Cloud Computing – Lessons Learned

CIO New York Summit 2014

Arthur Riel
April 10th, 2014
Cloud: The Sweet Spot (IaaS)

- The virtualization and commoditization of infrastructure has benefited numerous organizations
- Servers, storage and bandwidth are now priced like electricity
- Cloud promises agility and elasticity
- Many large organizations are effectively using cloud to run 100% of their operations: Netflix, Four Square.
Cloud: The Sweet Spot

- Data center decentralization has become very inexpensive, benefiting larger organizations
- Data center centralization has become less expensive (e.g. Indonesia)
- The World Bank is focused on the former
Cloud: The Sweet Spot (PaaS)

- Vendors are offering many platforms as a service
- SharePoint, Documentum, Jive, SAP
- Total cost of ownership can be substantially less than on-premise based solutions and solutions can be deployed much faster
Cloud: The Sweet Spot (SaaS)

- Vendors are offering many shrink wrapped packages in the cloud
- SalesForce, Sugar CRM, DropBox, Box, O365
- Turnkey solutions can allow an organization rapid deployment opportunities at much lower cost
Benefits of Cloud

1. On-demand Self-service
2. Resource Pooling
3. Broad Network Access
4. Rapid Elasticity
5. Measured Services

1. Software as a Service (SaaS)
2. Platform as a Service (PaaS)
3. Infrastructure as a Service (IaaS)
Cloud computing providers offer different deployment models

- Cloud solutions can be configured in many ways. Each deployment model has its own risk and cost characteristics:

  - Private clouds are services used exclusively by one organization and offer the greatest control.
  - Community clouds are services used by organizations that have shared concerns (e.g., UNICC).
  - Public clouds are services for open use by the general public (e.g., Microsoft Azure, Amazon Web Services).

Note: Illustration based on NIST service deployment models (Cloud Computing Reference Architecture, Special Publications 500-292).
Cloud: You are Already There!

- IT acquisition has gone from the enterprise to the end user, 180 degree turnaround
- End users are bringing solutions, many dangerous, into the enterprise, e.g. DropBox
- Webmail, SalesForce, Google Apps are already exposing organization’s confidential data outside of the perimeter
- The World Bank has thousands using these solutions without oversight
Preparing a Cloud Roadmap

- Creating a risk matrix that cross references data categories (strictly confidential, confidential, internal use only, public) with impact analysis (low, medium, high, extreme)
- Creating a risk governance process around the risk matrix, e.g. what body signs off on which risks
- Setting priorities: File sharing, email, web farm, databases, infrastructure (e.g. dev/QA servers) and storage
- Creation of the roadmap itself with dependencies, e.g. web applications/data source dependencies
- Opportunistic versus greenfield cloud migration
An Example Risk Matrix and Associated Governance Model

- Since some risks cannot be mitigated, an organization will need to accept residual risks as worthwhile in return for the advantages gained by adoption of cloud computing.

- A Cloud Computing Program Office (CCPO) should be created to work with the business to assess the potential impact and the appropriate deployment model, mitigating controls and acceptance of risk.

- The control framework will be implemented incrementally based on the CCPO assessment.

- Impact will be evaluated on a case by case basis and accepted by the corresponding authorities specified in the framework.

![An Example Risk Matrix and Associated Governance Model](image)

**CONTROL FRAMEWORK**

- Contractual Agreements
- Certification & Accreditation
- Periodic Risk Assessment/Review
- Data Encryption
- Security Architecture Assessment
- Security Certification
- Onsite Review
- External Penetration Testing
Case Studies

- File Sharing (Greenfield)
  - Created to address end user need
  - End users using DropBox and/or webmail to access files remotely – Corporate exposure
  - Box versus SkyDrive
- Email (Opportunistic)
  - O365 Cloud (Possibly Hybrid)
- Collaboration (Greenfield)
  - Jive and SharePoint in the cloud
- World Bank Web Farm (Opportunistic)
  - Web Farm hardware reached end of life
  - Complications: VPN latency
- Storage (Opportunistic)
  - Legacy Document Management
- Development/QA Servers
- CRM (Greenfield)
  - SalesForce/Sugar CRM/Dynamics
Risks

- Legal Risks
  - External data exposure
  - Reputational Risks
  - Immunities and Privileges
  - Thought: Why do you believe the cloud is less secure than on-premise?
  - Thought: Organizations already have their data outside of their perimeter, e.g. World Bank archives

- IT Security Risk
  - Similar concerns and thoughts as legal risk

- Operational Risk
  - SLAs often lack teeth

- Vendor Risk
  - Viability concerns

- Contract Risk
  - Contract renegotiations can cause problems due to the sticky nature of cloud deployments
Legal and IT Security Risk

- Ensure timely notification of subpoenas
- Geographic selection criteria
- Ensure proper security around the perimeter, e.g. encryption in transit/at rest, access logging
- IT Security review of all security assets of the cloud provider
- Requires substantial investment in hardware/software on-premise
Operational Risk

- Ensure a well crafted SLA with the cloud provider
- Examine current track record
- Work with reputable vendors
- IT Infrastructure/Architecture need to assess and review cloud providers setup and procedures
- Study BCP and DR capabilities
- Challenge: Vendors rarely provide financial penalties for missed SLAs
Vendor Risk

- Viability of the vendor is more important than with on-premise providers
- Bankruptcy can result in loss of service rather than simply a technology roadmap
- Contract dispute can imply loss of service
- Work with reputable vendors
- Ensure contract includes provisions for service continuity in the event of a contract dispute
- On premise backup plan strategies? These can be costly
Contract Risk

- Cloud based deployments tend to be stickier than on-premise
- Year-to-year nature of the service pricing can mean large price swings in the future
- Work with reputable vendors
- Ensure contract includes provisions for service continuity in the event of a contract dispute
- Ensure contract includes provisions for long lead times on price increase notification
- Ensure an exit strategy from the cloud, e.g. data dump of your CRM data, email data
A Caveat for the Cloud

- There is little case law in cross border cloud disputes and issues
- As the cloud obscures where data and solutions exist, as well as the number of instances and jurisdictions, there are possible complexities
- Some organizations (especially governments) implement their own internal cloud to avoid these legal issues
- These types of issues are not new to the cloud, US/EU email case study
Questions and Comments?