MAYER·BROWN JSM

Cloud Computing - Challenges in Contracting for Cloud Services

Presentation for Office of the Government Chief Information Officer of Hong Kong - Working Group on Provision and Use of Cloud Services

Geofrey L. Master

Partner, Business & Technology Sourcing

Mayer Brown JSM

+852 2843 4320

geofrey.master@mayerbrownjsm.com

27 July 2012

Agenda

- Overview - Contracting for Cloud Computing: Preliminary Challenges
- US Government Cloud Computing Materials
  - NIST S&P Guidelines - Highlights
- Key Issues in Cloud Computing
  - Privacy and Security
  - Other Critical Contracting Issues
  - Public vs. Private Cloud – Key Contracting Issues
- Conclusion: Contracting for Cloud Computing

Overview - Contracting for Cloud Computing: Preliminary Challenges

- One-sided contracts, with service provider-friendly terms and little or no opportunity to negotiate
- No accepted standards for contract terms, service levels, etc. for non-routine undertakings
- Offer “as is” products and services, without any representations or warranties
- Impose sole responsibility for adequate security, data protection and backups on client
- Disclaim all liability for direct or consequential damages
- Incorporate on-line forms, subject to unilateral change or even deletion
- Retain unilateral right to suspend service or terminate contract

Overview - Contracting for Cloud Computing: Preliminary Challenges, cont'd

- Are relative newcomers, with little outsourcing or even software licensing experience
- Emphasize low cost, standard offerings, leaving little room for robust contractual commitments or client-specific customization
- Are heavily dependent on third party software and platform service providers and unable to flow down the requested contractual commitments
- Are constrained by their delivery model, leaving them unable to offer audit or other such rights to individual clients.

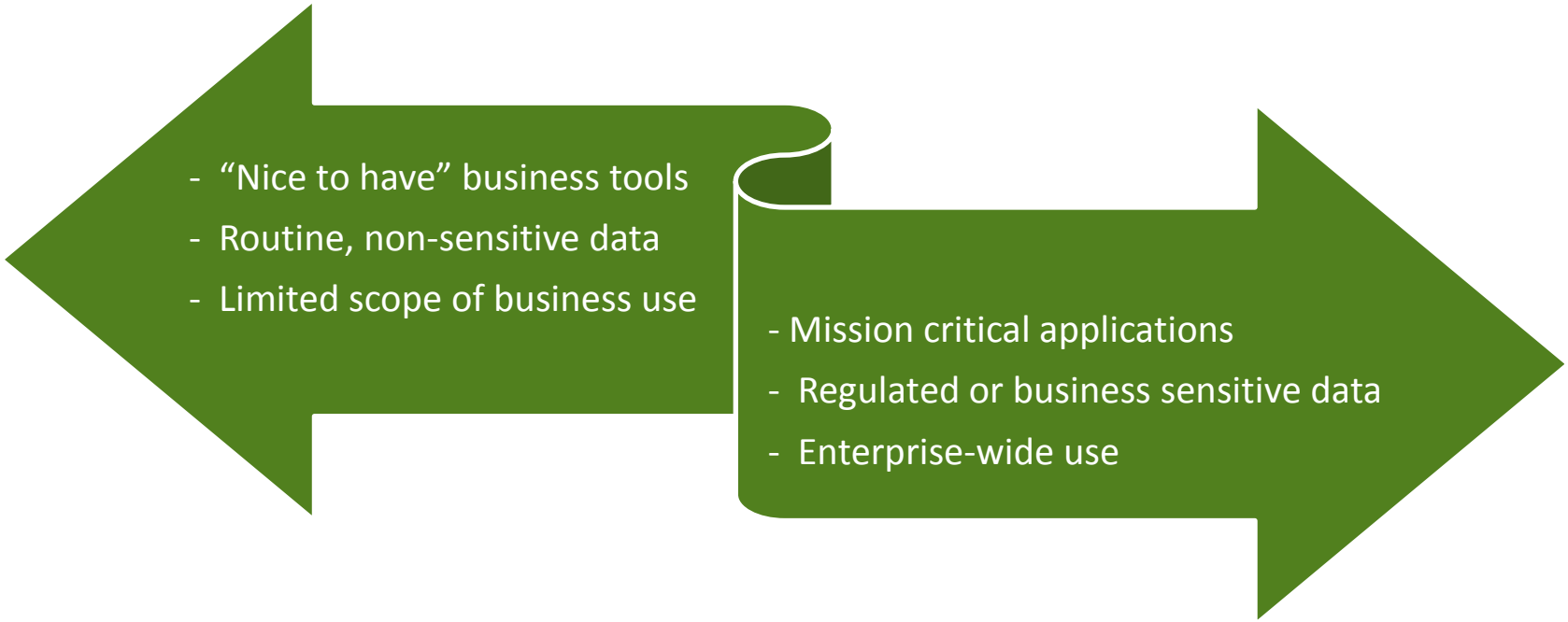
Overview - Contracting for Cloud Computing: Preliminary Challenges, cont'd

Cloud Clients Must Make Informed Tradeoffs

- There is no standard contract “form” that will work for all situations
- Traditional outsourcing and software licensing terms may be useful, but can not be inflexibly applied to cloud computing
- More robust contractual protection may or may not be the correct answer – it depends
- Prospective cloud clients must take into account –
  - criticality of the software, data and services in question,
  - unique issues associated with cloud computing, and
  - availability and pricing of various alternatives
- For "nice-to-have” business tools or routine data, a low cost solution may outweigh contractual protections
- Requiring robust contractual protections may increase the price and eliminate certain service providers altogether

Overview - Contracting for Cloud Computing: Preliminary Challenges, cont'd

Breadth of Cloud-Based Offerings



Each end of the spectrum presents different legal and contractual challenges, options and trade-offs

MAYER·BROWN JSM

US Government Cloud Computing Materials

- Federal Cloud Computing Strategy (a/k/a the "Cloud First Initiative"), US CIO - 8 February 2011
- NIST SP 800-144 (Dec'11): Guidelines on Security and Privacy in Public Cloud Computing ("NIST S&P Guidelines")
- NIST SP 500-293 (Nov'11) US Government Cloud Computing Technology Roadmap *- the first set of guidelines for how the federal government manages security and privacy in the cloud*
  - Vol. I: High Priority Requirements to Further USG Agency Cloud Computing Adoption
  - Vol. II: Useful Information for Cloud Adopters
  - Vol. III: Technical Considerations for USG Cloud Computing Deployment Decisions

US Government Cloud Computing Materials - NIST Security &Privacy Guidelines - Highlights

- **Negotiate** - Non-negotiable service agreements may be the norm in public cloud computing, but (like "traditional IT outsourcing contracts") negotiated service agreements can address security and privacy details.
- **Issues to negotiate** - security and privacy details, including:
  - vetting of employees;
  - data ownership and exit rights;
  - isolation of tenant applications;
  - data encryption and segregation;
  - tracking and reporting service effectiveness;
  - compliance with laws and regulations; and
  - the use of validated products meeting requisite standards (e.g., Federal Information Processing Standard 140).

US Government Cloud Computing Materials - NIST Security &Privacy Guidelines - Highlights, cont'd

- **Secure client side** - review organization's existing security architecture, have measures appropriate to maintain physical and logical security (e.g., challenges with embedded mobile devices, etc.)
- **Individual security vulnerabilities** - cloud computing heavily dependent on the individual security of many individual components; security and privacy needs to be maintained at each, including:
  - self-service;
  - resource metering;
  - data replication and recovery;
  - service level monitoring;
  - workload management; and
  - data storage.

US Government Cloud Computing Materials - NIST Security &Privacy Guidelines - Highlights, cont'd

- **Accountability** - audit mechanisms and tools should be in place to:
  - determine how data is stored, protected, and used;
  - validate services; and
  - verify policy enforcement.
- **Data location** - detailed information about the location of an organization's data may be unavailable, but when information crosses borders, he governing legal, privacy, and regulatory regimes can be ambiguous and raise a variety of concerns:
  - do laws of collection jurisdiction permit transfer;
  - do laws of collection jurisdiction continue to apply post transfer;
  - do laws of destination present additional risks or benefits; and
  - what technical, physical and administrative safeguards, such as access controls, apply.

Key Issues in Cloud Computing:
Privacy and Security - the Elephant in the Room

- Data transfer issues (EU and similar jurisdictions - §33 of the Personal Data (Privacy) Ordinance)
- Data location issues
- End-user location issues
- Movement and storage of data
- Use of subcontractors
- Lack of transparency and control
- Data breach issues
- Data destruction issues
- Ability to impose security and privacy requirements
- Confidentiality

Key Issues in Cloud Computing: Other Critical Contracting Issues for Cloud Clients

Regulatory and Compliance Challenges

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

Other Key Issues and Challenges

- Service levels / Availability
- Disaster recovery and business continuity
- Intellectual property issues
- Technology determination
- Change management issues
- Exit rights
- Financial stability of service providers/due diligence

Key Issues in Cloud Computing - Public vs. Private Cloud – Contracting Issues

Customer Need	Pure Public Cloud Solution	Enterprise Cloud Solution (Leveraged Private Cloud)
Need for diligence on provider	Physical diligence/inspection not permitted, and not possible if sub-processors are used	Basic diligence information is available – certifications, audit reports, etc.
Know where data is processed and stored	Data may be processed and stored anywhere	Location of data can be fixed in contract
Know places where data may be transferred	Data may be transferred to or accessed from anywhere	Location of data can be fixed in contract
Rights to approve of subprocessors	Frequent use of subprocessors (scalability, flexibility, variable use)	Notice of subprocessors as necessary for compliance (EU), and approval in some cases

MAYER·BROWN JSM

13

Key Issues in Cloud Computing - Public vs. Private Cloud – Contracting Issues, cont'd

Customer Need	Pure Public Cloud Solution	Enterprise Cloud Solution (Leveraged Private Cloud)
Response to data security incidents	Standardized offering, use of sub-processors and other limits may delay discovery of breaches, and ability to provide information regarding extent of breach	Notification of security incidents is offered, although extent of liability remains an item of negotiation
Audit rights	Typically not available, especially not for sub-processors	Some rights available, but may not include physical access
Proper disposal and destruction of data	No guarantee all data will be found and erased or returned	Data will be returned or destroyed
Change Control	Provider may make changes without notice or consent	Notification of changes provided, but customer may have to terminate or leave cloud if changes cause issues

MAYER·BROWN JSM

14

Key Issues in Cloud Computing - Public vs. Private Cloud – Contracting Issues, cont'd

Customer Need	Pure Public Cloud Solution	Enterprise Cloud Solution (Leveraged Private Cloud)
Established Contract Terms	Incorporation of additional online terms, subject to change by provider	Contract terms are established and should not materially change
Provider has some liability exposure for breaches and non-compliance	Extremely limited liability	More standard (ITO like) liability, although with different caps for security and confidentiality breaches around personal data
Controls on data and security standards	Standardized offering with use of cloud provider controls	Customer must review provider standards and determine sufficiency

MAYER·BROWN JSM

15

Conclusion: Contracting for Cloud Computing

- Client must determine if a cloud solution is compatible with overall requirements. Keep eye on –
  - the criticality of the software, data and services,
  - the unique issues associated with cloud computing, and
  - the availability and pricing of various alternatives
- Traditional outsourcing contracts and software and data use agreements offer good starting point

Questions?

Geofrey L. Master

Partner, Business & Technology Sourcing

Mayer Brown JSM

+852 2843 4320

geofrey.master@mayerbrown.jsm

MAYER·BROWN JSM