Cloud Computing: Security, Risk and Governance Issues & International Developments in the Banking Sector

Panagiotis Droukas CISA, CRISC, CGEIT

Business Case for Cloud Computing

- www.c-ebs.org average traffic during 2010 was 1K hits per day
- On Friday, July 23 2010 the EU wide stress test results were to be published
- From 17:30 BST onwards www.c-ebs.org traffic was expected to exceed 1K hits per minute, that is more than 1.5M hits per day
- The decision to publish the results and host a press conference was taken only a month ago

Business Case in Detail

- On the day of the event, www.c-ebs.org had to support downloading of large documents and live video streaming
- Investors, journalists and banks form all over the world were expecting the publication of the stress test results
- Disruptions in the live feed or glitches in document downloading would have caused problems ranging from negative publicity to stock market panic

First Thoughts

- Can our web hosting provider support this kind of transaction volume?
- Is it possible to upgrade the web site in less than a month?
- Is the network provider capable of providing more than 1.500x the current throughput?
- How much money for the whole package?
- What happens after the event? Should I continue spending money for services that I do not use?
- Will this solution suffice for next year?

Best Solution: Cloud Computing

- Pay as you go model
- Natural fit for small organizations
- Deadlines too close to try other solutions
- Costs seemed reasonable
- Hosting provider had experience with AWS S3
- Scalable Platform
- Up to the minute information on service availability
- Global coverage (Asian markets were expecting the results first)

Second Thoughts

- Does the web part moving to the cloud contain confidential / private information?
- Who is responsible in case something goes wrong? Hosting provider, cloud provider or both?
- Impact on internal controls, reputation
- Do we put live video streaming in the Cloud?
- Will Cloud Computing compromise in any way our internal IT infrastructure?
- How can we monitor performance?

Selection Criteria

- Which provider?
- Success stories / track record
- Business contingency management
- Monitoring functionality
- Certifications and Accreditations (SAS70 Type II, SSAE 16 SOC 1, ISO 27001)
- …
- I need help!

Some Useful Resources

- Cloud Computing: An Auditor's Perspective, ISACA Journal Vol. 6, 2009
- Cloud Computing: Benefits, risks and recommendations for information security, ENISA, 2009
- Cloud Computing Management Audit / Assurance Program, ISACA, 2010
- IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud, ISACA, 2011
- Guiding Principles for Cloud Computing Adoption and Use, ISACA White Paper, 2012

Banking Regulators and Cloud Computing

	Guideline	Regulatory Process
Monetary Authority of Singapore	Y	Y
Australian Prudential Regulation Authority	Y	Y
Comisión Nacional Bancaria y de Valores	N	Y
Nationale Bank van België	N	N
De Nederlandsche Bank	Y	N

Monetary Authority of Singapore

- A thorough risk assessment is required prior to entering a contract
- A complete questionnaire should be sent to MAS and MAS should be consulted
- Unique Risks:
  - Data integrity, confidentiality and recoverability
  - Ability to isolate customer data in case of multiple customer environment

Monetary Authority of Singapore

- Unique Risks:
  - Removal / destruction of data in case of contract termination
- Concerns:
  - Nested cloud scenarios

Australian Prudential Regulation Authority

- Concerns:
  - a financial institution’s ability to continue operations and meet core obligations, following a loss of cloud computing services;
  - confidentiality and integrity of sensitive (e.g. customer) data/information; and
  - compliance with laws and regulations

The Situation in EU

- Financial Institutions (FIs):
  - are experimenting (e.g. web / mail services, test environments, etc.)
  - try to balance cost, benefits and security
  - are looking for guidance on reference frameworks (ISACA, ENISA, Cloud Security Forum)
- Cloud Providers:
  - mostly ignorant on legal and regulatory requirements
  - contracts are usually "non-negotiable "

Related Supervisory Publications

- **Monetary Authority of Singapore,** Circular TR 01/2011: Information Technology Outsourcing http://www.mas.gov.sg/legislation_guidelines/banks/circulars/Banks_Circulars.html
- **Australian Prudential Regulation Authority,** Outsourcing and Offshoring: Specific considerations when using cloud computing services http://www.apra.gov.au/GI/Documents/Letter-on-outsourcing-and-offshoring-ADI-GI-LI-FINAL.pdf
- **De Nederlandsche Bank NV(DNB)**, Circular Cloud Computing http://www.toezicht.dnb.nl/binaries/Cloud%20computing_tcm50-224828.pdf

Thank you!

Panagiotis Droukas, CISA, CGEIT, CRISC
Treasurer, ISACA Athens Chapter
pdroukas@bankofgreece.gr