Financial Services and the Impact of New Technology

A SEMINAR HOSTED BY
THE VIETNAM BANKS ASSOCIATION
SUPPORTED BY AMCHAM HCMC, EUROCHAM
HCMC AND THE OPEN COMPUTING ALLIANCE, UK
NIKKO HOTEL,
HO CHI MINH CITY
JUNE 17TH 2014

MR. MICHAEL MUDD
SECRETARY – GENERAL, ASIA - PACIFIC
OPEN COMPUTING ALLIANCE-LONDON, UK
CHAIR, IT, IP AND TELECOM COMMITTEE,
AMCHAM HANOI
The numbers - by 2020 computing will process;

- Over 2 trillion financial transactions*
- On 31 billion devices*
- By 4 billion internet users*
- Using 25 million applications*
- Creating 1.2 Zettabytes of storage\(^1\)
- With Cloud spending reaching $250bn\(^2\)

---

1 Zt = 1000 Exabyte's or \(10^{21}\) bytes

\(^1\) Gartner Group
\(^2\) Forrester Research
Technology Evolution

Technology

Centralized computing & storage, thin clients

Economic

Optimized for efficiency due to high cost

Business

High upfront costs for hardware and software. ‘Analog ‘Mindset’

PCs and servers for distributed computing, Captive Outsourcing.

Optimized for agility due to low cost

Perpetual license for OS and application software. ‘Mindset’ evolving

Very large DCs, Virtualisation, Multi Tenant Outsourced Services

Order of magnitude higher efficiency and agility

Pay as you go, and only for what you use. Fully ‘Digital Mindset’
Why Implement Cloud?

**Benefits**
- ROI is great - 3x less costly
- OpEx vs CapEx
- Growth on demand

**Challenges**
- Need to speak “cloud”
- Requires changes (the regulator)
- Latency kills performance
- Security concerns
The OCA has had discussions in:
- Singapore
- Hong Kong
- Thailand
- Philippines
- Australia
- Vietnam

Banks and Insurance companies (and Regulators).
Service Providers (SP’s).
Industry Associations and Chambers.
What are the real issues to address?
Why New Technology?

- Bank core IT systems 50 years old; obsolete
- Major banks to increase capital ratios under Basel 3.
- Insurers and Securities companies need to lower costs?
- 4 years ago Cloud not on any FSI’s horizon for any SaaS, IaaS, etc under any circumstances; public; private or hybrid.
- Today the challenge is to reduce capex – to do this flexibility in opex is a must – Cloud delivers.
- The risk control question is really about confidence in audit and control, both from banks and the regulators.
Cloud is delivering for Banks now

- For Banks/FSI, Cloud is being adopted today.
- AXA, Capita PLC, Rabo Bank, Robeco, MKB Bank in France, the UK Netherlands and Hungary are using hybrid services hosted in Ireland.
- TienPhong Bank is using Cloud for banking now.
- Enterprise cloud is mature – look at USG; FISMA, FedRamp, HIPPA.
- SSAE 16 provides international audit standards
Some FSI’s already ‘in the cloud’?
Cross - Border Data Flows

- Efficiencies and benefits of cloud computing are best achieved when data – information - flows freely across borders – APEC, TPP, AEC
- The same as business in general; it’s all global now
- Privacy laws that overly restrict such flows can be an impediment to economic growth
- It’s the audit trail that is regulators - and investors - real concern
- This has been done for decades by the FSI
Security and Regulatory Challenges:

10 years ago...
- Security and privacy top of mind
- Hacking, virus propagation, cyber-espionage and cyber-warfare on the rise
- Enforcement officials need tools & training
- Vehicles for cross-border collaboration inadequate

Today...
- Security and privacy top of mind
- Hacking, virus propagation, cyber-espionage and cyber-warfare on the rise
- Enforcement officials need tools & training
- Vehicles for cross-border collaboration inadequate
So what has changed? It's all about trust

- **Service provider practices;**
  - Does the service provider have a documented information security program, and what does it say?
  - What security certifications does the service provider have?
  - Do they comply with your audit – and the regulators, needs?

- **Clear responsibilities of each party e.g., in the event of a data breach?**

- **Secure Frameworks for Cloud Computing now being implemented by Govt and SP’s.**

- **Third party security and business audits.**
Standards, Audits and Certifications

23001, 27001 & 31000

Article 29 compliance

FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA) IMPLEMENTATION PROJECT

Protecting the Nation’s Critical Information Infrastructure

Our Vision
To promote the development of key security standards and guidelines to support the implementation of and compliance with the Federal Information Security Management Act including:
What is the Article 29 Working Party?

- Set up under the EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data.
- Provides advice on whether countries outside of the EU adequately protect personal data transferred from the EU.
- Approve codes of conduct for the processing of personal data.
- Given that the EU has some of the most advanced data protection regulation in the world, these authorities play a critical role in global privacy law.
What are Model Clauses and why do they matter?

- The Model Clauses are a set of provisions developed by the Article 29 Working Party
- Adopted by the European Commission for use in contracts between service providers (like Microsoft) and their customers
- Designed to help ensure appropriate safeguards are in place to protect personal data that leaves the European Union
- Preferred way to legitimize the transfer of personal data outside the European Union
- Under EU law, Cloud customers remain the “controllers” of the personal data they collect and the primary obligations to protect that data rests with the Cloud customer
- Cloud providers that commit contractually to comply with the Model Clauses give their customers with needed reassurance that the data will be processed in compliance with strong EU data protection laws
Executive Order 13636—Improving Critical Infrastructure Cybersecurity

“It is the policy of the United States to enhance the security and resilience of the Nation’s critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties”.

NIST is directed to work with stakeholders to develop a voluntary framework for managing and reducing cyber risks to critical infrastructure, including banking.
The Framework

- **Includes** a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks.

- **Provides** a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk.

- **Identifies** areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations able technical innovation and account for organizational differences include guidance for measuring the performance of an entity in implementing the Cybersecurity Framework.

Courtesy Tim Grance, Cybersecurity Head, NIST
What does Business Really Want?

- To deliver services with:
  - Data Security
  - Confidentiality
  - Integrity
  - Availability
- To reduce costs and improve service.
- To respond to customers needs faster.
- To improve the balance sheet.
- To keep the regulators happy...
What do Regulators Really NEED?

- Example; Singapore is looking at Cloud as ‘3 P’s’*
  - Principles
  - Preparedness
  - Partnerships

- This may enable SP’s to deliver services with:
  - Confidentiality
  - Integrity
  - Availability

- Satisfying their due diligence process and minimizing risks.

What are FSI regulators doing?

**Singapore (MAS):**

MAS does not prohibit cloud computing. In fact, MAS has approved its use in particular cases.

*2013 MAS Guidelines on Technology Risk Management* *
- Statements of industry best practice for FSIs to adopt
- Observance of guidelines impact MAS’ risk assessment of an FSI
- FSI must have proper policies and procedures to evaluate, approve, review and control and monitor risks
- Emphasise powers to carry out inspections, supervise and examine service providers and facilities
- Specific attention to cloud providers’ abilities to isolate and ID customer data and right to request removal and destruction of data on termination

**Philippines (BSP)**

*2013 Circular 808 - Enhanced Guidelines on Information Technology Risk Management*

A 10 point framework

- Data and Location Transparency
- Limits On Data Use
- Data Separation or Isolation
- Conditions on Subcontracting
- Service Provider Reputation and Competence
- Confidentiality and Certified Security Standards
- Review, Monitoring and Control
- Audit
- Resilience and Business Continuity
- Conditions on Termination
Some Closing Thoughts

The FSI sector and forward looking regulators are already recognizing the transformational impact of new technology.

A principle driven framework may further assist Regulators to address Cloud services.

The ideas presented here may address some of their concerns.
What next?

Banks and their associations may work with the IT industry to create an acceptable set of recommendations to manage risk.

Regulators can take a lead and contribute to global best practices in markets for outsourced services.

Recommendation:
Industry and regulators need to agree a principle driven framework for Cloud enabled outsourcing.
The OCA

- UK based global ICT industry policy think tank with advocacy
  - Members are technology leaders in Asia - Pacific economies
- Creating Dialogue on Technology Policy;
  - Open Innovation and Competition.
  - Open Standards.
  - Fair trade and respect for IPR.
  - *Cloud Computing for Secure & Trusted IT.*
  - Energy efficient IT processes.
- ...to drive positive outcomes for all stakeholders - both public and private.
- Office in Hong Kong for Asia Pacific*. 
  
  mmudd@opencomputingalliance.org
  
  www.opencomputingalliance.org

* Represented by Asia Policy Partners LLC