Dịch vụ Tài chính và Tác động của Công nghệ mới

HỘI THẢO TỔ CHỨC BỞI

HIỆP HỘI NGÂN HÀNG VIỆT NAM

HỖ TRỢ BỞI PHÒNG THƯƠNG MẠI HOA KỲ TẠI TP.HCM, PHÒNG THƯƠNG MẠI CHÂU ÂU VÀ LIÊN MINH MÁY TÍNH MỞ, ANH

KHÁCH SẠN NIKKO,

17/6/2014

MR. MICHAEL MUDD

TỔNG THƯ KÝ, LIÊN MINH MÁY TÍNH MỞ TẠI CHÂU Á-THÁI BÌNH DƯƠNG - LONDON, ANH

CHỦ TỊCH ỦY BAN CNTT, GIAO THỨC LIÊN MẠNG VÀ VIỄN THÔNG,

PHÒNG THƯƠNG MẠI HOA KỲ TẠI HANOI

Con số - Đến 2020 máy tính sẽ xử lý;

- Hơn 2 ngàn tỉ giao dịch tài chính*
- Trên 31 tỉ thiết bị*
- Bởi 4 tỉ người dùng Internet*
- Sử dụng 25 triệu ứng dụng*
- Tạo ra1.2 Zettabytes dữ liệu số[1]
- Với việc tiêu dùng Đám Mây đạt 250 tỷ Đôla[2]

- Gartner Group
- 1 Digital Universe 20 0 EMC-IDC

1 1 Zt =1000 Exabyte's or 10^21 bytes

2 Forrester Research

Cách mạng công nghệ

	Công nghệ	Kinh tế	Kinh doanh
	Tin học và lưu trữ tập trung, máy tính của người dùng có cấu hình tối thiểu (thin clients)	Tối ưu hóa về hiệu quả do chí phí cao	Chi phí trả trước cao đối với phần mềm và phần cứng . 'Tư duy' tương tự (Analog)'
	Các máy tính và máy chủ cho điện toán phân tán, Thuê ngoài cố định.	Tối ưu hóa về độ nhanh nhạy do chi phí thấp	Giấy phép vĩnh viễn cho Hệ điều hành và phần mềm ứng dụng. 'Tư duy' phát triển
	Những bộ điều khiển miền (DC) rất lớn, Ảo hóa, Dịch vụ thuê ngoài mô hình đa người dùng Multi-tenant	Yêu cầu cường độ với hiệu quả và nhanh nhạy cao hơn	Dùng bao nhiêu-trả bấy nhiêu, và chỉ cho cái mà bạn sử dụng. Hoàn toàn 'Tư duy kỹ thuật số"

Tại sao cần triển khai Đám mây?

Lợi ích

Tỷ suất hoàn vốn đầu tư tốt- chi phí ít hơn 3 lần

CP hoạt động vs CP vốn

Tăng trưởng về nhu cầu

Thách thức

Cần phải SD ngôn ngữ "Đám mây"

Yêu cầu sự thay đổi (cơ quan quản lý)

Độ trễ làm triệt tiêu hiệu quả

Mối quan ngại về an ninh

Thảo luận

- OCA đã thảo luận tại;
  - Singapore
  - Hong Kong
  - Thailand
  - Philippines
  - Australia
  - Vietnam
- Ngân hàng và các công ty bảo hiểm (và các cơ quan quản lý).
- Các nhà cung cấp dịch vụ(CCDV).
- Hiệp hội và phòng thương mại ngành.
- Các vấn đề thực tế cần giải quyết?

Tại sao là Công nghệ mới?

- Hệ thống CNTT Ngân hàng lõi đã 50 năm ; lỗi thời
- Các ngân hàng lớn tăng tỷ lệ vốn theo Basel 3.
- Các cty bảo hiểm và cty chứng khoán cần giảm chi phí?
- 4 năm trước, Dịch vụ Đám mây không thuộc tầm nhìn của bất kỳ Tổ chức tài chính nào đối với bất kỳ SaaS, IaaS, … Dưới bất kỳ trường hợp nào; công cộng, cá nhân hay lai ghép.
- Ngày nay thách thức là giảm chi phí vốn– để làm điều này phải có sự linh động trong chi phí hoạt động – Dịch vụ Đám mây thực hiện điều đó.
- Vấn đề kiểm soát rủi ro chính là về độ tin cậy trong kiểm toán và kiểm soát, cả từ phía ngân hàng và các cơ quan quản lý.

Hiện nay Dịch vụ Đám mây đang được chuyển giao cho Ngân hàng

- Đối với Ngân hàng/Tổ chức tài chính, hiện nay Dịch vụ Đám mây đang được áp dụng.
- AXA, Capita PLC, Rabo Bank, Robeco, MKB Bank tại France, the UK Netherlands và Hungary đang sử dụng dịch vụ lai ghép máy chủ tại Ireland.
- TienPhong Bank hiện đang sử dụng dịch vụ Đám mây.
- Dịch vụ đám mây doanh nghiệp đã hoàn thiện – hãy xem USG; FISMA, FedRamp, HIPPA.
- SSAE 16 cung cấp tiêu chuẩn kiểm toán quốc tế

Một số Tổ chức tài chính đã triển khai ‘ Đám mây”

Luồng dữ liệu xuyên biên giới

- Hiệu quả và lợi ích của điện toán đám mây đạt được tốt nhất khi các luồng dữ liệu – thông tin được chuyển dịch tự do giữa các quốc gia – APEC, TPP, AEC
- Tương tự như kinh doanh nói chung, tất cả hiện đang toàn cầu
- Luật về quyền riêng tư hạn chế quá mức các luồng dữ liệu – thông tin như vậy có thể là một trở ngại tới sự phát triển kinh tế
- Được theo dõi sát sao các cơ quan quản lý – nhà đầu tư – mối quan tâm thực sự
- Các tổ chức tài chính đã thực hiện điều này qua hàng thập kỷ

An ninh và những thách thức về mặt pháp lý:

10 năm trước…

- An ninh và sự riêng tư là sự chú ý hàng đầu
- Đột nhập (hack), phát tán virus, đột nhập mạng và chiến tranh mạng đang tăng lên
- Các quan chức thực thi cần các công cụ và đào tạo
- Các phương tiện để hợp tác xuyên biên giới chưa đủ

Ngày nay…

- An ninh và sự riêng tư là sự chú ý hàng đầu
- Đột nhập (hack), phát tán virus, đột nhập mạng và chiến tranh mạng đang tăng lên
- Các quan chức thực thi cần các công cụ và đào tạo
- Các phương tiện để hợp tác xuyên biên giới chưa đủ

Vậy điều gì đã thay đổi? Đó là niềm tin

- Các thông lệ của nhà cung cấp dịch vụ;
  - Nhà cung cấp có chương trình bảo mật thông tin tài liệu không, và nhà cung cấp nói gì?
  - Nhà cung cấp có tiêu chuẩn về bảo mật nào?
  - Họ có tuân theo nhu cầu kiểm toán của cty và cơ quan quản lý?
- Trách nhiệm rõ ràng của mỗi bên vd, trong việc phá vỡ hợp đồng?
- Đảm bảo khuôn khổ cho Điện toán đám mây hiện đang được triển khai bởi Chính phủ và các nhà cung cấp dịch vụ.
- Bảo mật của bên thứ 3 và kiểm toán kinh doanh.

Các tiêu chuẩn, kiểm toán và chứng chỉ

ISO International Organization for Standardization

23001, 27001 & 31000

European Commission

Article 29 compliance

FedRAMP℠

Ensuring secure cloud computing for the Federal Government

SSAE 16

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:

HIPAA

Health Insurance Portability & Accountability Act

Khuôn khổ an ninh mạng của Hoa kỳ NIST

Sắc lệnh hành pháp 13636— Cải thiện cơ sở hạ tầng bảo mật mạng thiết yếu

"Đây là chính sách của Hoa Kỳ nhằm tăng cường bảo mật và khả năng phục hồi cơ sở hạ tầng thiết yếu của quốc gia và nhằm duy trì một môi trường mạng trong đó khuyến khích tính hiệu quả, sự đổi mới, và sự thịnh vượng kinh tế trong khi vẫn thúc đẩy tính an toàn, bảo mật , bí mật kinh doanh, quyền riêng tư và quyền tự do cá nhân"

NIST được định hướng để làm việc với các bên liên quan nhằm phát triển một khuôn khổ tự nguyện đối với quản lý và giảm rủi ro an ninh mạng của cơ sở hạ tầng thiết yếu, bao gồm ngân hàng.

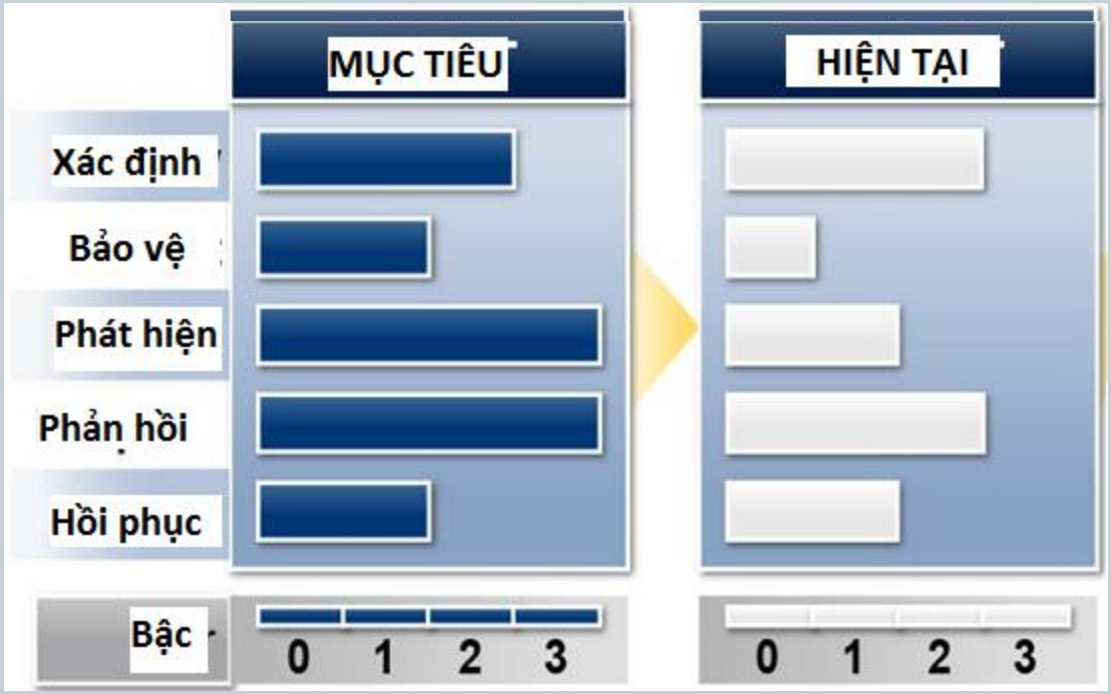
Courtesy Tim Grance, Cybersecurity Head, NIST

Khuôn khổ

- ***Bao gồm*** một bộ tiêu chuẩn, phương thức, quy trình và thủ tục mà làm hài hòa các phương pháp tiếp cận chính sách, kinh doanh và công nghệ để giải quyết rủi ro an ninh mạng.
- ***Cung cấp*** một phương pháp tiếp cận ưu tiên, linh động, có thể lặp lại, dựa trên kết quả và hiệu quả về chi phí, bao gồm các biện pháp an ninh thông tin và kiểm soát, nhằm giúp các chủ sở hữu và người điều hành các cơ sở hạ tầng thiết yếu có thể xác định, đánh giá và quản lý rủi ro an ninh mạng .
- ***Xác định*** các lĩnh vực cần cải thiện thông qua hợp tác với các ngành cụ thể và với các tổ chức phát triển tiêu chuẩn có thể đổi mới kỹ thuật và tính đến sự khác biệt về mặt tổ chức bao gồm hướng dẫn đo lường hiệu suất của một tổ chức trong việc triển khai Khuôn khổ an ninh mạng.

Courtesy Tim Grance, Cybersecurity Head, NIST

Đặc trưng và chức năng cốt lõi của Khuôn khổ



Xác định Rủi ro	Đánh giá Rủi ro	Sử dụng quy trình đánh giá rủi ro Để lựa chọn Hạng mục và Bậc	Triển khai Hạng mục phụ được lựa chọn

Courtesy Tim Grance, Cybersecurity Head, NIST

Doanh nghiệp thực sự *muốn* gì?

- Nhằm đem lại dịch vụ với:
  - An ninh dữ liệu
  - Tính bảo mật
  - Tính toàn vẹn
  - Tính sẵn có
- Nhằm giảm thiểu chi phí và cải thiện dịch vụ.
- Nhằm đáp ứng nhu cầu khách hàng ngày càng nhanh hơn.
- Nhằm cải thiện bản cân đối kế toán.
- Nhằm thỏa mãn các cơ quan quản lý …

Các cơ quan quản lý thực sự CẦN gì?

- Ví dụ; Singapore đang xem Đám mây như là '3 từ'*
  - Nguyên tắc
  - Sự chuẩn bị sẵn sàng
  - Quan hệ đối tác
- Điều này cho phép nhà cung cấp dịch vụ đưa ra dịch vụ với :
  - Tính bảo mật
  - Tính toàn vẹn
  - Tính sẵn có
- Thỏa mãn quy trình thẩm định của họ và giảm thiểu rủi ro.

*http://www.mas.gov.sg/news-and-publications/speeches-and-monetary-policy-statements/2013/managing-technology-risks-in-the-financial-sector.aspx

Các cơ quan quản lý tổ chức tài chính đang làm gì?

Singapore (MAS):

MAS không cấm điện toán đám mây. Thực tế, MAS đã chấp thuận nó trong các trường hợp đặc biệt.

2013 Hướng dẫn của MAS về Quản lý rủi ro công nghệ *

- Báo cáo thông lệ tốt nhất của ngành đối với tổ chức tài chính để áp dụng
- Chấp hành hướng dẫn tác động việc đánh giá rủi ro của MAS về 1 tổ chức tài chính
- Các tổ chức tài chính phải có chính sách và thủ tục phù hợp nhằm đánh giá, thông qua, xem xét và kiểm soát cũng như giám sát rủi ro
- Nhấn mạnh vào năng lực thực hiện kiểm tra, giám sát và kiểm nghiệm các nhà cung cấp dịch vụ và cơ sở vật chất
- Chú ý đặc biệt tới năng lực của nhà cung cấp dịch vụ đám mây trong việc phân tách và dữ liệu ID khách hàng cũng như quyền yêu cầu dỡ bỏ và tiêu hủy dữ liệu khi chấm dứt hợp đồng

Philippines (BSP)

2013 Thông tư 808 – Hướng dẫn nâng cao về quản trị rủi ro công nghệ thông tin

 *http://www.mas.gov.sg/news-and-publications/speeches-and-monetary-policy-statements/2013/managing-technology-risks-in-the-financial-sector.aspx

Khuôn khổ – TÍNH BẢO MẬT

- **Minh bạch dữ liệu và địa điểm**

  Nhà cung cấp dịch vụ (CCDV) nên minh bạch hoàn toàn về địa chỉ nơi dữ liệu sẽ được lưu trữ.

- **Giới hạn về sử dụng dữ liệu**

  Nhà CCDV không được sử dụng dữ liệu của khách hàng cho bất kỳ mục đích nào ngoài những mục đích cung cấp dịch vụ Đám mây trong hợp đồng.

- **Phân tách dữ liệu**

  Dữ liệu của khách hàng phải được phân tách khỏi các dữ liệu khác lưu trữ bởi nhà CCDV.

- **Điều kiện về hợp đồng phụ**

  Nhà CCDV chỉ có thể sử dụng nhà thầu phụ nếu nhà thầu phụ chịu sự kiểm soát tương đương như nhà CCDV.

Khuôn khổ – TÍNH TOÀN VẸN

- **Uy tín và năng lực của nhà CCDV**

  Khách hàng nên có sẵn một kế hoạch quản trị rủi ro bao gồm các phương pháp giải quyết các rủi ro khi sử dụng dịch vụ Đám mây của bên CCDV.

- **Bảo mật và các tiêu chuẩn chứng nhận bảo mật**

  Nhà CCDV phải có chứng nhận là có và duy trì các biện pháp an ninh và các chính sách an ninh toàn diện đáp ứng tối thiểu tiêu chuẩn quốc tế (ISO27001).

- **Xem xét, giám sát và kiểm soát**

  Trong suốt thời hạn hợp đồng Nhà CCDV phải cung cấp báo cáo và thông tin định kỳ thể hiện việc tuân thủ liên tục đối với các tiêu chuẩn, các yêu cầu hợp đồng và pháp lý theo thỏa thuận.

- **Kiểm toán**

  Hầu hết các cơ quan quản lý yêu cầu các nhà CCDV cho phép Cơ quan quản lý tài chính, và tổ chức tài chính thực hiện thanh tra nhà CCDV. Điều này cho phép cơ quan quản lý và tổ chức tài chính đảm bảo rằng nhà CCDV tuân thủ theo các yêu cầu về kinh doanh, hợp đồng và pháp lý .

Khuôn khổ –TÍNH SẴN CÓ

- **Khả năng phục hồi và kinh doanh liên tục**

  Dịch vụ đám mây phải đáng tin cậy.

  - Nhà CCDV phải có kế hoạch kinh doanh liên tục hiệu quả với sự sẵn có về dịch vụ phù hợp, và kế hoạch dự phòng.
- **Điều kiện chấm dứt hợp đồng**
  - Khách hàng phải có điều khoản chấm dứt phù hợp trong hợp đồng với nhà CCDV.
  - Trong phạm vi mà tổ chức tài chính yêu cầu, về chấm dứt, nhà CCDV phải hợp tác với tổ chức tài chính để hoàn trả dữ liệu lại cho tổ chức tài chính
  - Nhà CCDV được chứng nhận phải xóa vĩnh viễn dữ liệu từ hệ thống của nhà CCDV.
  - Bất kỳ dữ liệu nào không cần hoàn trả lại cho tổ chức tài chính phải được xóa vĩnh viễn bởi nhà CCDV.

Một vài suy nghĩ cuối cùng

Ngành dịch vụ tài chính và các cơ quan quản lý có tầm nhìn xa đang thừa nhận ảnh hưởng mạnh mẽ của công nghệ mới.

Một khuôn khổ xây dựng theo các nguyên tắc có thể hỗ trợ hơn nữa các cơ quan nhà nước quản lý dịch vụ Đám mây.

Ý tưởng được trình bày ở đây có thể giải quyết một phần mối quan tâm của các Cơ quan quản lý

Điều gì tiếp theo?

Ngân hàng và các hiệp hội có thể hợp tác với ngành CNTT để tạo ra một bộ khuyến nghị về quản lý rủi ro được chấp thuận rộng rãi.

Các cơ quan quản lý có thể giữ vai trò đứng đầu và đóng góp vào thông lệ tốt nhất toàn cầu trong việc cung ứng dịch vụ.

Khuyến nghị:

Ngành và các cơ quan quản lý cần chấp thuận một khuôn khổ xây dựng theo các nguyên tắc đối với việc cung ứng Dịch vụ Đám mây

Liên minh máy tính mở (OCA)

- Tổ chức chuyên gia cố vấn chính sách với sự ủng hộ tích cực ngành CNTT toàn cầu (trụ sở tại Anh)
  - Các thành viên là những tổ chức hàng đầu về công nghệ tại các thị trường Châu Á – Thái Bình Dương
- Tạo ra đối thoại về Chính sách công nghệ;
  - Mở rộng Cạnh tranh và đổi mới.
  - Tiêu chuẩn mở.
  - Thương mại công bằng và tôn trọng sở hữu trí tuệ
  - *Điện toán đám mây đáp ứng yêu cầu CNTT Đảm bảo và Đáng tin cậy.*
  - Tối đa hóa hiệu năng cho hệ thống IT
- ...nhằm mang lại kết quả tích cực cho tất cả các bên – cả công và tư.
- Khu vực Châu Á Thái Bình Dương đặt văn phòng tại Hongkong*.

mmudd@opencomputingalliance.org
www.opencomputingalliance.org

* Represented by Asia Policy Partners LLC