Best Practices for Sourcing Cloud Computing Services

Marc Lindsey
Partner
Levine, Blaszak, Block & Boothby, LLP
MLindsey@LB3Law.com
Disclaimer

This presentation is for informational purposes only and does not constitute legal advice. Discussions or answers to questions during the presentation should also not be relied upon as legal advice, and no attorney-client relationship will attach as a consequence of participation in this session.
Agenda

• Introduction to Cloud Computing
• Enterprise Cloud Risks and Responsibilities
• Contracting Tips
• Closing Thoughts
• Questions
Introduction
What is Cloud Computing?

- Key characteristics of cloud computing services
  - Hosted and managed by the vendor
  - Made available to customers remotely via an IP-based network
  - Designed on a shared services / multi-tenant platform
  - High elasticity and scalability of computing resources
  - Self-provisioning tools provided to customers on-line
  - Available under subscription / pay-as-you-go pricing
What is Cloud Computing?

- Service delivery categories (the “SPI” framework)
  - SaaS - Software as a Service
  - PaaS - Platform as a Service
  - IaaS - Infrastructure as a Service (VzB and AT&T call this CaaS)
What is Cloud Computing?

SaaS

PaaS

IaaS

Obtained via Creative Commons license
What is Cloud Computing?

• Cloud deployment models
  – **Public** – Third-party provides IT resources that reside in the vendor’s data centers and are exposed to customers via the Internet or “private” network connections
  – **Private** – Enterprise uses virtualization technologies within its own data center to create elastic and scalable IT resources
  – **Hybrid**
    • Private cloud used to host business critical applications and sensitive data
    • Public cloud for non-core applications and generic data
Key Cloud Computing Drivers

- Reduces implementation effort and cost
- No lump sum licensing fees or equipment purchases
- Rapid transition to new technologies and business processes
- Lower total cost of usage
- Better resource elasticity and scalability
- Improves availability of applications to mobile/remote workers
- More efficient and effective management of technology resources by vendors with specialized skills
- Avoids IT management-maintenance-upgrade hassles
Risks and Responsibilities in Enterprise Cloud Arrangements
Heightened Risks

- Familiar IT risks apply to services in the cloud
- Some risks are heightened, others are unique to cloud computing
  - Vendor lock-in
  - Security and privacy
Vendor Lock-In

• Three primary concerns
  – Data portability
  – Application portability
  – Infrastructure interoperability

• Lock-in concern is exacerbated because many cloud vendors are new entrants, and their long-term viability is uncertain
Vendor Lock-In

• Data portability
  – SaaS and PaaS
    • Data access, control and ownership should be negotiated
    • Is data in usable format readily loadable onto new cloud?
    • Are there effective automated tools to extract data and export it to sites you pick?
  – IaaS
    • Customer controls logical access to the applications, database and storage so raw data access isn’t a problem
    • But vendor tools and assistance to extract and transfer data are still desirable
Vendor Lock-In

- Application portability
  - Software built based on open standards promotes portability
  - **SaaS** – Often walled off, with little ability for customers to take applications elsewhere or in-house
  - **PaaS** – Platforms often use proprietary database structures and unique APIs between infrastructure components
  - **IaaS** – Applications are customer-provided, but server VM images may be locked-up or configured uniquely for the vendor’s infrastructure
Vendor Lock-In

- Infrastructure interoperability
  - **SaaS** – N/A
  - **PaaS** – Considerable re-programming and architecture changes often required to move to new PaaS vendor
  - **IaaS** – How portable are the server VM images, and how unique is your IaaS vendor’s virtualization layer?
  - How well do public clouds interact, and how easy is it to link private clouds to public clouds?
Vendor Lock-In

- Key takeaways
  - Limitations on portability
    - Major barriers to SaaS and PaaS enterprise adoption
    - Solvable impediment in IaaS
  - When picking a cloud vendor, favor one that
    - Uses open standard-based components and APIs
    - Uses standard 3rd party (e.g., VMware) virtualization layer
    - Offers its customers good porting tools, and demonstrates efficient portability under relevant use cases
  - Include vendor’s post-term migration assistance obligations in contract
  - Conduct financial due diligence on potential vendors
Information Security
Infrastructure Layer

• Threats
  – Network and host intrusions, DDoS, DoS, EDoS
  – Improper network and host segregation between customers

• Mitigation steps
  – Network access control and in-transit data encryption
  – Intrusion detection and prevention systems
  – Securing and compartmentalizing the virtualization layer

• Allocation of responsibility
  – SaaS & PaaS – Vendor responsible for network, hosts, and virtualization layer including all virtual machines (VMs)
  – IaaS – Vendor secures the network, hosts and virtualization layer, except customer is usually responsible for security management of its VMs
Information Security
Application Layer

• Threats and risks
  – Programming errors, back doors, poor patch management, hackers, viruses

• Mitigation steps
  – Secure code design, and periodic code review
  – Apply mature service management processes

• Allocation of responsibility
  – SaaS – Vendor should own security management for the full stack
  – PaaS – Vendor should own security up to the runtime engine, customer owns security for remainder of the apps it develops
  – IaaS – Customer fully owns all aspects of app and database security management
Information Security
Data Layer

- Threats to data are heightened by shared / multi-tenant storage architecture used by public clouds
  - Unauthorized access or disclosure
  - Loss or corruption
  - Impaired data lineage (where has the data been?)
  - Concerns about data processing accuracy (provenance)
  - Data remenance (gone but not forgotten)
Information Security
Data Layer

- Mitigation steps
  - Encryption – but it has its limits
  - Identity and access management (IAM) to enforce access rights and role-based permissions
  - Back-up and DR processes, procedures and tools
  - Data cleansing and sanitization
  - Avoid placing sensitive unencrypted data in public clouds
Information Security
Data Layer

• Allocation of responsibility in public clouds
  – SaaS
    • Vendor fully responsible, except end user notifications
    • Encryption
      – All in-transit data should be encrypted (e.g., VPNs)
      – Not always available for at rest data – impact on indexing and search-ability
      – Data is unencrypted while it is being processed
  – PaaS
    • For vendor-provided storage, vendor should be fully responsible
    • Otherwise, it depends on the deployment options selected
  – IaaS - Customer is primarily responsible for data security management
Information Security
User Access / Authentication Controls

• Standards and best practices are under development
• Key identity and access (IAM) management tasks
  – Identification
  – Authentication
  – Role based authorization
  – Monitoring and auditing access
• Federated single sign on (SSO) is IAM nirvana
Privacy and Compliance Programs

• You can assign privacy responsibility to vendors, but you can’t delegate-away accountability through contracts
• Map internal key controls to vendor responsibilities
  – Sources for key controls
  – Conduct pre-contract due diligence using a vendor information security questionnaire and key control mapping
  – Gap closure should become contractual commitments
• Governance mechanisms to manage vendor compliance
• Retain strong customer audit rights but . . .
  – Will vendors provide enough transparency?
  – Reliance on information security standards frameworks
    • Useful – ISO 27001 / 27002 and SysTrust
    • Not so much – SAS 70s
• Expose stealth subcontractors and multi-layered cloud suppliers, and include them in the program
Contracting Tips
Soliciting Proposals

- Enterprises must use a competitive (RFP) process to get a good deal
  - Identify 4 to 5 service providers, and assume at least 1 will “no bid”
  - Determine desirable vendor characteristics
    - E.g., Competitive price, quality, industry recognized leadership, geographic footprint, financial health, willingness to negotiate fair Ts & Cs, reputation, organizational culture, scope of services, process maturity
  - Due diligence to vet candidates before the RFP is issued
    - Consult with outside advisors
    - Check with other organizations
    - Financial health check (including “for sale” signs)
  - Select best bid(s) applying an apples-to-apples comparison through multiple down-select rounds
Commitments, Term and Pricing

• Term
  – Don’t need to commit to term, but vendors may try to make a term more attractive
  – Anything longer than 1-year should be scrutinized
  – Renewals at the customer’s option
  – Negotiate the early termination fees

• Revenue or resource minimum commitments
  – There shouldn't be any – they defeat the elasticity / scalability / on-demand public cloud benefits
  – Vendors may offer better unit pricing in exchange for minimum subscription levels and terms
Commitments, Term and Pricing

• Pricing models
  – IaaS
    • Per resource / per hour, day, month
      – Servers (physical/virtual); processing power; memory; applications; back-up
    • Charges for upgraded support, maybe implementation
  – PaaS
    • Per user / month
    • Per resource / per hour, day, month
    • Charges for upgraded resources, support
  – SaaS
    • Per user or concurrent user / per month, year
    • Per use (e.g., WebEx)
    • Extra charges for customization, implementation, upgraded support
    • Charges for additional storage
Service Levels

• Public cloud deals must include SLAs
• Deconstructing the SLA
  – The three distinct parts of an SLA:
    • The metrics and minimum requirements
    • The remedies
      – Pay credits
      – Fix it
      – Let the customer go
    • The conditions
Service Levels

• Key SPI SLA metrics
  – System availability/uptime
  – Management portal/tools availability/uptime
  – Incident response and problem-resolution times
  – Service desk performance
  – Back up data success rate, and data restoration times whenever the vendor hosts the customer’s production data
Service Levels

• Key IaaS-specific metrics
  – Resource deployment timeliness
  – Configuration change timeliness

• Key SaaS-specific metrics
  – Application response time
  – End user satisfaction
Service Levels

• SLA best practices
  – Credits should be proactively applied
  – Credits should vary based on the severity, duration and frequency of the service failures
  – Vendor root-cause analysis and corrective actions
  – Escalation of chronic or critical service-level problems
  – Chronic / critical failure remedies
  – Right to terminate for pre-defined critical failures
Vet End User Terms of Use

• PaaS and SaaS providers often attempt to push through click-wrap agreements to individual end users that access the cloud (EULAs)
  – Who are they trying to bind?
  – How do they affect the Ts&Cs in the enterprise agreement?
  – What about subsequent changes to the EULA?
Intellectual Property Matters

- Licenses to vendor’s intellectual property to use the services
- Incorporation of third-party licenses for vendor-provided software
  - Push back on entering into direct contracts with vendor’s suppliers
  - Consider using your own enterprise license with the third-party licensor
  - Vendors will attempt to disclaim responsibility for their third-party licensors
- Required consent from customer’s third-party licensors
- Allocation of intellectual property rights in new developments
  - Who should own the new work?
  - The other party gets an appropriate license
- Infringement indemnifications
  - Geographic limits on covered claims
  - Carve-outs for combinations and modifications
  - Exclusion from limits on liability
Managing Disputes

• Disputes between provider and customer
  – Which jurisdiction and venue applies?
  – Litigation or binding arbitration
  – The power of informal escalation

• Disputes with third parties arising out or cloud services
  – Consumers
  – Business partners
  – Employees
  – States, the Feds and foreign countries
Risk Shifting

• Confidentiality clauses
  – Include the boiler plate plus vulnerabilities, security events, and protections within scope of the provider’s responsibility

• Representations and warranties

• Other indemnifications covering 3rd party claims

• Disclaimers of liability and limitations on liability that don’t excuse the vendor from failing to perform its essential function

• Tailored force majeure clauses
Exit Strategies

• Termination for convenience
  – Most vendors require a termination fee of some sort
  – The termination fee should not be unduly punitive

• Termination for cause
  – Uncured material breach by either party
  – Vendor causes a “Critical Performance Failure”

• Post-termination rights
  – Cooperation and assistance with the new cloud vendor or internal staff
  – Return of any prepaid subscription fees intended to provide coverage during the unused portion of the service period
  – Migration assistance over an appropriate period
  – Access to and assistance with porting tools
Closing Thoughts
Enterprise Adoption

- **Cloud Myths vs. Reality**
  - It is not a new technology trend that will pass
  - It will not destroy on-premises traditional IT in the enterprise
  - Lock-in, security and privacy concerns are genuine
  - Open cloud standards must be developed to facilitate wide enterprise adoption

- **Public and hybrid clouds are valuable delivery methods in the right contexts**
  - Approach the cloud with a long-term vision
  - Negotiate your cloud contracts today to establish strong foundations that will support increasing reliance on cloud services
Questions?