for changing the platform, operating system or application?

- Can the customer refuse or delay a change?
- How much notification needs to be given?
  - Different notice periods for routine vs. emergency changes?
- Will a test environment be provided prior to implementing a change?
- How does pricing work?
- Are the number of changes in a given time (e.g., 6 month period) limited?

Peter J. Kinsella 303-291-2300

Service Levels

- How are service metrics defined?
  - Does entire service have to be unavailable, or only particular portions?
- How are service metrics reported?
  - Does the customer need to have access to vendor tools to understand or obtain metrics?
  - Does the customer need to complain to get the credit?
- Is there a process for strengthening service metrics over time?
- Are service credits the sole and exclusive remedy arising from a performance breach?

Peter J. Kinsella 303-291-2300

Common SLA Service Components

- Identifies the services that are provided
- May clarify the services that are not provided
- Identifies assumptions underlying service availability
- Establishes service standards (e.g., the timeframes in which services will be provided)
- Defines the responsibilities of both parties

Peter J. Kinsella 303-291-2300

Common SLA Management Components

- Establishes how service effectiveness will be tracked
- Identifies procedures for reporting service issues
- Identifies procedures for resolving service issues
- May identify procedures for revising services or service metrics

Peter J. Kinsella 303-291-2300

Example –Downtime Definition

"**Downtime**" means any period, [greater than ten minutes], within the Scheduled Available Time during which the Customer in unable to access or use the Service [because of an Error], excluding any such period that occurs during any Scheduled Downtime.

"Scheduled Downtime" means: (i) ___ hours per [day][week][month] from _____ to _____ [Day/time zone], [and, (ii) the time period identified by Provider in which it intends to perform any planned upgrades and/or maintenance on the Service or related systems and any overrun beyond the planned completion time.]

- Is notice needed prior to scheduled downtime?

Example – Error Definition

More Provider Friendly: “**Error(s)**” means the material failure of the Service to conform to the material Specifications that is caused by a component of the service.

More Customer Friendly: “**Error(s)**” means any event that causes or is likely to cause a disruption to the Service or any part of the Customer’s operations (including services provided to Customers).

Example – Error Exclusions

Unauthorized modification of the Service

Third party hardware or software issues

Improper operation by customer

Services, circumstances or events beyond the reasonable control of the Service Provider

Any issue if a customer has outstanding past due amounts

Service Level Calculations

Multiple service metrics can be measured, not just service uptime. For example:

- time between reporting a problem and acknowledging the report
- incidents resolved in time
- data bandwidth and latency issues
- timeliness of reports
- reporting and meetings

Sample Support Scorecard

Priority 1 (High)	
Targeted Initial Response Time	within one (1) hour of the receipt of an Incident Report
Targeted Repair period	[X] hours from the time of Acknowledgment.

- Note use of the word “Targeted”
- Issue: Does a workaround constitute a valid repair?

Sample Credit Calculations - 1

Uptime Credit Mechanism

Uptime Percentage	Available monthly Service Credit ---- Percentage of monthly fees paid by Customer
Equal to or Greater than 99.9%	No Service Uptime Breach
Less than 99.9% but more than 99.8%	10%
Less than 99.8% but more than 99.7%	20%
Less than 99.7% but more than 99.6%	30%
Less than 99.6% but more than 99.5%	40%
Less than 99.5% but more than 99.4%	50%
Less than 99.4% but more than 99.3%	60%
Less than 99.3% but more than 99.2%	70%
Less than 99.2% but more than 99.1%	80%
Less than 99.1% but more than 99.0%	90%
Less than 99.0%	100%

Sample Credit Calculations -2

Mechanism Involving Multiple Factors

Number of Key Performance Metrics (KPIs) breached in applicable reporting period	Service Credit percentage of the monthly Support Service Fee
Breach of one (1) KPI	4 %
Breach of two (2) KPI	8 %
Breach of three (3) KPI	16 %
Breach of four (4) KPI	32 %
Breach of five (5) KPI	64 %

Reporting Procedures

What reports does the vendor provide?

- Usage Statistics?
- Errors?
- Downtime?
- Resolution?
- Root Cause Analysis?

When are the reports supplied??

End User Conduct

- Contracts often allow the provider to suspend or terminate service for bad user conduct (and for other reasons)
- The customer will want to make sure that such right may only be exercised in well-defined situations, preferably with advanced notice. The customer will want to limit suspension:
  - To breaches that that significantly threaten the security or integrity of the cloud service
  - To the user accounts in which the breach occurred, rather than all of customer's accounts

Peter J. Kinsella 303-291-2300

Ownership of Custom Developments

- Shared Multi-Tenant – it is difficult for the vendor to convey IP ownership of any service feature, because all customers must use the same service
  - This is the tradeoff for obtaining the efficiency of using a cloud service model

- Single Tenant - customer ownership of improvements is at least possible, as the customer is able to use a personalized instance of the software

Peter J. Kinsella 303-291-2300

Data Center Diligence -1

Where is the data stored?

What are the characteristics of the data center?

- Redundant telecommunications, power, and cooling?

Physical security of data centers?

- Who has access to: facilities, infrastructure, platforms, applications, and data?

Data Center Diligence -2

Data Segregation

- Public vs. Private Cloud
- Encryption?
  - Transmission? Rest?
  - Who has the keys?
- Where and how is backed-up data stored?

Does the system have software and other access controls to prevent unauthorized access?

Is penetration testing routinely performed?

Data Center Diligence - 3

Does the service provider:

- have a business continuity plan?
- provide redundant operations from different sites?
- routinely test its back-up capability?
- routinely attempt to restore data?

It is important to consider the impact of bankruptcy on the ability to access data and the ownership of back-up media

Service Diligence -1

Subcontractors

- Are subcontractors used to provide the service?
  - Can the service provider impose contractual obligations on the subcontractors?
- Can vendor identify the subcontractors?
- Does the customer have a right to approve new subcontractors? (or a category of subcontractors?)
  - What is the approval/disapproval process?
  - Service providers are reluctant to provide approval right, but may provide a termination right

Peter J. Kinsella 303-291-2300

Disaster Recovery -1

- Does the service provider:
  - have a business continuity plan?
  - provide redundant operations from different sites?
  - routinely test its back-up capability?
  - routinely attempt to restore data?
- It is important to consider the impact of bankruptcy on the ability to access data and the ownership of back-up media (Next Slide)

Peter J. Kinsella 303-291-2300

Disaster Recovery - 2

- What events cause the service provider to engage in data recovery operations?
- Does the contract contain data recovery goals?
- What are the consequences if the data is not recovered within the specified time frames?
- Who takes priority if multiple customers of the service provider are affected?
- How will a force majeure event impact contractual obligations? (next slide)

Peter J. Kinsella 303-291-2300

“Force Majeure” Events

- Parties can bargain for effects of “FME”
- Consider scope and wording (what is/is not considered FME)
- What form of relief is granted (excused from performance, suspension of performance, termination, etc.)?
- What are the disaster recovery obligations during an FME?
  - Are some customers contractually prioritized?

Peter J. Kinsella 303-291-2300

Privacy -1

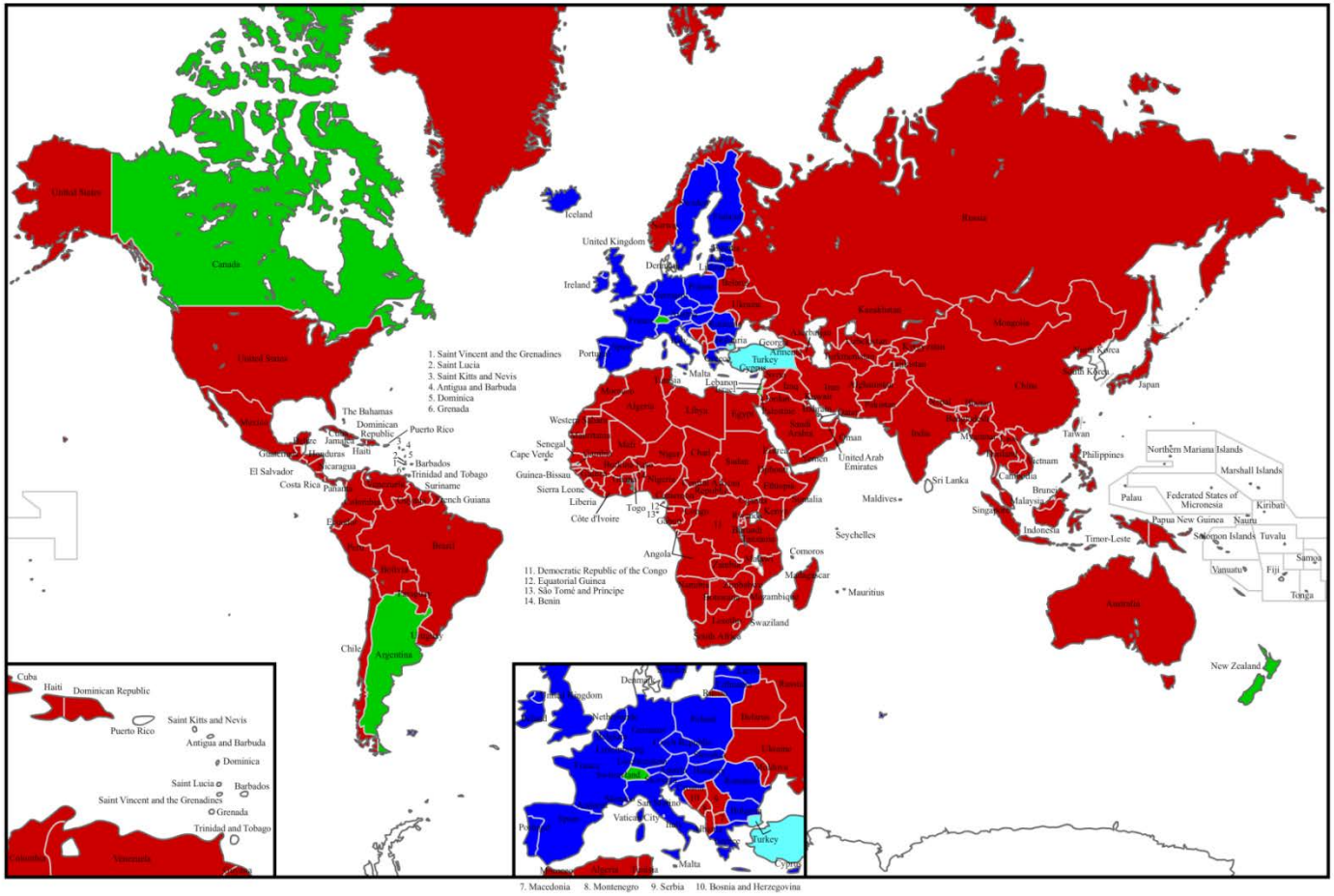
Frequently implicated data protection laws:

- EAR/ITAR (prohibits "export" of information)
- Patriot Act and other laws (U.S. gov't can access data)
- Sarbanes-Oxley (controls over financial information)
- EU Data Protection Act (see next slides)
- Patchwork of Federal Laws, For example:
  - Gramm-Leach-Bliley (banking/insurance information)
  - HIPAA (employee or third party health information)
  - FERPA (information concerning students)
- Patchwork of evolving state laws

Peter J. Kinsella 303-291-2300

Privacy -2

EU Restrictions on Data Transfer



Peter J.

PERKINSCOIE

EU Data Protection Laws -1

EU Data Protection Laws Issues

- Rule: Data must not be transferred to countries outside the EU that do not offer an “adequate level of protection”
  - Currently only: Andora, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, Uruguay.
- Exceptions:
  - ask permission from every “data subject” involved
  - for US - Dept. of Commerce “safe harbor” registration
  - EU model contract clauses
  - “Binding Corporate Rules”

Peter J. Kinsella 303-291-2300

EU Data Protection Laws -2

- Legislation makes fundamental distinction between:
  - **data controller**: party that defines the purpose and the means of processing the data
  - **data processor**: the party performing the tasks
- Data controller is liable towards the “data subjects”
- Data controller is obligated to select appropriate data processors, and must obtain adequate contractual protection from them

Peter J. Kinsella 303-291-2300

EU Data Protection Laws -3

EU law will apply when:

- A “controller” is located in its territory; or,
- When a “controller” outside the EU uses “equipment” within the EU territory

Applied to cloud computing:

- Using an EU-based data center triggers legal compliance obligation
- Many authorities interpret “equipment” in an extremely broad way (e.g., browser cookies)

Peter J. Kinsella 303-291-2300

Common Data Issues

- Define "data"
  - Stored data?
  - Who owns usage metrics, aggregate de-identified data?
- Specify ownership rights in the data
- Specify purposes for which the data may be used
  - Is the service provider permitted to use the data (or aggregate data) for other purposes?

Peter J. Kinsella 303-291-2300

Commonly Used Security Standards

- SSAE-16 requires management to provide a written assertion concerning the organization's systems, suitability and effectiveness
- ISO-27002 – comprehensive controls in areas such as access control, asset management, business continuity and how to handle security breaches.
- PCI DSS – credit card security
- HIPAA – security requirements for health information

Peter J. Kinsella 303-291-2300

Security Obligations – 1

- Are physical and logical security procedures required?
- Employee background screening?
- How is security verified?
  - Note that a customer audit may not be permitted under law or under other provider contracts
- Is a separate Data Protection Agreement needed?
  - Often used when handling EU data

Peter J. Kinsella 303-291-2300

Security Obligations – 2

- Data Protection Agreement - May cover a wide range of topics, such as:
  - Organizational measures, such as: security officer; security plan; staff functions
  - Technical measures, such as: authorization, identification, authentication, access controls, management of media
    - Note: may specify different measures based on sensitivity of data
  - Record Keeping

Peter J. Kinsella 303-291-2300

Security Events

- Agreements may distinguish between "Security Issues" and "Security Incidents" and provide different rights, obligations and remedies for each category.
  - Security Issues – issues that could give rise to a security breach
  - Security Incidents – actual breach of security

Peter J. Kinsella 303-291-2300

Security Issues

- How are security issues defined?
  - Objective vs. subjective definition
  - Are issues in the vendor's control and those in the control of its subcontractors differentiated?
  - Does every problem need to be investigated?
  - Does every problem need to be fixed?
- What is the process for fixing the issue?
  - Is there a specified time frame?
  - How is the time frame adjusted for fixes that take longer to implement?

Peter J. Kinsella 303-291-2300

Security Incident

- Notice requirement to other party
- Remediation efforts
  - Who does what?
  - Who pays for the remediation efforts?
  - Does the breach require end-user notification?
- Who has legal liability for the incident?
  - May want to address liability caused by third parties (e.g., hackers)

Peter J. Kinsella 303-291-2300

Confidentiality Clauses

- May impose a back door security obligation on the service provider
  - Is the service provider obligated to keep a customer's information "confidential"?
  - Some providers will state that they will employ "commercially reasonable efforts" to "protect" a customer's confidential information

Peter J. Kinsella 303-291-2300

Subpoenas/ E-Discovery

- Who bears the costs associated with subpoenas and e-discovery
  - Many vendors will attempt to make the data available to the customer and let them figure out what data is relevant
    - May need special procedures if the system produces metadata
- Vendor may not be able to disclose all subpoenas (e.g., national security subpoenas)

Peter J. Kinsella 303-291-2300

Data Retention Issues

- Customers tend to want two conflicting obligations
  - Vendor should keep the data as long as customer needs it
  - Vendor should promptly destroy it when it is no longer needed
- Depending on the service, vendor may not know the content of the data
- Contract should specify when data is destroyed

Peter J. Kinsella 303-291-2300

Compliance Requirements

- Customer may want the contract to contain procedures for auditing compliance issues:
  - Does the vendor data center facility allow visitors?
  - Will the audit disclose too much security information?
  - Will a customer's auditor have access to other customers' data?
- Customer may want to impose compliance obligations on the vendor

Peter J. Kinsella 303-291-2300

Risk Mitigation - 1

- Typically, the customer wants to impose a combination of the following obligations on the service provider:
  - Operating procedures
  - Warranties
  - Indemnities
  - Insurance
- Typically, the vendor wants to minimize obligations (especially any obligation that slows its ability to make changes or causes "out of process" deviations) and impose other limitations on its liability

Peter J. Kinsella 303-291-2300

Risk Mitigation - 2

- Operating procedures
  - Back-up and recovery procedures
  - Compliance procedures
  - Audit procedures
    - Contract should contain procedures for addressing deficiencies discovered during audits

Peter J. Kinsella 303-291-2300

Risk Mitigation - 3

- Warranties/covenants
  - Obligations found in hosting and outsourcing agreements may not be included in cloud computing contracts, due to the commoditized nature of the relationship
  - Customer will want to try to memorialize diligence results (including vendor procedures)
  - Vendors typically push to provide an indemnity rather than a warranty

Peter J. Kinsella 303-291-2300

Risk Mitigation - 4

Exemplary Types of Express Warranties:

- Conformance with Specification/Documentation/Sales literature
- Security Measures
- Scalability
- Operating Performance (system response)
- Non-Infringement (service and combinations)
- Data Conversion/Compatibility/Integrity
- Documentation
- Delivery Times/Methods
- Standard of Services
- Support and Response Times
- Lack of Viruses/Time Bombs
- Qualifications of Employees

Peter J. Kinsella 303-291-2300

Risk Mitigation - 5

- Indemnities
  - Like warranties, vendors typically provide very limited, if any, indemnification obligations
  - Vendors will vigorously push back on typical liability caps (damage cap and consequential damages cap)

Peter J. Kinsella 303-291-2300

Risk Mitigation - 6

- IP Indemnity - Vendors will typically:
  - Defend and pay finally awarded judgment
  - Want to exclude combinations created by the customer
    - Observation: The customer creates a combination in most cloud arrangements
    - Potential compromise: Vendor indemnifies for a combination, unless a reasonable non-infringing combination was available
  - Want to exclude certain customer data issues

Peter J. Kinsella 303-291-2300

Risk Mitigation - 7

- Software Escrows?
  - Typically, software escrows have little value in many cloud service arrangements, because the customer will not have the equipment/data center infrastructure to actually utilize the escrow
- Service Escrows: Situation may be different if service is an “app” running on commercial third party platform
- Data Escrows?
  - Data stored with a third party that can be accessed separately by customer

Peter J. Kinsella 303-291-2300

Risk Mitigation - 9

- Insurance
  - Contract may require a party to carry certain levels of insurance
  - CGL policy may not be enough to cover many cyber liability issues
  - Cyber liability policy may have lower limits for certain categories of damages (e.g., breach notification, credit reporting services)
  - Requires consultation with broker/agent

Peter J. Kinsella 303-291-2300

Limitation of Liability - 1

- Issues to consider:
  - Caps on the "type" of damages
    - Direct vs. Consequential vs. Incidental
  - Caps on the "amount" of damages
    - Different categories of damages may require different amounts
  - Exceptions to the one or both of the caps?
    - Indemnification
    - Security Breach

Peter J. Kinsella 303-291-2300

Termination and Transition

- Every contract will end at some time
  - It is important to plan for termination issues prior to contract execution
- Customer will want the contract to address
  - Transition assistance
    - Data migration
      - Format of data?
      - It may not be easy to copy or download the data
  - Continued provision of services until transition completed
- Vendor will want payment for post-termination services

Peter J. Kinsella 303-291-2300

Thanks!

Peter J. Kinsella

pkinsella@perkinscoie.com

303-291-2300