NGÂN HÀNG NHÀ NƯỚC

VIỆT NAM

**BẢN THUYẾT MINH CÁC NỘI DUNG DỰ THẢO QUY CHẾ**

**Quản lý, sử dụng dịch vụ điện toán đám mây trong ngành ngân hàng**

1. **SỰ CẦN THIẾT BAN HÀNH**

Điện toán đám mây (ĐTĐM) là mô hình cung cấp các tài nguyên máy tính (tính toán, xử lý và lưu trữ) dưới dạng dịch vụ (thay vì dưới dạng sản phẩm) qua môi trường mạng. Các tài nguyên máy tính này bao gồm: cơ sở hạ tầng (infrastructure) như: phần cứng máy chủ, thiết bị lưu trữ, …; môi trường nền tảng (platform) như: hệ điều hành, phần mềm hệ thống, cơ sở dữ liệu, phần mềm công cụ, …; và phần mềm như: phần mềm ứng dụng hoàn chỉnh, các chương trình tiện ích, …

ĐTĐM làm thay đổi cách thức sử dụng công nghệ thông tin của Đơn vị, Tổ chức. Theo cách thức truyền thống, Tổ chức phải mua sắm trang thiết bị CNTT (phần cứng, phần mềm) sau đó triển khai ứng dụng trên trang thiết bị và duy trì nhân sự vận hành, quản trị, duy trì hoạt động của hệ thống. Khi ứng dụng ĐTĐM, Tổ chức sẽ sử dụng các dịch vụ ĐTĐM từ Nhà cung cấp thay vì thực hiện một loạt các công việc nêu trên và thanh toán phí sử dụng dịch vụ theo định kỳ.

1. **Các đặc tính của ĐTĐM**

*1.1. Tự phục vụ theo nhu cầu*: Người sử dụng có thể tự mình thiết lập yêu cầu tài nguyên máy chủ, vùng lưu trữ, thời gian sử dụng mà không cần có sự tương tác trực tiếp với Nhà cung cấp dịch vụ.

*1.2. Truy cập, sử dụng dịch vụ qua mạng*: Người sử dụng đăng nhập vào qua cổng thông tin điện tử cung cấp dịch vụ qua mạng. Thiết bị sử dụng để truy cập dịch vụ có thể là các máy tính bảng, máy tính xách tay, máy tính cá nhân ...

*1.3. Dùng chung tài nguyên:* Tài nguyên máy tính của nhà cung cấp được tập trung lại để phục vụ cho nhiều khách hàng độc lập. Tài nguyên vật lý được ảo hóa và cấp phát động tùy theo yêu cầu của người dùng.

*1.4. Cho phép thay đổi cấu hình nhanh chóng:* Việc tạo, xóa, thay đổi cấu hình hệ thống CNTT được thực hiện rất dễ dàng và nhanh chóng.

*1.5. Đo đếm được tài nguyên sử dụng:* Giống như việc thuê bao sử dụng điện thoại, internet hàng tháng, việc sử dụng dịch vụ ĐTĐM được đo đếm, định lượng một cách minh bạch.

**2. Lợi ích và rủi ro**

*2.1. Lợi ích:*

1. Giảm chi phí do không phải đầu tư trang thiết bị, triển khai, nâng cấp, bảo trì, chi phí vận hành (điện năng, môi trường lắp đặt);
2. Tiện lợi khi xử lý công việc, triển khai công việc nhanh, dùng đến đâu trả tiền đến đó;
3. Dễ dàng đánh giá được hiệu quả hoạt động của từng đơn vị do định lượng được rõ ràng tài nguyên tiêu thụ cho từng đơn vị khai thác, từ đó tính được chi phí sử dụng;
4. Người dùng CNTT từ các đơn vị khác nhau trong tổ chức được gỡ bỏ những bận tâm về hạ tầng CNTT.

*2.2. Rủi ro:*

1. Khó khăn trong việc kiểm soát, bảo đảm an toàn thông tin mạng, bảo vệ dữ liệu; Tăng nguy cơ bị tấn công mạng, tăng nguy cơ lộ, lọt thông tin/dữ liệu mật.
2. Gián đoạn trong việc cung cấp dịch vụ do các sự cố liên quan đến kết nối mạng.

Điện toán đám mây đem lại nhiều lợi ích cho Tổ chức sử dụng, do vậy, nhu cầu sử dụng dịch vụ đám mây phát triển rất nhanh trên thế giới. Trong lĩnh vực tài chính, ngân hàng với đặc thù mang tính hệ thống cao, yêu cầu nghiêm ngặt về an ninh mạng và bảo vệ dữ liệu, việc ứng dụng điện toán đám mây chưa mạnh mẽ như các lĩnh vực khác. Các hoạt động được ngân hàng chuyển sang môi trường điện toán đám mây dùng chung thường là các hoạt động không nhạy cảm về an toàn, bảo mật[[1]](#footnote-1). Các hoạt động ngân hàng lõi, nghiệp vụ kinh doanh quan trọng vẫn được duy trì trên các Trung tâm dữ liệu của ngân hàng, với các trang thiết bị công nghệ thông tin hiện đại.

Với bản chất là dịch vụ cung cấp qua mạng, hoạt động CNTT trong môi trường ĐTĐM cần có hành lang pháp lý phù hợp để có khả năng kiểm soát, giám sát và quản lý. Tuy nhiên, hành lang pháp lý tại Việt Nam lại chưa tạo được thuận lợi cho triển khai, ứng dụng ĐTĐM. Là ngành đi đầu trong lĩnh vực ứng dụng CNTT tại Việt Nam, khai thác ĐTĐM được xem vừa là thách thức vừa là cơ hội cho ngành ngân hàng. Nếu khai thác được những thế mạnh mà ĐTĐM mang lại, trong khi vẫn bảo đảm an toàn, bảo mật dữ liệu; hoạt động tài chính ngân hàng sẽ đóng góp được nhiều hơn cho đời sống kinh tế, xã hội.

Thực hiện nhiệm vụ quản lý nhà nước lĩnh vực công nghệ thông tin, Cục Công nghệ thông tin nhận thấy việc xây dựng, ban hành quy định về quản lý, sử dụng dịch vụ điện toán đám mây trong ngành ngân hàng nhằm cân bằng những lợi ích và rủi ro cho hệ thống tài chính là quan trọng và cần thiết. Cục CNTT đề cao việc đảm bảo an ninh mạng, bảo mật dữ liệu trong khi dự thảo các quy định. Để cân bằng giữa lợi ích và rủi ro, phù hợp với xu hướng, thông lệ trên thế giới, ứng dụng ĐTĐM trong ngành ngân hàng, tại thời điểm này, đang được định hướng sử dụng ĐTĐM lai (Hybrid cloud). Theo đó, các Tổ chức vừa quản lý sử dụng hạ tầng CNTT của riêng mình (các trung tâm dữ liệu, điện toán đám mây riêng) để bảo đảm an toàn cho các nghiệp vụ ngân hàng quan trọng, vừa khai thác tối đa lợi ích từ các dịch vụ điện toán đám mây dùng chung cho các nghiệp vụ không thường xuyên, không có yêu cầu về an ninh, bảo mật dữ liệu.

1. **CƠ SỞ PHÁP LÝ**
* Luật Công nghệ thông tin số 67/2006/QH11;
* Luật số An toàn thông tin mạng số 86/2015/QH13;
* Nghị định 108/2016/NĐ-CP ngày 01/7/2016 Quy định về điều kiện kinh doanh dịch vụ an toàn thông tin mạng, sản phẩm, dịch vụ an toàn thông tin mạng;
* Nghị định 85/2016/NĐ-CP ngày 01/7/2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ;
* Quyết định 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;
* Thông tư 31/2015/TT-NHNN ngày 28/12/2015 của Ngân hàng Nhà nước quy định về dảm bảo an toàn, bảo mật hệ thống công nghệ thông tin trong hoạt động ngân hàng;
* Quyết định về độ mật của từng loại tài liệu, vật mang bí mật nhà nước trong ngành ngân hàng (Văn bản hợp nhất só 25/VBHN-NHNN ngày 11/6/2014 của Ngân hàng Nhà nước Việt Nam).

**III. CÁC NGUYÊN TẮC VÀ ĐỊNH HƯỚNG XÂY DỰNG QUY CHẾ**

**1. Nguyên tắc xây dựng**

* Tuân thủ Luật Công nghệ thông tin, Luật an toàn thông tin và các quy định bảo mật của Pháp luật và ngành ngân hàng.
* Phù hợp với xu hướng phát triển công nghệ thông tin và thông lệ quốc tế.
* Đơn giản, cụ thể, rõ ràng, dễ thực hiện, thuận lợi đối với Tổ chức tín dụng, Chi nhánh Ngân hàng Nước ngoài, các Trung gian thanh toán và cơ quan quản lý trong việc thực hiện, quản lý.

**2. Định hướng xây dựng**

* Để đảm bảo an toàn CNTT và an ninh dữ liệu cho việc ứng dụng ĐTĐM trong ngành ngân hàng, Quy chế được xây dựng bằng việc tiếp cận, xem xét những vấn đề an ninh gắn với ĐTĐM từ đó quản lý được những rủi ro về an toàn công nghệ thông tin khi sử dụng dịch vụ ĐTĐM.
* An toàn công nghệ thông tin gắn với ĐTĐM được xem xét trên 02 khía cạnh chính: *An ninh tổ chức* (Organizational security) và *An ninh vận hành* (Operational security), trong đó:
	+ *An ninh tổ chức:* là những nội dung mà Tổ chức phải xem xét, xử lý trước khi triển khai sử dụng dịch vụ ĐTĐM. An ninh tổ chức gồm các lĩnh vực : Điều hành, rủi ro và kiểm soát (Governance, Risk and Control), Những vấn đề pháp lý (Legal issues), Tuân thủ và kiểm toán (Compliance and Audit), Vai trò và trách nhiệm.
	+ *An ninh vận hành:* mô tả những nội dung/vấn đề mà Tổ chức cần phải quan tâm xử lý sau khi triển khai sử dụng dịch vụ ĐTĐM để bảo vệ tài sản, và để đảm bảo an toàn CNTT trong Tổ chức. An ninh vận hành gồm các lĩnh vực: Đảm bảo hoạt động liên tục cho nghiệp vụ và Dự phòng thảm họa (Business continuity and Disaster Recovery), Thỏa thuận mức độ dịch vụ và Quản lý nhà cung cấp (SLA and Vendor Mgnt), Quản lý kiểm soát truy cập và Nhận dạng (Identity and Access Control Mgnt), Nhận thức / Đào tạo nêu cao nhận thức.
* Bên cạnh đó là nội dung liên quan đến kiểm soát an toàn trong nội hàm của dịch vụ đám mây: An toàn vật lý và logic, An toàn cơ sở hạ tầng CNTT, An toàn quy trình và ứng dụng, An toàn thông tin và dữ liệu. Các nội dung này được tóm tắt cơ bản như sau:
	+ *An toàn vật lý và logic*:
		1. An toàn vật lý: là những cách thức kiểm soát, giám sát truy cập về mặt vật lý như bằng cách sử dụng các biện pháp kiểm soát truy cập sinh trắc học và giám sát bằng CCTV. Nhà cung cấp phải mô tả rõ việc truy cập về mặt vật lý đến các máy chủ phục vụ dịch vụ được quản lý như thế nào. An toàn vật lý là một dịch vụ hạ tầng CNTT để tạo ra những nhận thức về an toàn vật lý và khết hợp nó để đảm bảo an toàn CNTT. An toàn vật lý bao gồm các hệ thống giám sát, dò chuyển động, theo dõi và nhận dạng con người và đồ vật, kiểm soát lối vào, giám sát môi trường, nhiệt độ, nguồn điện …
		2. An toàn logic: đề cập đến các kỹ thuật an toàn logic được sử dụng song song với các giải pháp an toàn vật lý nhằm bảo vệ hệ thống và dữ liệu như: kiểm soát truy cập logic (username/passwd, OTP, RSA Token, …), DAC (Discretionary access control), MAC (mandatory access control), RBAC (Roles based access control)… An toàn logic thường dùng để nhận dạng, xác thực, cấp phép cho người dùng của hệ thống.
	+ *An toàn cơ sở hạ tầng CNTT*: Cung cấp sự bảo vệ an toàn các góc độ:
		1. An toàn hệ thống mạng (Network security);
		2. An toàn môi trường ảo hóa (Virtual Environment Security);
		3. Mã hóa và quản lý khóa (Encryption and Key Mgnt);
		4. Giám sát (Monitoring).
	+ *An toàn quy trình và ứng dụng*: Nội dung này đề cập đến đảm bảo an toàn cho ứng dụng, cho các quy trình và cho các bản vá lỗi và các bản cập nhật phiên bản.
	+ *An toàn thông tin và dữ liệu*: cung cấp sự bảo vệ dữ liệu khỏi những nguy cơ lộ bí mật, mất mát, chuyển nhượng và truy cập không có quyền tùy thuộc theo giá trị kinh doanh và giá trị tự nhiên của thông tin.

**IV. CÁC NỘI DUNG CƠ BẢN CỦA DỰ THẢO QUY CHẾ**

**1. Bố cục**

Dự thảo Quy chế gồm 5 Chương, 16 Điều, cụ thể:

* Chương I: từ **Điều 1 đến Điều 4** - Những quy định chung.
* Chương II: từ **Điều 5 đến Điều 6** – Phạm vi và điều kiện sử dụng dịch vụ đám mây.
* Chương III: từ **Điều 7 đến Điều 9** – Trước khi sử dụng dịch vụ đám mây.
* Chương IV: từ **Điều 10 đến Điều 14** – Quản lý và sử dụng dịch vụ đám mây.
* Chương V: từ **Điều 15 đến Điều 16** – Tổ chức thực hiện.

**2. Những nội dung cơ bản của Dự thảo Quy chế**

* 1. ***Phạm vi và đối tượng điều chỉnh***

 - Quy chế này hướng dẫn việc thuê ngoài, quản lý và sử dụng dịch vụ điện toán đám mây trong ngành ngân hàng *(Khoản 1, Điều 2)*

 - Quy chế này áp dụng đối với các tổ chức tín dụng, chi nhánh ngân hàng nước ngoài và các tổ chức cung ứng dịch vụ trung gian thanh toán (sau đây gọi chung là Tổ chức) có hoạt động thuê ngoài dịch vụ điện toán đám *(Điều 2)*

* 1. ***Giải thích từ ngữ***

 Các khái niệm được quy định tại dự thảo Quy chế được xây dựng trên nguyên tắc đầy đủ, dễ hiểu, dễ áp dụng, tránh tra cứu nhiều văn bản. Dự thảo Quy chế quy định một số khái niệm và thuật ngữ được sử dụng nhiều trong dự thảo như: điện toán đám mây, dịch vụ điện toán đám mây, mô hình dịch vụ đám mây, nhà cung cấp dịch vụ.

* 1. ***Phạm vi và điều kiện sử dụng dịch vụ đám mây***
* Nhằm khuyến khích việc triển khai dịch vụ đám mây trong ngành Ngân hàng, dự thảo xây dựng theo hướng trao quyền cho các Tổ chức tự quyết định lựa chọn mô hình dịch vụ đám mây. Tuy nhiên, để đảm bảo tính bí mật và an toàn cho các dữ liệu trong ngành ngân hàng, các Tổ chức không được phép dùng dịch vụ đám mây dùng chung để xử lý, lưu trữ các dữ liệu MẬT, TỐI MẬT, TUYỆT MẬT (theo quy định bảo vệ bí mật nhà nước trong ngành Ngân hàng) . *(Điều 5)*
* Để giảm thiểu các rủi ro khi triển khai dịch vụ điện toán đám mây dùng chung, Dự thảo cũng đưa ra các điều kiện để các Tổ chức phải rà soát, cân nhắc, đánh giá và thực hiện trước khi áp dụng điện toán đám mây. *(Điều 6)*
	1. ***Các nội dung Tổ chức cần thực hiện trước khi sử dụng dịch vụ đám mây***

Trước khi các Tổ chức quyết định sử dụng dịch vụ đám mây, các Tổ chức cần thực hiện:

* Đánh giá rủi ro công nghệ thông tin, rủi ro hoạt động trên các khía cạnh như: (i) Nhận diện rủi ro, phân tích, ước lượng mức độ tổn hại, mối đe dọa; (ii) Xác định rõ vai trò, trách nhiệm của các bên liên quan; (iii) Xây dựng, chuẩn bị các biện pháp nhằm giảm thiểu rủi ro, biện pháp ứng cứu, khắc phục sự cố. *(Điều 7)*
* Xây dựng các tiêu chí để lựa chọn nhà cung cấp dịch vụ, như các tiêu chí về mặt kỹ thuật đảm bảo việc cung cấp dịch vụ an toàn, liên tục. Trong đó có những quy định cụ thể áp dụng riêng đối với các trường hợp nhà cung cấp dịch vụ không hoạt động trên lãnh thổ Việt Nam, hay các quy định trong trường hợp trung tâm dữ liệu của nhà cung cấp dịch vụ nằm ngoài lãnh thổ Việt Nam *(Điều 8)*
* Để bảo vệ quyền lợi cho các Tổ chức trong việc ký kết hợp đồng dịch vụ đám mây cũng như đảm bảo tính minh bạch, cam kết trong việc sử dụng dịch vụ Dự thảo quy định các điều khoản tối thiểu cần có trong hợp đồng sử dụng dịch vụ đám mây. *(Điều 9)*
	1. ***Các nội dung Tổ chức cần thực hiện trong quá trình quản lý và sử dụng dịch vụ đám mây*** *(Điều 10~14)*

Để đảm bảo tính toàn vẹn, bí mật đối với các dữ liệu cũng như đảm bảo yêu cầu hoạt động liên tục đối với các nghiệp vụ được triển khai trên nền tảng dịch vụ điện toán đám mây, các Tổ chức cần thực hiện các nhiệm vụ như: quản lý tài sản công nghệ thông tin; Kiểm soát thiết bị sử dụng để truy cập sử dụng dịch vụ đám mây; Giám sát hoạt động dịch vụ đám mây; Kiểm tra tuân thủ đối với Nhà cung cấp dịch vụ; thực hiện Chế độ báo cáo đối với NHNN.

 **V. MỘT SỐ VẤN ĐỀ CẦN XIN Ý KIẾN**

1. Phạm vi, điều kiện triển khai dịch vụ đám mây;

2. Quy định đối với các Tổ chức tín dụng, chi nhánh ngân hàng nước ngoài, các trung gian thanh toán cần thực hiện hiện trước và trong khi sử dụng dịch vụ đám mây.

3. Quy định đối với các nhà cung cấp dịch vụ đám mây; Quy định đối với Nhà cung cấp dịch vụ đám mây bên ngoài lãnh thổ Việt Nam (không chịu sự quản lý của pháp luật Việt Nam);

4. Đề xuất các nội dung khác cần điều chỉnh/quản lý chưa đề cập trong dự thảo.

 **CỤC CÔNG NGHỆ THÔNG TIN**

1. Tham khảo[*http://www.cio.com/article/3013953/cloud-computing/how-goldman-sachs-and-bank-of-america-use-the-cloud-and-containers.html*](http://www.cio.com/article/3013953/cloud-computing/how-goldman-sachs-and-bank-of-america-use-the-cloud-and-containers.html) [↑](#footnote-ref-1)