Nguyên Tắc Đám Mây An Toàn Dành Cho Hệ Thống Tổ chức tài chính

HỘI THẢO TỔ CHỨC BỞI
HIỆP HỘI NGÂN HÀNG VIỆT NAM
ĐỒNG TỔ CHỨC BỞI HIỆP HỘI THƯƠNG MẠI HOA KỲ, HIỆP HỘI THƯƠNG MẠI CHÂU ÂU VÀ CÔNG TY OPEN COMPUTING ALLIANCE, ANH QUỐC
,
JUNE 17TH 2014

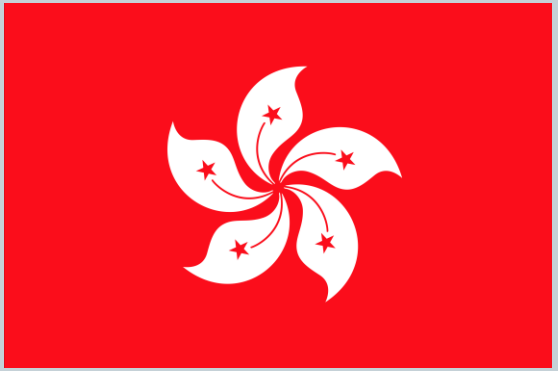
ÔNG . STACY BAIRD
CỐ VẤN VỀ CHÍNH SÁCH, CÔNG TY OPEN COMPUTING ALLIANCE HỒNG KÔNG
CHI NHANH CHÂU Á THÁI BÌNH DƯƠNG

Đáp Ứng Yêu Cầu Các Cấp Quản Lý & Nội Bộ

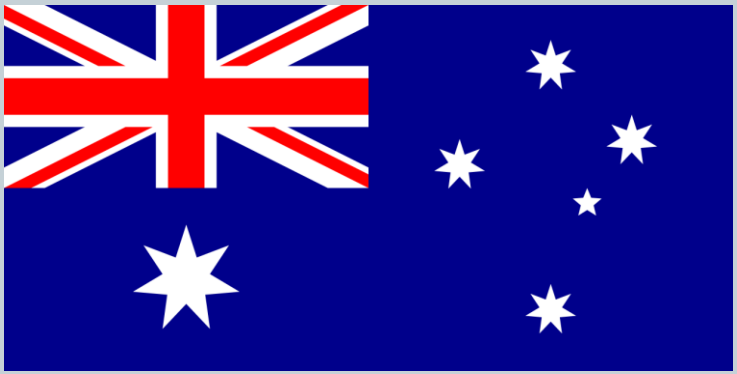
- **Các tổ chức cung ứng dịch vụ tài chính phải duy trì được việc quản lý các hoạt động cũng như các số liệu liên quan.**
- **Cơ quan quản lý tài chính phải có khả năngkiểm toán các nhà cung cấp dịch vụ**
- **Dữ liệu tài chính, đặc biệt là thông tin khách hàng, phải được lưu trữ bảo mật và an toàn, không được sử dụng vào bất cứ mục đích nào khác ngoài cung cấp thông tin để hỗ trợ các nhà quản lý tài chính trong hoạt động kinh doanh.**
- **Các yêu cầu bảo mật phải chặt chẽ và xây dựng theo quy chuẩn**
- **Yêu cầu sự minh bạch trong việc sắp xếp địa điểm lưu trữ các dữ liệu tài chính**
- **Thông tin khách hàng phải được tách riêng với các loại dữ liệu, thông tin khác.**

Hướng dẫn bởi ai? So sánh với hệ thống nào?

- **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. Địa điểm lưu trữ và sự minh bạch trong quản lý

- **Nhà cung cấp dịch vụ điện toán đám mây phải chỉ rõ địa điểm các dữ liệu được lưu trữ.**
- **Các tổ chức tài chính phải đảmbảo Địa điểm lưu trữ thông tin dữ liệu tài chính ổn định và an toàn về mặt chính sách quản lý, kinh tế, và thủ tục pháp lý.**

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. Giới hạn trong việc sử dụng dữ liệu

- **Các nhà cung cấp dịch vụ điên toán đám mây không được phép sử dụng các thông tin tài chính vào bất cứ mục đích nào khác ngoài cung cấp cho dịch vụ cho khách hàng.**
- **Hợp đồng ký kết phải ghi rõ việc không cho phép các nhà cung cấp dịch vụ sử dụng dữ liệu tài chính cho bất kỳ mục đích nào khác.**

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. Tách biệt hoặc cách ly dữ liệu

- **Thông tin khách hàng phải được tách biệt với các loại thông tin khác. Các nhà cung cấp dịch vụ phải xác định được các tệp thông tin khách hàng và phân loại riêng rẽ với các dữ liệu khác.**

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. Điều kiện sử dụng nhà thầu phụ

- **Các nhà cung cấp dịch vụ điên toán đám mây chỉ có thể sử dụng các nhà thầu phụ khi mà các nhà thầu này thuộc quyền quản lý và giám sát của các nhà cung cấp đó.**

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. Năng lực và danh tiếng của nhà cung cấp dịch vụ

- **Các tổ chức tài chính dưới sự hỗ trợ của nhà cung cấp dịch vụ thực hiện đánh giá rủi ro và thẩm định hoạt động để đảm bảo các nhà cung cấp dịch vụ hoàn thành đầy đủ nghĩa vụ pháp lý, các điều khoản của hợp đồng giữa hai bên.**
- **Các tổ chức tài chính cần có sẵn kế hoạch đánh giá rủi ro bao gồm các biện pháp kiểm soát những nguy cơ tiềm ẩn khi sử dụng dịch vụ điện toán đám mây.**

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. Bảo mật & các tiêu chuẩn chứng nhận an toàn

- **Các nhà cung cấp dịch vụ cần phải có các hệ thống đo lường bảo mật tiêu chuẩn và các quy định bảo mật chặt chẽ được công nhân trên toàn cầu (ISO27001)**
- **Các nhà cung cấp dịch vụ nên sử dụng các công nghệ được mã hóa được tiêu chuẩn hóa toàn cầu để đảm bảo sự an toàn cho các dữ liệu, thông tin tài chính trong bất kỳ hoàn cảnh nào.**

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. Xem xét, theo dõi và quản lý

- **Trong suốt quá trình hợp đồng có hiệu lực, các nhà cung cấp cần thường xuyên chuẩn bị và cung cấp các báo cáo về hoạt động và quá trình tuân thủ liên tục các thủ tục pháp lý.điều lệ quản lý và điều khỏan hợp đồng cho khách hàng.**
- **Các nhà cung cấp dịch vụ cũng như các tổ chức tài chính cần họp thường xuyên để xem xét báo cáo và mức độ hiệu suất**
- **Hợp đồng cung cấp dịch vụ nên được chuẩn bị thêm các điều khoản về khắc phục hậu quả khi các vấn đề phát sinh hoặc vi phạm hợp đồng.**

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. Kiểm toán

- **Hầu hết các Cơ quan quản lý tài chính đều yêu cầu được quyền được thanh tra hoạt động cung cấp dịch vụ nhà cung cấp dịch vụ.**
- **Điều này đảm bảo rằng các nhà cung cấp dịch vụ tuân thủ đúng quy tắc, điều khoản và luật lệ yêu cầu bởi các nhà quản lý tài chính.**

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. Kế hoạch dự phòng và tính duy trì của dịch vụ

- **Dịch vụ điện toán đám mây phải đáng tin cậy và có thể chứng thực được độ tin cậy.**
- **Các nhà cung cấp dịch vụ phải có kế hoạch phát triển và duy trì kinh doanh hợp lý, cung cấp đầy đủ các dịch vụ cần thiết cho khách hàng, có khả năng khôi phục kinh doanh, thêm vào đó quy trình và hệ thống phải thường xuyên được cập nhật và kiểm tra nhằm đảm bảo đáp ứng được các mục tiêu trên.**
- **Rủi ro của hệ thống cần được giảm thiểu bằng việc chuẩn bị kế hoạch dự phòng và hỗ trợ cho việc khôi phục hệ thống trong trường hợp khẩn cấp.**

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. Điều khoản thanh lý hợp đồng

- **Các nhà quản lý tài chính nên găn thêm điều khoản thanh lý trong hợp đồng với các nhà cung cấp dịch vụ khi cần thiết. Điều này đảm bảo cho việc hoàn trả các thông tin dữ liệu sau khi kết thúc hợp đồng, ngoài ra cũng khẳng định trách nhiệm của các nhà cung cấp dịch vụ là phải hoàn toàn tiêu hủy các dữ liệu của khách hàng còn lại trong hệ thống của họ sau khi hoàn trả.**
- **Bất kỳ tài liệu nào không được yêu cầu hoàn trả, các nhà dịch vụ vẫn được yêu cầu xóa bỏ hoàn toàn các dữ liệu này ra khỏi hệ thống của họ.**

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

Các bước tiếp theo

Khi xây dựng hệ thống theo những nguyên tắc này, các nhà cung cấp dịch vụ và các nhà quản lý tài chính có thể cùng hợp tác để cung cấp được một hệ thống thông tin theo chuẩn pháp lý và xây dựng được nguyên tắc,định hướng đồng nhất cho việc cung cấp và sử dụng dịch vụ điện toán đám mây một cách hiệu quả.

Vài nét về công ty
Open Computing Alliance

- Một công ty công nghệ thông tin và truyên thông đa quốc gia bắt nguồn từ Anh Quốc
  - Các công ty thuộc của OCA đều dẫn đầu trên thị trường CNTT Châu Á Thái Bình Dương
- Mở ra các cuộc đối thoại về chính sách công nghệ;
  - Mở rộng phát triển và cạnh tranh.
  - Các tiêu chuẩn mở.
  - Tôn trọng quyền sở hữu trí tiệu.
  - *Công nghệ điện toán đám mây đáp ứng yêu cầu an toàn cho ngành CNTT*
  - Tối đa hóa hiệu năng cho hệ thống IT.
- ...cung cấp kết quả hoạt động tốt và lợi ích tối đa cho các tổ chức kinh doanh.
- Chi nhanh tại Châu Á Thái Bình Dương được đặt tại Hông Kông.

* Represented by Asia Policy Partners LLC