MORRISON | FOERSTER

Creating Value in the Cloud by Minimizing Risk and Maximizing Governance

Russell G. Weiss
March 28, 2012

Presenter

Russell “Rusty” Weiss
Partner
Los Angeles Office
(213) 892-5640
rweiss@mofo.com

Presentation Objectives

1. Identify the leading risks involved in utilizing a cloud computing environment
2. Determine how to mitigate such risks through planning, negotiation, and implementation
3. Demonstrate the importance of governance in a cloud computing environment
4. Provide instruction on how to implement governance in a cloud computing environment

Risk Factors: Public vs. Private Clouds

PUBLIC

- On-demand, scalable resources are provided over the internet
- By a third-party provider who shares resources ("multi-tenancy") and bills on a fine-grained utility-computing basis
- With less customer control over data security, compliance, and reliability
- With little or no capital cost to the customer
- At a lower operational cost than a private cloud, since the provider has fewer restrictions
- With little flexibility, since the offering is highly standardized

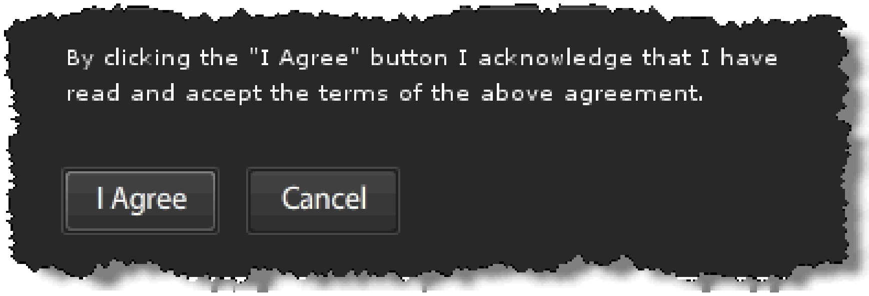
PRIVATE

- On-demand, scalable resources are provided over the internet or private networks
- By internal department or trusted third-party ITO outsourcer
- Allows customer control over data security, compliance, and reliability
- Customer has to build and manage its data center(s)
- At a higher operational cost than a public cloud, since provider has more restrictions
- With greater flexibility, since the solution is more easily customized

Hybrid clouds are a combination of the two, linking privately managed resources to business applications and functions that have been placed in public clouds.

Risk Factors: Contracts & Negotiation

- **cloud computing is generally not amenable to in-depth negotiation**
  - In order to make their offerings cost-effective, cloud providers offer a scalable “one-size-fits-all” service to many customers
  - Generally, cloud providers must treat most customers in substantially the same way in terms of service levels, indemnification obligations, and other contractual provisions
- **“Clickwrap” agreements generally are the norm for smaller agreements**

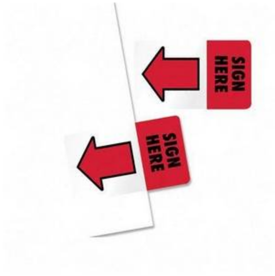


By clicking the "I Agree" button I acknowledge that I have read and accept the terms of the above agreement.

Risk Factors: Contracts & Negotiation (cont'd)

Would You Sign This Contract?

- You are the company's General Counsel. An employee informs you that she is entering into a contract on behalf of the company. The contract includes the following terms:
  - The other party can suspend your right and license to use services, or terminate the agreement in its entirety, for any reason or no reason, at its discretion at any time with, at most, 60 day's notice
  - In the event of a suspension of service, the other party will not intentionally erase your data (but will not represent that it will preserve it), and can condition return of your data upon your compliance with terms and conditions the other party may establish in the future
  - Your access to services may be suspended without notice, and the other party will have no liability with regard to such downtime
  - You bear sole responsibility for adequate security, protection, and backup of your data, even though the other party is hosting it
  - The contract terms can be changed at any time by the other party
  - Your company must indemnify the other party from all claims relating to your use of the other party's services, with no limitations on liability



Risk Factors: Contracts & Negotiation (cont'd)

- Because cloud providers' default contracts are usually one-sided (in the provider's favor) and difficult, if not impossible, to change, due diligence is crucial
  - Due diligence is one of a customer's few protections when choosing among several vendors with non-negotiable contracts
- Customers should still try to negotiate terms, as some providers are seeking to improve the acceptability of their products
- Larger customers with significant leverage will often be able to negotiate terms. Check to determine if enterprise terms are available
- Competitive bidding is very important, and third-party resellers may have more flexibility in contracting for cloud computing solutions
- Providers are striving to provide compliance "out of the box" to address the risk issues inherent in their business models
- Public Cloud Leverage vs. Private Cloud Leverage

Risk Factors: Contracts & Negotiation (cont'd)

- Cloud providers are usually reluctant to negotiate SLAs, but, when pressed, may offer additional remedies for service level failures
  - While the amount of a service level credit may be negotiated, the form such credit takes is often additional use of the service
  - Consider if additional use of the service is a suitable remedy if the service is unavailable for extended periods
- Providers may also be willing to add language relating to security breaches, but only to the limit of what is required by law
- Using Requests for Proposals ("RFPs") and Requests for Quotes ("RFQs") will also allow a customer to have more detailed information prior to choosing a provider, which will assist in due diligence and often result in upfront concessions from the service provider

Risk Factors: Contracts & Negotiation (cont’d)

Resellers May Mitigate Contracts & Negotiation Risk

- Resellers may purchase services from cloud providers and resell them, often as part of additional services
- Adding another party (such as a reseller) to the mix can allow for more flexibility, especially if that party is willing to take on risk
- Additionally, resellers can help customers to implement a cloud solution, as it can be complicated to perform the initial transfers of data and setting up of accounts
- City of Los Angeles/Google/CSC Example
  - The City was able to negotiate a separate clickwrap agreement with Google
  - Google agreed to store and process certain data only in the United States
  - Established liquidated damages for Google’s breach of nondisclosure and confidentiality obligations

Risk Factors: Contracts & Negotiation (cont'd)

Disaster Recovery Plan: Don't Be Cheap!

Amazon Web Services Disruption Example

- Certain Amazon Web Services operating from a data center in Northern Virginia suffered disruption at about midnight on April 21, 2011, until about 6:00 p.m. on April 23, 2011
- Impacts of the disruption:
  - Web services unavailable for 66 hours
  - Permanent data loss on 0.07% of volumes in the affected data center
  - 10-day credit for customers of the affected data center, regardless of whether they experienced downtime
- Netflix subscribes to Amazon's redundant cloud architecture and was unscathed. BigDoor, a small technology publisher for online publishers, was effectively shut down for a day and a half and only received a 10-day credit as its remedy.

Risk Factors: Privacy & Protection

Generally…

- Provisions concerning data security and indemnification are often sticking points in cloud computing deals
- These agreements are, in essence, all about data transfer—even if a customer cannot alter terms, it is crucial to understand who is responsible for what
- A customer may find itself having to take on additional obligations, which can change the cost analysis:
  - Back-up
  - Encryption
  - Compliance

Risk Factors: Privacy Compliance

- A business considering a cloud-based solution must consider compliance with privacy laws and regulations:
- U.S. issues:
  - Sector-specific privacy laws regulate sharing with third parties, including vendors (e.g., Gramm-Leach-Bliley Act, HIPAA)
  - State data security laws require safeguards when using vendors
    - Massachusetts data security regulations are high-profile examples
    - But at least 10 other states also have data security laws
  - State security breach notification laws—over 45 states
    - Typically cover name *plus* Social Security number, driver' s license number, credit or debit card number or financial account number, health information, etc.
    - Generally provide an exception for encrypted data
    - Notice obligation falls on data owner, even if breach occurs at vendor

Risk Factors: Privacy Compliance (cont.)

International issues:

- Broader privacy laws, typically covering all sectors and all types of personally identifiable information ("PII")
  - Examples: name, email address, work address, home address, government-issued ID number, employee ID number, performance appraisals, compensation information, time and attendance, health information, credit card number, bank account number, driver's license number, mother's maiden name
  - Covered "data subjects" include consumers, employees, consultants, vendors, service providers, individuals at corporate customers
- Limitations on outsourcing of PII
- Restrictions on cross-border transfers of PII
- Registration requirements in some countries
- Notice and consent requirements
- Evolving breach notification laws/guidelines

Risk Factors: Privacy Compliance (cont.)

Countries with Privacy Laws

- **North America**
  - Canada
  - Mexico
  - United States
- **Central & South America**
  - Argentina
  - Brazil (Pending)
  - Chile
  - Colombia
  - Costa Rica (Pending)
  - Ecuador (Pending)
  - Paraguay
  - Peru (Pending)
  - Uruguay
- **Middle East**
  - Israel
  - UAE (DIFC)
- **Africa**
  - South Africa (Pending)
  - Tunisia
- **Asia-Pacific Rim**
  - Australia
  - Hong Kong
  - India
  - Japan
  - Malaysia
  - New Zealand
  - Philippines (Pending)
  - Singapore
  - South Korea
  - Taiwan
  - Thailand (Pending)
  - Vietnam
- **Europe**
  - 27 EU Member States
  - Norway
  - Russia
  - Serbia
  - Switzerland
  - Turkey (Pending)
  - Ukraine

Risk Factors: Data Security

- Data security involves both internal, company-sensitive information (e.g., employee information, company data, trade secrets) and the security of personal information
  - Does the provider provide representations concerning security in its agreement?
  - Some providers may use customer data to gather analytics that are then resold or used for other purposes
- 87% of businesses surveyed are concerned about security issues (IDC)
  - For vendors, security needs to be a core competency
  - Security often is not a core competency for customers (for some consumers, moving data to the cloud may mean better security)
- Emerging standards for third-party certification may help to alleviate some data security concerns
  - ISO 27001—Information Security Management System (ISMS) standard, requiring specific internal controls and audits to maintain third-party certification
  - SAS 70—a type of audit now being utilized to assess internal security controls (soon to be replaced by new standards)
  - Enterprise Cloud Leadership Council and Cloud Security Alliance may help push for standards in this area

Risk Factors: Data Security

What’s the Solution?

- Choose services that fit the sensitivity of your PII and privacy obligations
- Implement mechanism for cross-border transfers, where required
- Limit cloud usage to nonsensitive data until better security standards are implemented by your provider
- Encrypt data before sending it to the cloud
- Actively manage access to PII
- Mandatory password changes every 90 days
- Use intrusion detection software
- Data center must have 24-hour monitoring and always be locked
- Cloud vendor security measures must be certified by third-party
- Annual security training for all employees

Governance in the Cloud

Why Governance Is Needed

Since cloud computing environments can involve dozens of different services and solutions, they need governance in order to maximize the benefits offered.

Governance in the Cloud (cont'd)

What does governance mean in a cloud computing environment?

Governance means the designing, building, and testing of policies and procedures that monitor and govern the use of the services being offered in the cloud.

cloud computing service providers must have polices, procedures and tools in place that allow the customer to govern how the cloud computing services are used.

You can't drive an Indy race car without a steering wheel.

Governance in the Cloud (cont'd)

Key Questions to Be Addressed in Order to Achieve Cloud Governance:

1. Who can access the service(s) offered in the cloud?
2. What can (and can't) they do with the service(s)?
3. What types of security measures will be used to protect access to the service(s) and the corresponding data?
4. Who will be allowed to set up and maintain service levels?
5. Who will have access to provisioning, versioning and upgrades?
6. What types of restrictions should be placed on such provisioning, versioning and upgrades?

Governance in the Cloud (cont'd)

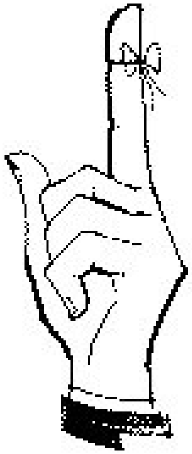
Key Questions to Be Addressed in Order to Achieve Cloud Governance (cont'd):

7. Who can audit the use and operation of the cloud?
8. Who will have access to the data (especially personally identifiable information) stored in the cloud?
9. Where will individuals be allowed to access such data (especially personally identifiable information)?
10. Can such data (especially personally identifiable information) be saved to a local computer?
11. What types of measures are in place to allow the customer to comply with audit demands of applicable governmental authorities?
12. What types of measures are in place to allow the customer to comply with litigation discovery requests?

And Remember…

- While cloud computing is attractive because it can reduce costs and offers added efficiency and flexibility, there are many risk factors and governance issues that must be properly addressed in order to maximize the foregoing benefits

- If these risk factors and governance issues are not properly considered and addressed, you will have a cloud computing failure on your hands instead of a cloud computing solution



For More Information

www.mofo.com/cloud

www.mofo.com/outsourcing

Questions?