Law and Regulatory Policy Meets Data in the Cloud

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

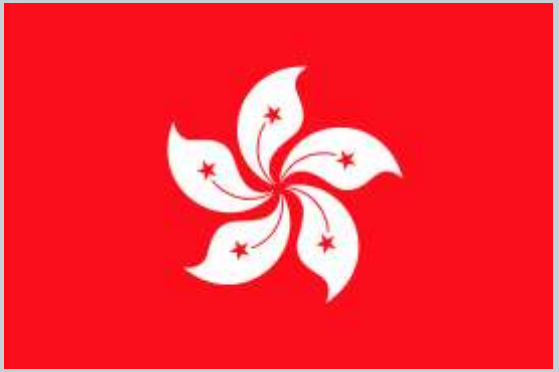
MR. STACY BAIRD
POLICY ADVISOR, ASIA – PACIFIC
OPEN COMPUTING ALLIANCE
HONG KONG

Meeting Regulator's (and Internal) Requirements

- **FIs must maintain control over their activities & Data**
- **Financial Regulators must be able to audit the CSP**
- **FI's Data, particularly Customer Data, must be kept in strict confidence and not be used for any other purpose than providing the service to the FI**
- **Security requirements are prescriptive**
- **There must be transparency as to the exact location of the FI's Data**
- **FI Customer Data must be segregated from all other data**

Guided by what? Compared to what?

- **Singapore**
  - MAS Outsourcing Guidelines
  - MAS TRM Guidelines
  - MAS Outsourcing Questionnaire
  - MAS Banking Secrecy Notice
  - Banking Act
  - PDPA



- **Hong Kong**
  - HKMA Outsourcing Guidelines
  - HKMA Technology Guidelines
  - HKMA BCP Guidelines
  - PDPO

- **Australia**
  - APRA Outsourcing Standard
  - APRA Outsourcing Guide
  - APRA Security Guide
  - APRA BCM Standard
  - APRA Data Risk Guide
  - APP

1. Data Location and Transparency

- **CSPs must disclose exactly where Data will be located.**
- **FIs should ensure that the government policies, economic and legal conditions of the identified locations are safe and stable.**

MAS Outsourcing Guidelines Para 6.2, 6.3
MAS TRM Guidelines Para 5.1, 5.2
MAS Outsourcing Questionnaire
MAS Banking Secrecy Notice

HKMA Outsourcing Guidelines Para 2.2, 2.3

APRA Outsourcing Standard Para 22
APRA Outsourcing Guide

2. Limits On Data Use

- **CSPs should not use FI's Data for any purpose other than that which is necessary to provide the Cloud Service.**
- **The contract should prevent CSPs from using FI Data for any secondary purpose at all times.**

MAS Outsourcing Guidelines, Para 6.7
MAS TRM Guidelines, Para 5
MAS Outsourcing Questionnaire

HKMA Outsourcing Guidelines, Para 2.1, 2.6

Banking Ordinance, Seventh Principle

APRA Outsourcing Standard, Paras 17 and 37
APRA Outsourcing Guide

3. Data Separation or Isolation

- **FI Customer Data must be segregated from other Data held by the CSPs. CSPs must be able to identify the FI's Customer Data and at all times be able to distinguish it from other Data held by the CSP.**

MAS Outsourcing Guidelines, Para 6.8
MAS Banking Secrecy Notice
MAS Outsourcing Questionnaire

HKMA Outsourcing Guidelines, Para 2.8

APRA Outsourcing Standard, Para 30

4. Conditions on Subcontracting

- **CSPs may only use subcontractors if the subcontractors are subject to equivalent controls as the CSP.**

MAS Outsourcing Guidelines, Para 6.5
MAS TRM Guidelines
Banking Act, Section 47
MAS Banking Secrecy Notice
MAS Outsourcing Questionnaire
PDPA, Section 24

HKMA Outsourcing Guidelines, Para 2.5
HKMA Technology Guidelines
PDPO, Schedule 1, Data Protection Principles, 4

APRA Outsourcing Standard, Paras 21 and 41
APRA Data Risk Guide
APRA Security Guide
APP 11

5. Service Provider Reputation & Competence

- **FIs must carry out, and CSPs must assist in facilitating, a risk assessment and due diligence on the CSP to ensure that the CSP and its services meet the legal, regulatory, contractual and business requirements.**
- **FIs should have in place a risk management plan that includes measures to address the risks associated with the use of Cloud Services.**

MAS Outsourcing Guidelines, Para 6.6
MAS BCM Guidelines
MAS TRM Guidelines
MAS Outsourcing Questionnaire

HKMA Outsourcing Guidelines, Para 2.7
HKMA Technology Guidelines, Para 5.4
HKMA BCP Guidelines

APRA Outsourcing Standard, Para 23 and 41
APRA BCM Standard
APRA Data Risk Guide

6. Confidentiality & Certified Security Standards

- **CSPs must be certified to have and maintain robust security measures and comprehensive security policies that meet or exceed international standards (ISO27001 at a minimum).**
- **CSPs should use encryption technology that meets or exceeds international standards to protect and secure the FI's Data at all times.**

MAS Outsourcing Guidelines, Para 6.9
MAS Outsourcing Questionnaire
PDPA, Section 26

HKMA Outsourcing Guidelines, Para 2.9
PDPO, Section 33

APRA Outsourcing Standard, Para 35
APRA Outsourcing Guide
APP 8

7. Review, Monitoring and Control

- **CSPs must provide regular reporting and information to demonstrate continued compliance with the legal, regulatory, contractual and business requirements throughout the duration of a contract.**
- **FIs and CSPs must meet regularly to review the reports and performance levels.**
- **The contract must provide for an effective mechanism for remedial actions arising from any issues that emerge or non-compliance.**

MAS Outsourcing Guidelines
MAS Outsourcing Questionnaire
PDPA, Section 18

HKMA Outsourcing Guidelines, Para 2.5.2
PDPO, Schedule 1, Data Protection Principles, 3

APRA Outsourcing Standard, Para 21
APRA Data Risk Guide
APP 3

8. Audit

- **Most Financial Regulators require that CSPs allow the Financial Regulator rights to carry out an inspection of the CSP.**
- **This will enable the Financial Regulator and FI to confirm that CSPs are complying with these Principles, regulatory, contractual and business requirements of the FI.**

MAS Outsourcing Guidelines, Para 6.5
MAS TRM Guidelines, Para 5.2
MAS Outsourcing Questionnaire

HKMA Outsourcing Guidelines, Para 2.5.2

APRA Data Risk Guide

9. Resilience and Business Continuity

- **The Cloud Service must be reliable and be able to document that reliability.**
- **CSPs must have an effective business continuity plan with appropriate service availability, recovery and resumption objectives and with regularly tested and updated procedures and systems in place to meet those objectives.**
- **The risks of downtime should be minimized through good planning and a high degree of system resilience.**

MAS Outsourcing Guidelines, Para 6.4
MAS Outsourcing Questionnaire
PDPA, Section 17

HKMA Outsourcing Guidelines, Para 2.6
PDPO, Schedule 1, Data Protection Principles, 4(2)

APRA Outsourcing Standard, Para 25 and 26
APRA Outsourcing Guide
APP 6

10. Conditions on Termination

- **FIs must have appropriate exit provisions in the contract with the CSP. To the extent that the FI requires, on termination, the CSP must work with the FI to return the FI's Data to the FI and then the CSP must permanently delete the Data from the CSP's systems.**
- **Any Data that does not need to be returned to the FI must be permanently deleted by the CSP.**

MAS Outsourcing Guidelines, Para 6.4
MAS Outsourcing Questionnaire
MAS TRM Guidelines
PDPA, Section 25

HKMA Outsourcing Guidelines, Para 2.5.4
PDPO, Schedule 1, Data Protection Principles, 2(3)

APRA Outsourcing Standard, Para 25
APRA Outsourcing Guide, Para 15
APP 11

Next Steps

Building on these Principles, industry, service providers and regulators can work together to establish a principle-driven regulatory 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*.
- URL: www.opencomputingalliance.com
- Contact: mmudd@opencomputingalliance.com

* Represented by Asia Policy Partners LLC