ỦY BAN BASEL VỀ GIÁM SÁT NGÂN HÀNG

CÁC NGUYÊN TẮC QUẢN TRỊ RỦI RO TRONG NGÂN HÀNG ĐIỆN TỬ

Tháng 7-2003

MỤC LỤC

Tiểu ban về Ngân hàng Điện tử
của Uỷ ban Basel về Giám sát Ngân hàng

Chủ tịch:

Ông John Hawke, Jr – Cơ quan Giám sát Tiền tệ, Washington DC

Thành viên:

Cơ quan Quản lý Thận trọng Australia, Australia	Ông Graham Johnson
Ủy ban Ngân hàng và Tài chính, Bỉ	Ông Jos Meuleman
	Ông Koen Algoet
Văn phòng Giám sát Thể chế Tài chính, Canada	Cô Judy Cameron
	Mr Abilash Bhachech
Ủy ban Ngân hàng, Pháp	Ông Alain Duchâteau
Ngân hàng Trung Ương Đức, Đức Germany	Ông Sven Jongebloed
Cơ quan Giám sát Thể chế Tài chính Liên bang, Đức	Ông Stefan Czekay
Cơ quan Tiền tệ Hồng Kông, Hồng Kông SAR	Ông Shu-Pui Li
	Ông Brian Lee
Ngân hàng Trung Ương Ý, Italia	Ông Filippo Siracusano
	Ông Tullio Pra
Ngân hàng Trung Ương Nhật bản, Nhật bản	Ông Toshihiko Mori
	Ông Hiroaki Kuwahara
	Ông Tomoko Suzuki
Cơ quan Dịch vụ Tài chính, Nhật bản	Ông Koji Hamada
	Cô Yoko Ota
Ủy ban Giám sát Khu vực Tài chính, Luxembourg	Ông David Hagen
	Ông Claude Bernard De
Ngân hàng Quốc gia Hà lan N.V., Hà lan	Ông Erik Smid
Cơ quan Tiền tệ Singapore	Ông Leon Chang
	Ông Enoch Ch'ng
	Ông Tony Chew
Ngân hàng Quốc gia Tây Ban nha, Tây Ban nha	Cô Maria Jesús Nieto
Cơ quan Giám sát Tài chính, Thụy điển	Cô Christina Westerling
Ủy ban Ngân hàng Liên bang, Thụy sĩ	Ông Daniel Schmid
Cơ quan Dịch vụ Tài chính, Anh quốc	Ông Peter MacCormack
Ngân hàng Dự trữ Liên bang New York, Hoa kỳ	Ông George Juncker

	Cô Barbara Yelcich
Văn phòng Giám sát Tiền tệ (OCC), Hoa kỳ	Ông Hugh Kelly
	Ông Clifford Wilke
Hội đồng Thống đốc Hệ thống Dự trữ Liên bang, Hoa kỳ	Cô Angela Desmond
	Ông Jeff Marquardt
Tập đoàn Bảo hiểm Tiền gửi Liên bang, Hoa kỳ	Cô Sandra Thomson
Ngân hàng Trung ương Châu Âu	Ông Christian Fehlker
Ban Thư ký, Ủy ban Basel về Giám sát Ngân hàng Ngân hàng Thanh toán Quốc tế	Ông Laurent Le Mouël

Các Nguyên tắc Quản lý Rủi ro trong Ngân hàng Điện tử

Tóm tắt

Những sáng kiến công nghệ ngày càng phát triển cùng sự cạnh tranh giữa các tổ chức ngân hàng và những thành viên mới tham gia thị trường đã tạo điều kiện cho khách hàng bán buôn và bán lẻ tiếp cận tới ngày càng nhiều các sản phẩm và dịch vụ ngân hàng thông qua một kênh cung cấp dịch vụ điện tử được gọi chung là dịch vụ ngân hàng điện tử. Tuy nhiên, ngoài các lợi ích của ngân hàng điện tử, sự phát triển nhanh chóng của loại hình dịch vụ này cũng tiềm ẩn nhiều rủi ro.

Ủy ban Basel về Giám sát Ngân hàng cho rằng các ngân hàng cần xác định, xử lý và quản lý các rủi ro này một cách cẩn trọng phù hợp với các tính chất căn bản và thách thức của các dịch vụ ngân hàng điện tử. Các tính chất này bao gồm tốc độ thay đổi chưa từng có về các sáng kiến kỹ thuật và dịch vụ khách hàng, tính chất phát triển rộng rãi và sẵn có của các hệ thống điện tử, sự tích hợp các ứng dụng ngân hàng điện tử với các hệ thống máy tính cũ và sự phụ thuộc ngày càng tăng của ngân hàng vào bên thứ ba cung cấp công nghệ thông tin cần thiết. Trong văn bản này, Uỷ ban không đề cập tới những rủi ro mới mà chỉ lưu ý rằng các tính chất này đã thay đổi và đã sửa đổi một số rủi ro truyền thống liên quan đến hoạt động ngân hàng, đặc biệt là rủi ro chiến lược, tác nghiệp, pháp lý và uy tín có tác động đến tổng mức độ rủi ro của ngân hàng.

Dựa trên các kết luận này, Ủy ban cho rằng các nguyên tắc quản trị rủi ro hiện nay vẫn có thể áp dụng trong hoạt động ngân hàng điện tử nhưng cần được chỉnh sửa phù hợp và trong một số trường hợp cần mở rộng nhằm giải quyết các vấn đề liên quan đến rủi ro phát sinh từ tính chất của hoạt động ngân hàng điện tử. Hiện nay, Ủy ban cho rằng Hội đồng Quản trị và Ban (tổng) giám đốc ngân hàng đương nhiệm cần triển khai nhằm đảm bảo rằng ngân hàng đã đánh giá và chỉnh sửa nếu cần thiết các chính sách và qui trình quản trị rủi ro đối với hoạt động ngân hàng điện tử đã hoặc sắp triển khai. Ủy ban cũng cho rằng việc tích hợp các ứng dụng ngân hàng điện tử với các hệ thống máy tính cũ cũng dẫn tới sự cần thiết phải có phương thức tiếp cận quản trị rủi ro tích hợp đối với toàn bộ hoạt động của ngân hàng.

Nhằm hỗ trợ cho các hoạt động này, Ủy ban đã xác định mười bốn *Nguyên tắc Quản lý Rủi ro trong Ngân hàng Điện tử* nhằm giúp ngân hàng mở rộng các chính sách và qui trình giám sát rủi ro hiện tại để quản lý hoạt động ngân hàng điện tử.

Các Nguyên tắc Quản trị Rủi ro này không phải là các yêu cầu bắt buộc hoặc "thông lệ tốt nhất". Ủy ban cho rằng việc mô tả chi tiết các yêu cầu quản trị rủi ro trong lĩnh vực ngân hàng điện tử có thể gây phản tác dụng, lý do là vì các yêu cầu này sẽ nhanh chóng trở nên lỗi thời vì tốc độ thay đổi về công nghệ và sáng kiến dịch vụ khách hàng. Do đó, Ủy ban chỉ nêu lên những kỳ vọng về công tác giám sát và hướng dẫn được thể hiện bằng *Các Nguyên tắc Quản trị Rủi ro* nhằm tăng cường tính an toàn và hoạt động hiệu quả của các hoạt động ngân hàng điện tử trong khi vẫn bảo toàn sự năng động cần thiết trong quá trình triển khai thực tế xuất phát từ tốc độ thay đổi trong lĩnh vực này. Hơn nữa, Ủy ban nhận định rằng mức độ nguy cơ rủi ro của mỗi ngân hàng là khác nhau và cần có phương thức quản trị rủi ro phù hợp được điều chỉnh cụ thể tùy thuộc vào qui mô của hoạt động ngân hàng điện tử, mức độ nghiêm trọng của các rủi ro hiện tại, sự sẵn sàng và khả năng quản trị rủi ro của ngân hàng. Điều này cho thấy phương thức "áp dụng chung cho mọi đối tượng" trong vấn đề quản trị rủi ro ngân hàng điện tử là không phù hợp.

Cũng vì lý do này mà *Các Nguyên tắc Quản trị Rủi ro* do Ủy ban đề ra không phục vụ mục đích cung cấp các giải pháp kỹ thuật cụ thể hoặc các tiêu chuẩn liên quan đến ngân hàng điện tử. Các ngân hàng sẽ tự giải quyết các vấn đề liên quan đến giải pháp kỹ thuật và đưa ra các tiêu chuẩn phù hợp với thực tế phát triển của công nghệ. Tuy nhiên, nhằm hỗ trợ cho *Các Nguyên tắc Quản trị Rủi ro*, phần phụ lục của Báo cáo này đã liệt kê một số thông lệ đang được sử dụng rộng rãi hiện nay làm ví dụ trong vấn đề hạn chế rủi ro của dịch vụ ngân hàng điện tử.

Do đó, *Các Nguyên tắc Quản trị Rủi ro* và các thông lệ tốt nhất được đề cập trong Báo cáo này có thể được các cơ quan giám sát ngân hàng quốc gia sử dụng làm công cụ và chỉnh sửa cho phù hợp với các yêu cầu và mức độ rủi ro cụ thể tại các quốc gia đó. Trong một số vấn đề, Ủy ban hoặc các cơ quan giám sát ngân hàng quốc gia đã đề cập tới các Nguyên tắc này trong các văn bản hướng dẫn trước đây của Uỷ ban. Tuy nhiên, một số vấn đề như quản lý quan hệ thuê ngoài (outsourcing), kiểm soát an ninh, quản trị rủi ro pháp lý và uy tín đã bổ sung thêm các nguyên tắc chi tiết hơn so với các văn bản hướng dẫn đã phát hành từ đây trước đến nay do tính chất đặc thù và bối cảnh của kênh cung cấp dịch vụ qua mạng Internet.

Các Nguyên tắc Quản trị Rủi ro được chia làm ba phần và có sự liên kết với nhau. Các vấn đề được phân theo từng nhóm nhằm đề cập rõ ràng đến các vấn đề sau: *Giám sát của Hội đồng Quản trị và Ban (tổng) giám đốc; Kiểm soát An ninh; và Quản trị Rủi ro Pháp lý và Uy tín của ngân hàng.*

Giám sát của Hội đồng Quản trị và Ban (tổng) giám đốc

Vì Hội đồng Quản trị và Ban (tổng) giám đốc chịu trách nhiệm xây dựng chiến lược kinh doanh và cơ chế quản lý giám sát hiệu quả đối với rủi ro nên họ cần ra quyết định chiến lược được thể hiện rõ ràng bằng văn bản đối với việc ngân hàng có kế hoạch cung cấp dịch vụ ngân hàng điện tử hay không và nếu có thì sẽ được triển khai như thế nào. Quyết định ban đầu cần tính tới các trách nhiệm giải trình cụ thể, chính sách và biện pháp kiểm soát đối với các rủi ro, bao gồm cả những rủi ro phát sinh trong bối cảnh vượt phạm vi biên giới. Việc kiểm soát quản lý hiệu quả cần bao gồm việc đánh giá và chấp thuận các vấn đề chủ yếu trong quá trình kiểm soát an ninh của ngân hàng như việc xây dựng và duy trì một cơ sở hạ tầng kiểm soát an ninh nhằm bảo vệ các hệ thống và dữ liệu của dịch vụ ngân hàng điện tử trước các mối đe dọa xuất phát nội bộ và bên ngoài. Kiểm soát quản lý hiệu quả cũng bao gồm một qui trình quản lý rủi ro tổng thể gắn liền tới mức độ phức tạp và sự phụ thuộc ngày càng tăng vào các mối quan hệ thuê ngoài và các nhà cung cấp dịch vụ là bên thứ ba để thực hiện chức năng dịch vụ ngân hàng điện tử quan trọng.

Kiểm soát An ninh

Trong khi Hội đồng Quản trị có trách nhiệm đảm bảo triển khai các qui trình kiểm soát an ninh phù hợp đối với dịch vụ ngân hàng điện tử thì nội dung của các qui trình này cần sự quan tâm đặc biệt của Ban (tổng) giám đốc vì dịch vụ ngân hàng điện tử luôn làm nảy sinh các vấn đề về an ninh với mức độ ngày càng tăng. Điều này bao gồm việc xây dựng cơ chế đặc quyền cấp phép phù hợp và các biện pháp chứng thực, giới hạn truy cập phần cứng và hệ thống, có biện pháp an ninh phù hợp với cơ sở hạ tầng nhằm duy trì ranh giới và giới hạn hoạt động của người sử dụng nội bộ và bên ngoài, toàn vẹn dữ liệu của các giao dịch, hồ sơ và thông tin. Ngoài ra, cần phải đảm bảo luôn lưu giữ đầy đủ các tập bản ghi bằng chứng của tất cả các giao dịch ngân hàng điện tử và có các biện pháp nhằm bảo toàn tính bảo mật của

các thông tin ngân hàng điện tử quan trọng phù hợp với mức độ nhạy cảm của các thông tin này.

Mặc dù các hệ thống luật pháp qui định khác nhau về sự riêng tư và bảo vệ khách hàng nhưng nói chung, ngân hàng có trách nhiệm rõ ràng tạo cho khách hàng cảm thấy thoải mái trong việc công bố thông tin, bảo vệ dữ liệu khách hàng và khả năng cung cấp dịch vụ ngân hàng tương tự với mức độ mà khách hàng nhận được khi sử dụng các kênh cung cấp dịch vụ ngân hàng truyền thống.

Nhằm giảm thiểu rủi ro uy tín và pháp lý liên quan đến các hoạt động ngân hàng điện tử cung cấp trong và ngoài nước, ngân hàng cần công bố đầy đủ thông tin trên trang chủ và triển khai các biện pháp phù hợp nhằm đảm bảo rằng tính riêng tư của khách hàng được bảo vệ theo qui định của pháp luật tại nơi ngân hàng cung cấp dịch vụ ngân hàng điện tử.

Quản trị Rủi ro Pháp lý và Uy tín

Nhằm bảo vệ ngân hàng trước rủi ro kinh doanh, pháp lý và uy tín, dịch vụ ngân hàng điện tử phải được cung cấp trên cơ sở nhất quán và kịp thời như khách hàng mong đợi, nhanh chóng và liên tục phục vụ nhu cầu giao dịch có thể tăng cao. Ngân hàng phải có khả năng cung cấp dịch vụ ngân hàng điện tử cho tất cả người sử dụng đầu cuối và trong mọi hoàn cảnh. Cơ chế xử lý tình huống hiệu quả cũng quan trọng nhằm giảm thiểu các rủi ro tác nghiệp, pháp lý và uy tín nảy sinh từ các sự kiện bất thường, bao gồm các vụ tấn công nội bộ và từ bên ngoài có thể gây ảnh hưởng tới sự cung cấp và hệ thống dịch vụ ngân hàng điện tử. Để đáp ứng kỳ vọng của khách hàng, ngân hàng cần có khả năng cung cấp dịch vụ, kế hoạch dự phòng và duy trì kinh doanh hiệu quả. Ngân hàng cần xây dựng các kế hoạch xử lý tình huống phù hợp, bao gồm các chiến lược truyền thông nhằm đảm bảo duy trì kinh doanh, kiểm soát rủi ro uy tín và hạn chế trách nhiệm liên quan đến việc ngừng trệ dịch vụ ngân hàng điện tử.

Các Nguyên tắc Quản trị Rủi ro trong Ngân hàng Điện tử

I. Giới thiệu

Ngân hàng đã cung cấp dịch vụ điện tử và dịch vụ kinh doanh từ xa cho khách hàng trong nhiều năm. Dịch vụ chuyển tiền điện tử bao gồm các khoản thanh toán có mệnh giá nhỏ và các hệ thống quản lý tiền mặt cho công ty cũng như các máy rút tiền tự động dành cho công chúng và quản lý tài khoản bán lẻ là những bộ phận cố định. Tuy nhiên, mạng Internet[1] được thế giới chấp nhận rộng rãi đóng vai trò là một kênh cung cấp các sản phẩm và dịch vụ ngân hàng đã đem lại các cơ hội kinh doanh mới cho ngân hàng cũng như đem lại các tiện ích phục vụ khách hàng.

Các sáng kiến công nghệ ngày càng phát triển và sự cạnh tranh liên tục giữa các ngân hàng và những thành viên mới tham gia thị trường đã tạo điều kiện cho các khách hàng bán buôn và bán lẻ tiếp cận với các sản phẩm và dịch vụ ngân hàng điện tử[2] đa dạng hơn. Các sản phẩm này bao gồm các hoạt động ngân hàng truyền thống như việc truy cập thông tin tài chính, đi vay và mở tài khoản tiền gửi cũng như các sản phẩm và dịch vụ khá mới như dịch vụ thanh toán hóa đơn điện tử, các "cổng" tài chính cá nhân, hợp nhất tài khoản[3] và thị trường trao đổi và gặp gỡ của các doanh nghiệp.

Mặc dù các sáng kiến công nghệ đem lại nhiều lợi ích có giá trị nhưng sự phát triển nhanh chóng của dịch vụ ngân hàng điện tử cũng làm nảy sinh nhiều rủi ro và điều quan trọng là các ngân hàng cần xác định và quản lý những rủi ro này một cách thận trọng[4]. Những phát triển này là cơ sở để Ủy ban Basel về Giám sát Ngân hàng tiến hành một nghiên cứu sơ bộ về các khuyến nghị quản trị rủi ro trong ngân hàng điện tử và tiền điện tử (e-money) vào năm 1998[5]. Nghiên cứu sơ bộ này cho thấy sự cần thiết phải nghiên cứu thêm trong lĩnh vực quản trị rủi

[1] Trong Báo cáo này, mạng Internet được định nghĩa bao gồm tất cả các công nghệ liên quan đến web và các hệ thống viễn thông có tính mở từ kết nối theo kiểu quay số (dial-up connections), Mạng Toàn Cầu (www) công cộng và các mạng riêng ảo.

[2] Trong Báo cáo này, ngân hàng điện tử hoặc ***e-banking*** là việc cung cấp các sản phẩm và dịch vụ ngân hàng bán lẻ có giá trị thấp thông qua các kênh điện tử cũng như các dịch vụ thanh toán điện tử có giá trị lớn và các dịch vụ ngân hàng bán buôn được cung cấp qua kênh điện tử.

[3] Dịch vụ hợp nhất tài khoản cho phép khách hàng nhận được thông tin cân đối chung trên tài khoản tài chính và phi tài chính. Nhân viên hợp nhất thực hiện vai trò là một đại lý cung cấp cho khách hàng thông tin đã được cân đối trên tài khoản của họ mở tại các thể chế tín dụng khác nhau. Khách hàng cung cấp cho nhân viên hợp nhất mật mã an ninh hoặc mã số nhận dạng cá nhân cần thiết để truy cập thông tin và cân đối tài khoản chủ yếu thông qua việc chia nhỏ màn hình, một quá trình lựa chọn dữ liệu từ trang chủ của các ngân hàng khác, thông thường là ngân hàng không biết, hoặc thông qua việc cung cấp dữ liệu trực tiếp theo hợp đồng đã ký kết giữa các thể chế tài chính với nhau.

[4] Vì sự phát triển nhanh chóng của công nghệ thông tin nên không thể mô tả một cách thấu đáo các rủi ro này. Tuy nhiên, các rủi ro đối với ngân hàng cung cấp dịch vụ ngân hàng điện tử phần lớn không phải là mới và các rủi ro này đã được phân loại và đề cập trong Các Nguyên tắc Cơ bản trong Giám sát Ngân hàng Hiệu quả của Ủy ban hồi tháng 9 năm 1997. Tài liệu hướng dẫn này xác định 8 loại rủi ro bao gồm rủi ro tín dụng, rủi ro quốc gia, rủi do chuyển đổi, rủi ro thị trường, rủi ro lãi suất, rủi ro thanh khoản, rủi ro tác nghiệp, rủi ro pháp lý và rủi ro uy tín. Có thể tham khảo Các Nguyên tắc Cơ bản tại trang chủ của Ngân hàng Thanh toán Quốc tế (BIS), http://www.bis.org.

[5] Tham khảo tài liệu "Quản trị Rủi ro trong Hoạt động Ngân hàng Điện tử và Tiền Điện tử", Tháng 3 năm 1998, tại trang chủ của Ngân hàng Thanh toán Quốc tế, http://www.bis.org.

ro ngân hàng điện tử và điều này đã thúc đẩy sự thành lập một nhóm công tác có sự tham gia của các cơ quan giám sát ngân hàng và ngân hàng trung ương có tên là Nhóm Công tác về Ngân hàng Điện tử (EBG) vào tháng 11 năm 1999.

Ủy ban Basel đã phát hành Báo cáo của Nhóm Công tác về quản trị rủi ro và các vấn đề giám sát nảy sinh từ việc phát triển dịch vụ ngân hàng điện tử vào tháng 10 năm 2000[6]. Báo cáo này đã xếp loại và đánh giá các rủi ro chính liên quan đến ngân hàng điện tử, cụ thể là rủi ro chiến lược, rủi ro uy tín, rủi ro tác nghiệp (bao gồm rủi ro an ninh và rủi ro pháp lý)[7], rủi ro tín dụng, rủi ro thị trường và rủi ro thanh khoản. Nhóm Công tác về Ngân hàng Điện tử đã kết luận rằng các rủi ro có thể nảy sinh trong hoạt động ngân hàng điện tử đều đã được xác định trong tài liệu mà Ủy ban phát hành trước đó. Tuy nhiên, Ủy ban lưu ý rằng dịch vụ ngân hàng điện tử đang phát triển và đã sửa đổi một số các rủi ro truyền thống, theo đó sẽ có tác động tới toàn bộ khả năng chịu đựng rủi ro của ngân hàng (risk profile). Đặc biệt, rủi ro chiến lược, rủi ro tác nghiệp và rủi ro uy tín rõ ràng đã trở nên phức tạp hơn do sự xuất hiện và phát triển nhanh chóng về mức độ phức tạp của công nghệ trong hoạt động ngân hàng điện tử.

A. Các thách thức trong Quản trị Rủi ro

Nhóm Công tác lưu ý rằng các tính chất căn bản của ngân hàng điện tử (và thương mại điện tử nói chung) đã đặt ra một số thách thức đối với quản trị rủi ro:

- Tốc độ thay đổi về công nghệ và sáng kiến dịch vụ khách hàng trong ngân hàng điện tử là chưa từng xảy ra. Trước đây, các nghiệp vụ ngân hàng mới chỉ được triển khai sau khi đã được thử nghiệm kỹ lưỡng trong một thời gian dài. Tuy nhiên, ngày nay với những áp lực cạnh tranh gay gắt, các ngân hàng cần khẩn trương triển khai những nghiệp vụ kinh doanh mới chỉ trong một khoảng thời gian rất eo hẹp – thông thường chỉ có một vài tháng để triển khai ý tưởng thành sản phẩm cụ thể. Sự cạnh tranh này đã làm gia tăng thách thức trong công tác quản trị đối với việc đảm bảo thực hiện đánh giá chiến lược phù hợp, phân tích rủi ro và đánh giá an ninh trước khi triển khai các nghiệp vụ ngân hàng điện tử.

- Các trang chủ giao dịch ngân hàng điện tử và các nghiệp vụ kinh doanh bán buôn và bán lẻ kèm theo thường được tích hợp tối đa ở mức có thể với các hệ thống máy tính cũ để xử lý thẳng các giao dịch điện tử. Qui trình xử lý tự động thẳng làm giảm rủi ro nhầm lẫn do yếu tố con người và gian lận trong quá trình xử lý thủ công, nhưng điều này cũng làm tăng sự phụ thuộc vào thiết kế và kiến trúc hệ thống hợp lý cũng như khả năng tương tác hệ thống và mở rộng hoạt động.

- Ngân hàng điện tử làm tăng sự phụ thuộc của ngân hàng vào công nghệ thông tin, do đó làm tăng mức độ phức tạp về kỹ thuật trong nhiều vấn đề tác nghiệp và an ninh và có xu hướng tăng cường quan hệ đối tác, liên minh và thuê ngoài với bên thứ ba, trong đó có nhiều đối tượng chưa có qui định chế tài. Điều này đã dẫn tới sự ra đời của các mô hình kinh doanh mới cho các đối tượng là ngân hàng và phi ngân hàng ví

[6] Tham khảo tài liệu "Các Sáng kiến của Nhóm Công tác về Ngân hàng Điện tử và Các Nghiên cứu", tháng 10 năm 2000 tại trang chủ của Ngân hàng Thanh toán Quốc tế (BIS), http://www.bis.org.

[7] Báo cáo này sử dụng định nghĩa của Ủy ban về rủi ro tác nghiệp, bao gồm rủi ro an ninh và rủi ro pháp lý (tham khảo tài liệu Thỏa thuận Mới về Vốn của Ủy Ban Basel về Giám sát Ngân hàng, tháng 4 năm 2003, đoạn 607: "rủi ro gây mất mát do qui trình nội bộ không phù hợp hoặc không hoạt động, vì lý do con người và hệ thống hoặc các sự kiện bên ngoài").

dụ như các nhà cung cấp dịch vụ Internet, công ty viễn thông và các công ty hoạt động trong lĩnh vực công nghệ khác.

- Mạng Internet có ở khắp nơi và mang tính toàn cầu. Đó là một mạng có tính mở và bất kỳ ai cũng có thể truy cập từ mọi nơi trên thế giới, với những thông điệp xuất phát từ bất kỳ đâu qua những địa điểm vô danh và thông qua những thiết bị không dây đang ngày một phát triển. Do đó, điều này đã làm tăng thêm tầm quan trọng của các biện pháp kiểm soát an ninh, kỹ thuật chứng thực khách hàng, bảo vệ dữ liệu, qui trình lưu bản ghi bằng chứng phục vụ đánh giá độc lập và các tiêu chuẩn bảo vệ sự riêng tư của khách hàng.

B. Nguyên tắc Quản trị Rủi ro

Dựa trên các nghiên cứu trước đây của Nhóm Công tác về Ngân hàng Điện tử, Ủy ban kết luận rằng trong khi các nguyên tắc quản trị rủi ro ngân hàng truyền thống là có thể ứng dụng cho các hoạt động ngân hàng điện tử thì tính chất phức tạp của kênh chuyển giao là mạng Internet cho thấy việc áp dụng các nguyên tắc này cần được điều chỉnh phù hợp với nhiều hoạt động ngân hàng trực tuyến và các khó khăn trong quản trị rủi ro. Do đó, Ủy ban cho rằng Hội đồng Quản trị và Ban (tổng) giám đốc ngân hàng cần có trách nhiệm trong việc triển khai các bước để đảm bảo rằng ngân hàng đã đánh giá và chỉnh sửa nếu thấy cần thiết các chính sách và qui trình quản trị rủi ro hiện thời nhằm quản lý được các hoạt động ngân hàng điện tử hiện tại và trong trương lai. Ngoài ra, vì Ủy ban cho rằng các ngân hàng cần áp dụng phương thức quản trị rủi ro tích hợp cho toàn bộ các hoạt động ngân hàng nên điều quan trọng là việc giám sát quản lý rủi ro đối với các hoạt động ngân hàng điện tử phải trở thành một phần không thể tách rời trong cơ cấu quản trị rủi ro tổng thể của ngân hàng.

Để thực hiện được việc này, Ủy ban đề nghị Nhóm Công tác về Ngân hàng Điện tử xác định những nguyên tắc quản trị rủi ro then chốt nhằm giúp đỡ ngân hàng mở rộng các chính sách và thủ tục giám sát quản trị rủi ro hiện đang áp dụng để đáp ứng các hoạt động ngân hàng điện tử và ngược lại, giúp nâng cao khả năng cung cấp các sản phẩm và dịch vụ ngân hàng điện tử một cách an toàn và hiệu quả.

Các Nguyên tắc Quản trị Rủi ro trong Ngân hàng Điện tử được đề cập trong Báo cáo này không phải là những yêu cầu bắt buộc hoặc được coi là "thông lệ tốt nhất" mà chỉ là hướng dẫn nhằm nâng cao an toàn và hiệu quả trong hoạt động ngân hàng điện tử. Ủy ban cho rằng việc đưa ra các yêu cầu quản trị rủi ro chi tiết trong lĩnh vực ngân hàng điện tử có thể gây phản tác dụng vì các yêu cầu này sẽ nhanh chóng trở nên lỗi thời vì tốc độ thay đổi về công nghệ và sáng kiến dịch vụ khách hàng. Do đó, các nguyên tắc đề cập trong báo cáo này chỉ thể hiện những kỳ vọng trong công tác giám sát đối với mục tiêu giám sát tổng thể ngân hàng nhằm đảm bảo sự an toàn và hiệu quả của hệ thống tài chính hơn là các qui định chặt chẽ.

Ủy ban có quan điểm rằng những giám sát kỳ vọng cần được chỉnh sửa và áp dụng đối với kênh cung cấp dịch ngân hàng điện tử nhưng không khác biệt về căn bản so với những giám sát kỳ vọng đang áp dụng đối với các hoạt động ngân hàng cung cấp các qua kênh khác. Do đó, các nguyên tắc trình bày dưới đây phần lớn bắt nguồn và được sửa đổi từ các nguyên tắc giám sát đã được Ủy ban hoặc các cơ quan giám sát ngân hàng quốc gia trình bày trong nhiều năm. Trong một số phần, ví dụ về quản lý quan hệ thuê ngoài, kiểm soát an ninh, quản lý rủi ro pháp lý và uy tín, tính chất và phạm vi của kênh cung cấp là mạng Internet cho thấy sự cần thiết phải có những nguyên tắc cụ thể hơn những gì đã được trình bày từ trước đến nay.

Ủy ban nhận thấy ngân hàng sẽ cần xây dựng các qui trình quản trị rủi ro phù hợp với mức độ chịu đựng rủi ro cụ thể của từng ngân hàng, cơ cấu tác nghiệp và văn hóa quản trị công ty cũng như việc tuân thủ với những yêu cầu và chính sách quản trị rủi ro của các cơ quan giám sát ngân hàng tại (các) quốc gia. Ngoài ra, nhiều thông lệ quản trị rủi ro trong ngân hàng điện tử trong Báo cáo này tuy hiện tại đang là những thông lệ tốt nhất nhưng cũng không phải là tổng thể hoặc tiêu chuẩn vì nhiều biện pháp kiểm soát an ninh hoặc các kỹ thuật quản trị rủi ro khác tiếp tục thay đổi nhanh chóng nhằm theo kịp sự thay đổi công nghệ và các ứng dụng kinh doanh mới.

Báo cáo này không tập trung vào việc đưa ra các giải pháp kỹ thuật cụ thể để giải quyết các rủi ro cụ thể hoặc đề ra các tiêu chuẩn kỹ thuật đối với ngân hàng điện tử. Khi công nghệ phát triển thì các vấn đề kỹ thuật sẽ được ngân hàng và các tổ chức liên tục tự giải quyết. Ngoài ra, khi ngành công nghiệp ngân hàng tiếp tục giải quyết các vấn đề kỹ thuật trong ngân hàng điện tử bao gồm các thách thức về an ninh thì nhiều sáng kiến và giải pháp quản lý rủi ro tiết kiệm chi phí sẽ xuất hiện. Các giải pháp này cũng giải quyết các vấn đề liên quan đến sự khác nhau về qui mô, mức độ phức tạp và văn hóa quản trị rủi ro và các qui định về luật pháp và qui chế áp dụng tại các quốc gia trong việc quản lý hoạt động ngân hàng.

Vì vậy, Ủy ban cho rằng việc áp dụng phương thức "áp dụng chung cho mọi đối tượng" trong vấn đề quản trị rủi ro ngân hàng điện tử là không phù hợp và Ủy ban cũng khuyến khích việc trao đổi các thông lệ tốt nhất và các tiêu chuẩn để giải quyết các khía cạnh rủi ro khác của kênh chuyển giao ngân hàng điện tử. Để quán triệt tư tưởng giám sát này, các nguyên tắc quản trị rủi ro và các thông lệ tốt nhất được đề cập trong Báo cáo này được coi là những công cụ phục vụ cho các cơ quan giám sát quốc gia và được triển khai có chỉnh sửa nhằm thể hiện các yêu cầu giám sát cụ thể của quốc gia trong trường hợp cần thiết và hỗ trợ nâng cao sự an toàn và hiệu quả trong việc triển khai và hoạt động ngân hàng điện tử.

Ủy ban nhận thấy mức độ chịu đựng rủi ro của từng ngân hàng là khác nhau và cần có phương thức kiềm chế rủi ro phù hợp đối với qui mô của nghiệp vụ ngân hàng điện tử, mức độ rủi ro hiện tại, và sự sẵn sàng và khả năng của ngân hàng trong việc quản trị rủi ro. Những sự khác biệt cũng cho thấy các nguyên tắc quản trị rủi ro được đề cập trong Báo cáo này là đủ linh hoạt để ngân hàng tại nhiều quốc gia có thể triển khai. Các cơ quan giám sát quốc gia sẽ đánh giá mức độ rủi ro liên quan đến các hoạt động ngân hàng điện tử hiện hữu tại một ngân hàng cụ thể và xác định liệu cơ cấu quản trị rủi ro của ngân hàng có thể đáp ứng được các nguyên tắc quản trị rủi ro đối với ngân hàng điện tử hay không và nếu có thì ở mức độ nào.

II. Các Nguyên tắc Quản trị Rủi ro trong Ngân hàng Điện tử

Các nguyên tắc quản trị rủi ro đề cập trong Báo cáo này được chia làm 2 phần và có sự liên kết với nhau với các nhóm vấn đề. Tuy nhiên, các nguyên tắc này không được sắp xếp theo mức độ quan trọng. Vì mức độ quan trọng sẽ có thể thay đổi theo thời gian, do đó, tốt nhất là chỉ đề cập đến các vấn đề chung và tránh việc ưu tiên các nguyên tắc này so với nguyên tắc khác.

A. Giám sát của Hội đồng Quản trị và Ban (tổng) giám đốc[8] (Nguyên tắc 1-3):

1. Giám sát quản trị hiệu quả đối với các hoạt động ngân hàng điện tử.

2. Xây dựng một qui trình kiểm soát an ninh tổng thể.

3. Qui trình giám sát quản trị và tuân thủ tổng thể đối với các quan hệ thuê ngoài và sự phụ thuộc vào các bên thứ ba khác.

B. Kiểm soát An ninh (Nguyên tắc 4-10):

4. Chứng thực khách hàng sử dụng dịch vụ ngân hàng điện tử.

5. Không khước từ và trách nhiệm giải trình đối với các giao dịch ngân hàng điện tử.

6. Các biện pháp đảm bảo phân công nhiệm vụ phù hợp.

7. Biện pháp kiểm soát chứng thực phù hợp trong hệ thống, cơ sở dữ liệu và ứng dụng.

8. Toàn vẹn dữ liệu của các giao dịch, hồ sơ và thông tin.

9. Xây dựng các tập tin dữ liệu bằng chứng phục vụ cho kiểm tra độc lập đối với các giao dịch ngân hàng điện tử.

10. Bảo mật các thông tin quan trọng của ngân hàng.

C. Quản trị Rủi ro Pháp lý và Rủi ro Uy tín (Nguyên tắc 11-14):

11. Công bố thông tin phù hợp đối với các dịch vụ ngân hàng điện tử.

12. Sự riêng tư của thông tin khách hàng.

13. Năng lực, duy trình kinh doanh và kế hoạch dự phòng nhằm đảm bảo hoạt động liên tục của các dịch vụ và hệ thống ngân hàng điện tử.

14. Kế hoạch xử lý tình huống.

Mỗi vấn đề nêu trên được thảo luận cụ thể hơn trong các phần sau vì các vấn đề này liên quan đến ngân hàng điện tử và các nguyên tắc quản trị rủi ro tương ứng cần phải được ngân hàng

[8] Văn bản này đề cập đến một cơ cấu quản lý bao gồm hội đồng quản trị và ban (tổng) giám đốc. Uỷ ban Basel nhận thức rằng có những khác biệt đáng kể trong khuôn khổ lập pháp và giám sát giữa các quốc gia liên quan đến chức năng nhiệm vụ của hội đồng quản trị và ban (tổng) giám đốc. Ở một số quốc gia, hội đồng quản trị có chức năng chính, nếu không muốn nói là duy nhất, trong việc giám sát cơ quan điều hành (ban tổng giám đốc, ban (tổng) giám đốc) để bảo đảm cơ quan này hoàn thành nhiệm vụ của mình. Vì lý do này, trong một số trường hợp hội đồng quản trị còn được gọi là hội đồng giám sát. Điều này có nghĩa là hội đồng không có chức năng điều hành. Ở các quốc gia khác, hội đồng có thẩm quyền rộng hơn trong việc xây dựng khuôn khổ chung cho quản lý ngân hàng. Do những khác biệt này mà thuật ngữ "hội đồng quản trị" và "ban (tổng) giám đốc" được sử dụng trong văn bản này không phải để phân biệt giữa các chủ thể pháp lý mà để phân biệt hai chức năng ra quyết định trong ngân hàng.

xem xét giải quyết. Trong trường hợp cần thiết, các thông lệ tốt nhất được đề cập trong phần phụ lục kèm theo có thể được coi là những phương thức hiệu quả nhằm đối phó với các rủi ro này.

A. Giám sát của Hội đồng Quản trị và Ban (tổng) giám đốc (Nguyên tắc 1-3)

Hội đồng Quản trị và Ban (tổng) giám đốc chịu trách nhiệm xây dựng chiến lược kinh doanh của ngân hàng. Một chiến lược rõ ràng cần được quyết định xem liệu Hội đồng Quản trị có mong muốn cung cấp dịch vụ giao dịch ngân hàng điện tử hay không trước khi bắt đầu cung cấp các dịch vụ đó. Cụ thể là Hội đồng Quản trị cần đảm bảo rằng kế hoạch ngân hàng điện tử được tích hợp chặt chẽ với các mục đích chiến lược, có phân tích rủi ro đối với các hoạt động ngân hàng điện tử được đề xuất, biện pháp hạn chế rủi ro phù hợp và xây dựng quá trình theo dõi đối với các rủi ro đã được xác định và cần đánh giá liên tục kết quả của các hoạt động ngân hàng điện tử so với các mục đích và kết quả kinh doanh của ngân hàng.

Ngoài ra, Hội đồng Quản trị và Ban (tổng) giám đốc cần đảm bảo rằng các khía cạnh liên quan đến tác nghiệp và rủi ro an ninh của ngân hàng trong chiến lược kinh doanh ngân hàng điện tử đã được cân nhắc và giải quyết phù hợp. Việc cung cấp các dịch vụ tài chính trên mạng Internet có thể làm thay đổi to lớn và/hoặc tăng các rủi ro đối với các nghiệp vụ ngân hàng truyền thống (có nghĩa là rủi ro chiến lược, rủi ro uy tín, rủi ro tác nghiệp, rủi ro tín dụng và rủi ro thanh khoản). Do đó cần triển khai các bước nhằm đảm bảo rằng các qui trình hiện tại trong quản trị rủi ro, kiểm soát an ninh, tính tuân thủ và giám sát đối với các quan hệ thuê ngoài đã được đánh giá và chỉnh sửa phù hợp phục vụ cho dịch vụ ngân hàng điện tử.

Nguyên tắc 1: Hội đồng Quản trị và Ban (tổng) giám đốc cần xây dựng cơ chế giám sát hiệu quả đối với các rủi ro liên quan đến các hoạt động ngân hàng điện tử, bao gồm việc xây dựng các cơ chế trách nhiệm giải trình, chính sách và biện pháp kiểm soát quản lý rủi ro.

Việc đề cao cảnh giác trong giám sát là cần thiết trong cơ chế kiểm soát nội bộ hiệu quả đối với các hoạt động ngân hàng điện tử. Ngoài các tính chất đặc biệt của kênh cung cấp dịch vụ là mạng Internet đã được thảo luận trong phần Giới thiệu, các vấn đề sau liên quan đến ngân hàng điện tử có thể sẽ là thách thức to lớn đối với các qui trình quản trị rủi ro truyền thống:

- Các yếu tố chính của kênh cung cấp dịch vụ (mạng Internet và các công nghệ liên quan) nằm ngoài sự kiểm soát trực tiếp của ngân hàng.

- Mạng Internet hỗ trợ cho kênh cung cấp dịch vụ hiện diện tại các quốc gia với các qui định pháp lý khác nhau, bao gồm cả những dịch vụ hiện ngân hàng không cung cấp tại trụ sở.

- Sự phức tạp của các vấn đề liên quan đến ngân hàng điện tử và điều này liên quan đến các khái niệm và thuật ngữ kỹ thuật chuyên ngành mức độ cao và đa phần là nằm ngoài sự hiểu biết truyền thống của Hội đồng Quản trị và Ban (tổng) giám đốc.

Với các tính chất đặc thù của ngân hàng điện tử, các dự án ngân hàng điện tử mới có khả năng tác động không nhỏ đến mức độ chịu đựng rủi ro của ngân hàng và Hội đồng Quản trị và Ban (tổng) giám đốc cần đánh giá chiến lược của ngân hàng bằng việc phân tích lợi/hại và phân tích chiến lược phù hợp. Nếu không đánh giá chiến lược phù hợp ngay từ đầu và liên tục đánh giá quá trình thực hiện so với kế hoạch thì ngân hàng sẽ chịu rủi ro trong việc đánh

giá sai lệch chi phí và/hoặc đánh giá quá cao khả năng bù đắp của các sáng kiến ngân hàng điện tử.

Ngoài ra, Hội đồng Quản trị và Ban (tổng) giám đốc cần đảm bảo rằng ngân hàng sẽ không triển khai nghiệp vụ kinh doanh ngân hàng điện tử mới hoặc áp dụng các công nghệ mới khi chưa có kinh nghiệm cần thiết nhằm giám sát quản trị rủi ro một cách đầy đủ. Kinh nghiệm quản lý và trình độ của nhân viên phải tương xứng với tính chất và mức độ phức tạp của các ứng dụng ngân hàng điện tử cùng các công nghệ có liên quan. Việc có đủ trình độ là cần thiết cho dù hệ thống và dịch vụ ngân hàng điện tử được nội bộ quản lý hay thuê bên thứ ba. Qui trình giám sát của Ban (tổng) giám đốc cần phải năng động nhằm can thiệp chính xác và hiệu quả vào bất kỳ vấn đề gì quan trọng trong hệ thống ngân hàng điện tử hoặc trường hợp xảy ra đột nhập an ninh. Rủi ro uy tín ở mức độ cao hơn trong nghiệp vụ ngân hàng điện tử cho thấy sự cần thiết phải cảnh giác theo dõi khả năng hoạt động của hệ thống, sự hài lòng của khách hàng cũng như phải có cơ chế báo cáo giải quyết tình huống cho Hội đồng Quản trị và Ban (tổng) giám đốc.

Cuối cùng, Hội đồng Quản trị và Ban (tổng) giám đốc cần đảm bảo rằng các qui trình quản trị rủi ro đối với các hoạt động ngân hàng điện tử được tích hợp vào phương thức quản trị rủi ro tổng thể của ngân hàng. Các chính sách và qui trình quản trị rủi ro của ngân hàng cần được đánh giá nhằm đảm bảo có khả năng giải quyết các rủi ro mới nảy sinh từ các hoạt động ngân hàng điện tử hiện nay hoặc trong tương lai. Các bước bổ sung trong giám sát quản trị rủi ro mà Hội đồng Quản trị và Ban (tổng) giám đốc nên cân nhắc xem xét bao gồm:

- Xây dựng mức độ chấp nhận rủi ro cụ thể đối với nghiệp vụ ngân hàng điện tử của ngân hàng.

- Xây dựng cơ chế báo cáo và phân công quyền hạn bao gồm các thủ tục báo cáo theo cấp bậc trong trường hợp xử lý tình huống có ảnh hưởng đến sự an toàn, hiệu quả và uy tín của ngân hàng (có nghĩa là việc xâm nhập hệ thống, vi phạm an ninh của nhân viên và bất kỳ việc sử dụng sai mục đích nghiêm trọng nào đối với các thiết bị máy tính)[9].

- Xử lý bất kỳ yếu tố rủi ro đặc trưng nào liên quan đến việc đảm bảo an ninh, toàn vẹn và sẵn sàng của các dịch vụ và sản phẩm ngân hàng điện tử và yêu cầu các đối tượng bên thứ ba mà ngân hàng thuê cung cấp hệ thống hoặc ứng dụng quan trọng phải có các biện pháp xử lý tương tự.

- Đảm bảo phải tiến hành phân tích rủi ro và tuân thủ phù hợp trước khi ngân hàng triển khai các hoạt động nghiệp vụ ngân hàng điện tử quốc tế.

Mạng Internet hỗ trợ rất nhiều cho khả năng cung cấp dịch vụ và sản phẩm của một ngân hàng trong vùng lãnh thổ không giới hạn về địa lý giữa các quốc gia. Nếu hoạt động ngân hàng điện tử vượt phạm vi biên giới này được triển khai mà không được cấp phép bằng văn bản cụ thể tại "quốc gia chủ nhà" thì ngân hàng càng chịu nguy cơ rủi ro về pháp lý, qui định và rủi ro quốc gia do có sự khác biệt lớn giữa các hệ thống luật pháp liên quan đến việc cấp phép hoạt động, giám sát ngân hàng và các qui định bảo vệ khách hàng. Vì cần phải tránh việc không tuân thủ luật và qui định tại một quốc gia nước ngoài cũng như cần phải quản trị

[9] Ngoài các yêu cầu về báo cáo nội bộ, thủ tục báo cáo tình huống cũng cần đề cập đến sự cần thiết phải báo cáo cho cơ quan giám sát ngân hàng.

các yếu tố rủi ro quốc gia có liên quan nên các ngân hàng triển khai nghiệp vụ ngân hàng điện tử quốc tế cần phải tìm hiểu kỹ các rủi ro trước khi triển khai và quản lý có hiệu quả các nghiệp vụ này[10].

Dựa vào qui mô và mức độ phức tạp của các hoạt động ngân hàng điện tử mà qui mô và cơ cấu các chương trình quản trị rủi ro sẽ khác nhau giữa các tổ chức ngân hàng. Các nguồn lực cần thiết để theo dõi dịch vụ ngân hàng điện tử cần phải tương xứng với chức năng giao dịch và tầm quan trọng của các hệ thống, khả năng bị thương tổn của các hệ thống và sự nhạy cảm của các thông tin được lưu chuyển.

Nguyên tắc 2: Hội đồng Quản trị và Ban (tổng) giám đốc cần đánh giá và chấp thuận các lĩnh vực then chốt trong qui trình kiểm soát an ninh của ngân hàng.

Hội đồng Quản trị và Ban (tổng) giám đốc cần giám sát việc xây dựng và duy trì liên tục một cơ sở hạ tầng kiểm soát an ninh nhằm bảo vệ cho các hệ thống và dữ liệu ngân hàng điện tử đối với các nguy cơ xuất phát từ bên trong và bên ngoài. Điều này bao gồm việc xây dựng các đặc quyền cấp phép phù hợp, kiểm soát truy cập lôgíc và truy cập ở mức vật lý, và cơ sở hạ tầng an ninh phù hợp nhằm duy trì các giới hạn hợp lý và hạn chế đối với các hoạt động của người sử dụng nội bộ và bên ngoài.

Bảo vệ tài sản của ngân hàng là một trong các trách nhiệm được giao của Hội đồng Quản trị và là một trong những trách nhiệm cơ bản của Ban (tổng) giám đốc. Tuy nhiên, đây là một nhiệm vụ có nhiều thách thức trong môi trường ngân hàng điện tử thay đổi nhanh chóng vì các rủi ro an ninh phức tạp gắn liền với việc hoạt động trên mạng công cộng Internet và sử dụng các công nghệ luôn đổi mới.

Để có những biện pháp kiểm soát an ninh phù hợp đối với các hoạt động ngân hàng điện tử, Hội đồng Quản trị và Ban (tổng) giám đốc cần đảm bảo rằng ngân hàng có một qui trình an ninh tổng thể, bao gồm các chính sách và thủ tục, đối phó với các nguy cơ an ninh tiềm tàng xuất phát từ bên trong hoặc bên ngoài trên cơ sở ngăn chặn và xử lý các tình huống xảy ra. Các yếu tố quan trọng của một qui trình an ninh ngân hàng điện tử hiệu quả bao gồm:

- Phân công trách nhiệm rõ ràng cho giám đốc/nhân viên trong việc giám sát việc xây dựng và duy trì các chính sách an ninh công ty[11].

- Có biện pháp kiểm soát phù hợp cụ thể nhằm ngăn chặn truy cập trái phép ở mức vật lý vào môi trường máy tính.

- Có biện pháp kiểm soát lôgíc và qui trình theo dõi phù hợp[12] nhằm ngăn chặn truy cập trái phép từ nội bộ[13] hoặc bên ngoài vào các ứng dụng và cơ sở dữ liệu ngân hàng điện tử.

[10] Để biết thêm chi tiết, tham khảo tài liệu của Ủy ban Basel về Giám sát Ngân hàng, Quản trị và Giám Sát các Hoạt động Ngân hàng Điện tử vượt phạm vi biên giới, tháng 7 năm 2003.

[11] Trách nhiệm này thông thường không phải là một phần trong chức năng kiểm toán, chức năng này có trách nhiệm đảm bảo rằng chức năng giám sát rủi ro được thực hiện một cách có hiệu quả.

[12] Bao gồm các quyền và đặc quyền truy cập được kiểm soát cũng như việc theo dõi liên tục các cố gắng thâm nhập hệ thống.

[13] Bao gồm nhân viên, nhà thầu và những đối tượng có quyền truy cập thông qua quan hệ thuê ngoài.

- Thường xuyên đánh giá và kiểm tra các biện pháp và kiểm soát an ninh bao gồm việc liên tục theo dõi sự phát triển của ngành công nghiệp an ninh hiện tại, cài đặt nâng cấp phần mềm, bản sửa lỗi phù hợp và các biện pháp cần thiết khác[14].

Phụ lục I đề cập bổ sung một số các thông lệ tốt nhất giúp đảm bảo an ninh cho ngân hàng điện tử.

Nguyên tắc 3: Hội đồng Quản trị và Ban (tổng) giám đốc cần xây dựng một qui trình giám sát và đánh giá tuân thủ liên tục và tổng thể nhằm quản lý các mối quan hệ thuê ngoài của ngân hàng và việc phụ thuộc vào bên thứ ba khác trong việc hỗ trợ dịch vụ ngân hàng điện tử.

Việc ngày càng phụ thuộc vào các đối tác và nhà cung cấp dịch vụ là bên thứ ba để thực hiện các chức năng ngân hàng điện tử quan trọng sẽ làm giảm khả năng kiểm soát trực tiếp của Ban (tổng) giám đốc ngân hàng. Do đó, cần có một qui trình tổng thể nhằm quản lý các rủi ro liên quan đến việc thuê ngoài và sự phụ thuộc vào các bên thứ ba khác. Qui trình này bao gồm các hoạt động của đối tác và các nhà cung cấp dịch vụ là bên thứ ba, bao gồm cả việc thuê thầu phụ đối với các hoạt động thuê ngoài có khả năng tác động lớn đến ngân hàng.

Trước đây, việc thuê ngoài thường chỉ giới hạn đối với một nhà cung cấp dịch vụ đơn lẻ đối với một chức năng cụ thể. Tuy nhiên, trong những năm gần đây, quan hệ thuê ngoài của ngân hàng đã tăng lên cả về qui mô lẫn mức độ phức tạp vì lý do trực tiếp liên quan đến sự phát triển về công nghệ thông tin và sự xuất hiện của nghiệp vụ ngân hàng điện tử. Ngoài sự phức tạp thì có một thực tế là các dịch vụ ngân hàng điện tử được thuê ngoài có thể được thầu phụ là các nhà cung cấp dịch vụ khác đảm nhận và/hoặc được thực hiện ở nước ngoài. Hơn nữa, vì các ứng dụng và dịch vụ ngân hàng điện tử đã phát triển ở mức độ cao về mặt công nghệ và đã trở nên quan trọng về mặt chiến lược nên một số chức năng hoạt động của nghiệp vụ ngân hàng điện tử sẽ phụ thuộc vào một số ít bạn hàng hoạt động chuyên biệt và cung cấp dịch vụ là bên thứ ba. Những vấn đề này có thể dẫn tới việc tập trung nhiều rủi ro hơn và cần có sự quan tâm của từng ngân hàng cũng như đối với toàn hệ thống.

Ngoài ra, các yếu tố này cũng cho thấy sự cần thiết phải đánh giá tổng thể và liên tục các quan hệ thuê ngoài và sự phụ thuộc bên ngoài, bao gồm những nguy cơ rủi ro tiềm ẩn đối với ngân hàng và khả năng giám sát quản trị rủi ro[15]. Việc giám sát của Hội đồng Quản trị và Ban (tổng) giám đốc đối với các quan hệ thuê ngoài và phụ thuộc vào bên thứ ba cần đặc biệt chú trọng nhằm đảm bảo rằng:

- Ngân hàng hiểu rõ các rủi ro liên quan đến việc ký kết hợp đồng thuê ngoài hoặc hợp đồng đối tác trong các hệ thống và ứng dụng ngân hàng điện tử.

[14] Bao gồm các biện pháp theo dõi hoạt động hệ thống, ghi nhận các cố gắng thâm nhập và báo cáo về sự kiện đột nhập an ninh nghiêm trọng

[15] Việc đánh giá như vậy cần tính đến mức độ kiểm soát được bên thứ ba thực hiện. Trong nhiều trường hợp, một cổ đông chính trong một công ty liên doanh thực hiện kiểm soát nhiều hơn so với quan hệ hợp đồng với một nhà cung cấp dịch vụ. Tuy nhiên, trong sự khác biệt ở trên thì không nên hiểu lầm rằng việc kiểm soát của cổ đông đối với công ty liên doanh hoặc đối tác là đủ, đặc biệt trong trường hợp công nghệ và dịch vụ cần thiết để thực hiện kinh doanh được cổ đông nhỏ hơn cung cấp. Sự khác biệt như vậy chỉ hữu dụng khi lập luận rằng việc đánh giá cần phải được thực hiện đối với từng trường hợp cụ thể.

- Đánh giá tính tuân thủ phù hợp về trình độ và khả năng tài chính của bất kỳ nhà cung cấp dịch vụ hoặc đối tác nào là bên thứ ba trước khi ký kết bất kỳ hợp đồng nào liên quan đến dịch vụ ngân hàng điện tử.

- Vấn đề trách nhiệm giải trình theo hợp đồng của tất cả các bên đối với vấn đề thuê ngoài[16] hoặc quan hệ đối tác phải được xác định rõ ràng. Ví dụ, trách nhiệm trong việc cung cấp và tiếp nhận thông tin từ nhà cung cấp dịch vụ cần phải được xác định rõ ràng.

- Tất cả các hệ thống và hoạt động ngân hàng điện tử được thuê ngoài phải tuân theo các chính sách về quản trị rủi ro, an ninh và tính riêng tư đáp ứng tiêu chuẩn của chính ngân hàng.

- Cần thực hiện kiểm toán nội bộ và/hoặc bên ngoài độc lập đối với các hoạt đông thuê ngoài ít nhất cũng theo đúng qui định như nội bộ tự thực hiện.

- Có kế hoạch dự phòng phù hợp đối với các hoạt động ngân hàng điện tử được thuê ngoài.

Phụ lục II đề cập bổ sung một số thông lệ tốt nhất đối với việc quản lý các hệ thống ngân hàng điện tử được thuê ngoài và sự phụ thuộc vào bên thứ ba.

B. Kiểm soát An ninh (Nguyên tắc 4-10)

Trong khi Hội đồng Quản trị có trách nhiệm đảm bảo xây dựng các qui trình kiểm soát an ninh phù hợp đối với nghiệp vụ ngân hàng điện tử thì nội dung của các qui trình này cần có sự quan tâm đặc biệt của Ban (tổng) giám đốc vì thách thức về an ninh ngày càng tăng trong nghiệp vụ ngân hàng điện tử[17]. Những vấn đề sau cần được xác định rõ:

- Xác thực

- Không khước từ

- Toàn vẹn dữ liệu và giao dịch

- Phân công nhiệm vụ

- Kiểm soát cấp phép

- Duy trì tập tin lưu giữ bằng chứng phục vụ đánh giá độc lập

- Bảo mật thông tin quan trọng của ngân hàng

[16] Bao gồm cả các nhà thầu phụ

[17] Ví dụ, khi Hội đồng Quản trị phụ thuộc vào nhà cung cấp dịch vụ ngân hàng điện tử là bên thứ ba thì cần đảm bảo rằng nhà cung cấp đã giải quyết các vấn đề một cách hợp lý hoặc ít nhất thì cũng đáp ứng các tiêu chuẩn của riêng ngân hàng.

Nguyên tắc 4: Ngân hàng cần triển khai những biện pháp cần thiết để chứng thực[18] danh tính và cấp phép cho khách hàng thực hiện giao dịch qua mạng Internet.

Trong nghiệp vụ ngân hàng cần phải xác nhận rằng sự liên hệ, giao dịch hoặc yêu cầu truy cập cụ thể là hợp lệ. Do đó, ngân hàng cần sử dụng các biện pháp đáng tin cậy để xác minh danh tính và cấp phép cho khách hàng mới cũng như chứng thực danh tính và cấp phép cho khách hàng cũ có nhu cầu thực hiện giao dịch điện tử.

Xác thực khách hàng trong quá trình truy gốc tài khoản là vấn đề quan trọng trong việc giảm rủi ro mất cắp danh tính, sử dụng tài khoản gian lận và rửa tiền. Việc ngân hàng không có khả năng chứng thực khách hàng một cách hiệu quả có thể dẫn tới trường hợp đối tượng bất hợp pháp có thể truy cập tài khoản ngân hàng điện tử và cuối cùng gây ra tổn thất về tài chính và uy tín do gian lận, rò rỉ thông tin mật hoặc hành động phạm tội.

Việc xây dựng và chứng thực danh tính cá nhân cũng như cấp phép truy cập vào hệ thống ngân hàng trong môi trường mở hoàn toàn có tính chất điện tử có thể là một nhiệm vụ khó khăn. Việc cấp phép cho người sử dụng hợp pháp có bị làm sai lệch bằng việc sử dụng một số kỹ thuật gọi là "tấn công lừa đảo"[19] Tin tặc trực tuyến cũng có thể giành quyền kiểm soát phiên giao dịch của một cá nhân đã được xác nhận là hợp pháp bằng việc sử dụng kỹ thuật "đánh hơi"[20] và thực hiện các hoạt động có tính chất phá hoại hoặc tội phạm. Ngoài ra, các qui trình kiểm soát chứng thực có thể bị vô hiệu hóa bằng việc thay đổi trong cơ sở dữ liệu chứng thực.

Do vậy, điều quan trọng là ngân hàng cần có chính sách và thủ tục chính thức để xác định các phương thức phù hợp nhằm đảm bảo rằng ngân hàng xác thực một cách đầy đủ danh tính và cấp phép xác nhận cá nhân, đại lý hoặc hệ thống[21] bằng cách sử dụng các biện pháp duy nhất và nếu thực tế cho phép thì vô hiệu hóa tất cả các đối tượng hoặc hệ thống không được cấp phép[22]. Ngân hàng có thể cung cấp cho chúng ta một số phương thức chứng thực như mã số nhận dạng cá nhân (PIN), mật khẩu, thẻ thông minh, các phương pháp chứng thực sinh trắc học và kỹ thuật số[23]. Các phương pháp này có thể sử dụng một hoặc nhiều yếu tố (có nghĩa là

[18] Khái niệm chứng thực được sử dụng trong Báo cáo này là các kỹ thuật, thủ tục và qui trình được sử dụng để kiểm chứng danh tính và cấp phép cho khách hàng. Xác định danh tính là các thủ tục, kỹ thuật và qui trình được sử dụng để xác định danh tính khách hàng khi mở tài khoản. Cấp phép là các thủ tục, kỹ thuật và qui trình được sử dụng để xác định rằng một khách hàng hoặc một nhân viên có thẩm quyền hợp pháp được truy cập vào tài khoản của ngân hàng hoặc có quyền thực hiện các giao dịch trên tài khoản đó.

[19] Tấn công lừa đảo là việc mạo danh một khách hàng hợp pháp bằng việc sử dụng số tài khoản, mật khẩu, mã số nhận diện cá nhân (PIN) và/hoặc địa chỉ thư điện tử.

[20] Đánh hơi là một thiết bị có khả năng nghe trộm trong quá trình giao dịch trên hệ thống viễn thông, thu giữ mật khẩu và dữ liệu đang lưu chuyển.

[21] Hệ thống bao gồm trang chủ của ngân hàng.

[22] Hệ thống phải đảm bảo đang giao dịch với một cá nhân, đại lý hoặc hệ thống đã được chứng thực và phải có một cơ sở dữ liệu chứng thực hoạt động hiệu quả.

[23] Một ngân hàng có thể phát hành một giấy chứng nhận số sử dụng cơ sở hạ tầng khóa công khai (PKI) cho khách hàng nhằm đảm bảo an ninh cho giao dịch với ngân hàng. Giấy chứng số và cơ sở hạ tấng khóa công khai được thảo luận cụ thể hơn trong Nguyên tắc 5.

sử dụng cả hai công nghệ là mật khẩu và sinh trắc học[24] để chứng thực). Phương pháp chứng thực sử dụng nhiều yếu tố nói chung có mức độ bảo mật cao hơn.

Ngân hàng cần xác định phương thức chứng thực cần sử dụng dựa trên việc đánh giá rủi ro của Ban (tổng) giám đốc ngân hàng xuất phát từ hệ thống ngân hàng điện tử nói chung hoặc từ các tiểu cấu phần khác. Việc phân tích rủi ro này cần đánh giá khả năng giao dịch[25] của hệ thống ngân hàng điện tử (có nghĩa là chuyển tiền, thanh toán hóa đơn, truy nguyên nguồn gốc khoản vay, hợp nhất tài khoản v.v), mức độ nhạy cảm và giá trị của dữ liệu ngân hàng điện tử đang được lưu trữ và mức độ dễ sử dụng của phương pháp chứng thực đối với khách hàng.

Các qui trình xác định danh tính và chứng thực khách hàng tinh vi trong môi trường hệ thống giao dịch vượt phạm vi biên giới là đặc biệt quan trọng trong bối cảnh có thêm khó khăn nảy sinh từ các giao dịch điện tử giữa các khách hàng nằm ngoài phạm vi biên giới, bao gồm mức độ rủi ro cao hơn trong việc xác định danh tính và mức độ khó khăn cao hơn trong việc kiểm tra mức độ tin cậy đối với khách hàng tiềm năng.

Trong quá trình thay đổi của các phương pháp chứng thực, ngân hàng được khuyến khích theo dõi và áp dụng các thông lệ tốt nhất trong lĩnh vực này nhằm đảm bảo rằng:

- Cơ sở dữ liệu chứng thực cấp phép truy cập vào tài khoản ngân hàng điện tử cho khách hàng hoặc các hệ thống nhạy cảm phải được bảo vệ chống lại giả mạo và bị thay đổi. Bất kỳ sự giả mạo nào như vậy cần phải được phát hiện và có bằng chứng kiểm soát ghi lại.

- Ngoài ra, việc xóa bỏ hoặc thay đổi đối tượng, đại lý hoặc hệ thống trong cơ sở dữ liệu chứng thực cần phải được cấp phép đầy đủ bởi một nguồn được chứng thực[26].

- Cần có các biện pháp phù hợp nhằm kiểm soát kết nối hệ thống ngân hàng điện tử để làm sao các bên thứ ba không thể thay đổi các khách hàng hiện thời.

- Các phiên giao dịch ngân hàng điện tử được chứng thực vẫn an toàn trong toàn bộ thời gian của phiên giao dịch hoặc trong trường hợp có sai sót an ninh trong phiên làm việc thì cần yêu cầu chứng thực lại.

Nguyên tắc 5: Ngân hàng cần sử dụng các phương pháp chứng thực giao dịch nhằm nâng cao khả năng không khước từ và xây dựng các biện pháp giải trình đối với các giao dịch ngân hàng điện tử.

Không khước từ bao gồm việc tạo ra bằng chứng gốc hoặc chuyển giao thông tin điện tử để bảo vệ người gửi trong trường hợp bị người nhận cố tình từ chối đã tiếp nhận dữ liệu hoặc bảo vệ người nhận trong trường hợp bị người gửi cố tình từ chối không gửi dữ liệu. Rủi ro

[24] Công nghệ sinh trắc học là việc đánh giá tự động đặc điểm hành vi hoặc sinh lý học được sử dụng để xác định và/hoặc để chứng thực một đối tượng. Các hình thức công nghệ sinh trắc học bao gồm việc quét khuôn mặt, vân tay, mống mắt, tròng mắt, bàn tay, chữ ký, giọng nói và tốc độ sử dụng bàn phím. Hệ thống nhận dạng sinh trắc học là một phương pháp chứng thực rất hiệu quả, nhưng triển khai phức tạp hơn so với các phương thức nhận dạng/chứng thực khác.

[25] Các biện pháp chứng thực hiệu quả cũng làm giảm rủi ro không khước từ, trong đó một người sử dụng hợp pháp sau đó từ chối việc mình đã thực hiện một giao dịch nào đó (tham khảo Nguyên tắc 5).

[26] Trong một số trường hợp, nguồn được chứng thực có thể là một nguồn điện tử.

của khước từ giao dịch vốn đã là một vấn đề trong các giao dịch thông thường như thẻ tín dụng hoặc các giao dịch chứng khoán. Tuy nhiên, rủi ro này trong dịch vụ ngân hàng điện tử càng trở nên trầm trọng hơn vì những khó khăn trong việc chứng thực khẳng định danh tính và quyền hạn của các bên trong giao dịch, khả năng thay đổi hoặc bắt cóc các giao dịch điện tử và khả năng những người sử dụng dịch vụ ngân hàng điện tử tuyên bố rằng những giao dịch đó đã bị thay đổi nhằm mục đích gian lận.

Để giải quyết vấn đề này, ngân hàng cần triển khai phù hợp với tính chất và loại hình giao dịch ngân hàng điện tử để đảm bảo rằng:

- Hệ thống ngân hàng điện tử được thiết kế nhằm giảm mức độ người sử dụng được cấp phép thực hiện các giao dịch không có ý định thực hiện và khách hàng hiểu rõ các rủi ro liên quan đến bất kỳ giao dịch nào họ thực hiện.

- Tất cả các bên tham gia giao dịch đều được chứng thực được sử dụng và cần duy trì kiểm soát đối với kênh giao tiếp đã được chứng thực.

- Dữ liệu giao dịch tài chính cần được bảo vệ chống lại thay đổi và cần phát hiện bất kỳ sự thay đổi nào xảy ra.

Tổ chức ngân hàng đã bắt đầu sử dụng các kỹ thuật khác nhau nhằm thiết kế cơ chế không khước từ và đảm bảo tính chất bảo mật và toàn vẹn của các giao dịch ngân hàng điện tử như chứng nhận số sử dụng cơ sở hạ tầng khóa công khai (PKI)[27]. Một ngân hàng có thể phát hành một chứng nhận số cho một khách hàng hoặc một đối tác để cho phép duy nhất họ có thể được nhận dạng/chứng thực và giảm rủi ro không khước từ trong thực hiện giao dịch. Mặc dầu tại một số quốc gia, một số văn bản pháp lý đã qui định quyền của khách hàng trong việc từ chối thực hiện giao dịch nhưng tại một số quốc gia khác thì luật lệ đã được thông qua trong đó qui định rằng chữ ký điện tử là có hiệu lực pháp lý. Khi công nghệ tiếp tục phát triển thì các kỹ thuật như vậy ngày càng có xu hướng được chấp nhận rộng rãi hơn.

Nguyên tắc 6: Ngân hàng cần đảm bảo có những biện pháp phù hợp trong việc phân công nhiệm vụ một cách hợp lý trong hệ thống ngân hàng điện tử, cơ sở dữ liệu và ứng dụng.

Phân công nhiệm vụ là biện pháp kiểm soát nội bộ cơ bản được thiết kế nhằm giảm rủi ro gian lận trong qui trình tác nghiệp và hệ thống cũng như đảm bảo rằng các giao dịch và tài sản của công ty được xác nhận, lưu hồ sơ và bảo vệ một cách phù hợp. Việc phân công nhiệm vụ là quan trọng nhằm đảm bảo tính chính xác và toàn vẹn của dữ liệu và được sử dụng ngăn ngừa một đối tượng có hành động gian lận. Nếu nhiệm vụ đã được phân công phù hợp thì gian lận chỉ có thể xảy ra thông qua câu kết thông đồng.

[27] Trong cơ sở hạ tầng khóa công khai (PKI), mỗi bên sẽ có một cặp khóa cá nhân/công khai. Khóa cá nhân được giữ bí mật chỉ dành cho một người sử dụng. Tất cả các bên đều sử dụng khóa công khai. Khóa cá nhân tạo ra một chữ ký điện tử trên tài liệu và cặp khóa này được thiết kế để thông điệp được mã hóa bằng khóa cá nhân chỉ có thể đọc được khi sử dụng khóa còn lại. Một ngân hàng có thể đóng vai trò là một cơ quan cấp chứng nhận (CA) hoặc dựa vào một bên thứ ba có thể tin tưởng để cấp giấy chứng nhận số cho đối tượng hoặc một thực thể. Tuy nhiên, nếu một ngân hàng chỉ dựa vào giấy chứng nhận số do bên thứ ba cấp thì ngân hàng cũng cần phải xác nhận rằng cơ quan đó, khi cấp giấy chứng nhận là đã sử dụng kỹ thuật chứng thực với mức độ tương tự mà ngân hàng đã sử dụng để chứng thực đối tượng đó. Hạn chế của hệ thống chứng thực sử dụng khóa công khai này chủ yếu là mức độ phức tạp hơn khi triển khai.

Dịch vụ ngân hàng điện tử có thể sẽ làm điều chỉnh phương thức phân công trách nhiệm được thực hiện và duy trì vì các giao dịch được thực hiện trên hệ thống điện tử mà tại đó danh tính có thể bị che dấu hoặc giả mạo. Ngoài ra, trong nhiều trường hợp, các chức năng tác nghiệp và giao dịch ngày càng trở nên cô đọng và tích hợp trong các ứng dụng ngân hàng điện tử. Do đó, những biện pháp kiểm soát truyền thống để duy trì sự phân công trách nhiệm cần phải được đánh giá lại và áp dụng để đảm bảo duy trì mức độ kiểm soát phù hợp. Vì truy cập vào các cơ sở dữ liệu có mức độ bảo mật kém ngày càng trở nên dễ dàng hơn từ các hệ thống nội bộ và bên ngoài nên cần phải có thủ tục nhận dạng và cấp phép chặt chẽ, an toàn và kiến trúc hiệu quả đối với các qui trình xử lý thẳng theo luồng và có các tập tin lưu giữ bằng chứng phục vụ kiểm tra độc lập.

Những thông lệ chung được sử dụng để xây dựng và duy trì phân công nhiệm vụ trong môi trường ngân hàng điện tử bao gồm:

- Cần thiết kế các qui trình giao dịch và hệ thống nhằm đảm bảo rằng không nhân viên hoặc nhà cung cấp dịch vụ được thuê ngoài nào có thể nhập, cấp phép và hoàn tất một giao dịch.

- Cần duy trì sự tách biệt giữa các bộ phận sử dụng dữ liệu tĩnh (bao gồm nội dung trang web) và bộ phận chịu trách nhiệm xác thực tính toàn vẹn của dữ liệu.

- Cần thử nghiệm các hệ thống ngân hàng điện tử để đảm bảo rằng không thể bỏ qua việc phân công nhiệm vụ.

- Cần duy trì việc phân công nhiệm vụ giữa các hệ thống phát triển và quản lý ngân hàng điện tử[28].

Nguyên tắc 7: Ngân hàng cần đảm bảo cần kiểm soát cấp phép phù hợp và đặc quyền truy cập trong hệ thống, cơ sở dữ liệu và ứng dụng ngân hàng điện tử.

Để duy trì việc phân công trách nhiệm, ngân hàng cần kiểm soát chặt chẽ việc cấp phép và đặc quyền truy cập. Việc không có biện pháp kiểm soát cấp phép phù hợp có thể giúp cho đối tượng thay đổi quyền hạn, làm cho việc phân công trách nhiệm mất tác dụng và có thể truy cập vào hệ thống, cơ sở dữ liệu hoặc ứng dụng ngân hàng điện tử mà đối tượng đó không có quyền hạn truy cập.

Trong hệ thống ngân hàng điện tử, quyền cấp phép và truy cập được thực hiện tập trung hoặc phân tán trong một ngân hàng và thường được lưu trữ trong cơ sở dữ liệu. Do đó, điều quan trọng là phải bảo vệ các cơ sở dữ liệu này không bị thay đổi hoặc phá hỏng, phục vụ cho việc kiểm soát cấp phép hiệu quả.

Phụ lục III đề cập một số thông lệ tốt nhất nhằm giúp xây dựng các biện pháp kiểm soát phù hợp đối với quyền cấp phép và truy cập vào hệ thống, cơ sở dữ liệu và ứng dụng ngân hàng điện tử.

Nguyên tắc 8: Ngân hàng cần đảm bảo có các biện pháp phù hợp nhằm bảo vệ tính toàn vẹn của các giao dịch, hồ sơ và thông tin ngân hàng điện tử.

[28] Hoặc cần có các biện pháp kiềm chế thay thế.

Toàn vẹn dữ liệu là sự đảm bảo rằng các thông tin đang lưu chuyển hoặc lưu trữ không bị thay đổi mà không được phép. Sự thất bại trong duy trì tính toàn vẹn dữ liệu trong các giao dịch, hồ sơ và thông tin sẽ gây ra tổn thất tài chính cho ngân hàng cũng như gây ra rủi ro về uy tín và pháp lý.

Tính chất của qui trình xử lý thẳng theo luồng trong ngân hàng điện tử có thể gây khó khăn trong việc sớm phát hiện ra lỗi lập trình hoặc các hoạt động gian lận. Do đó, điều quan trọng là ngân hàng cần triển khai xử lý thẳng theo luồng thế nào để đảm bảo an toàn và hiệu quả cũng như đảm bảo tính toàn vẹn của dữ liệu.

Vì ngân hàng điện tử được giao dịch trên mạng công cộng, do đó, các giao dịch có nguy cơ bị phá hủy dữ liệu, gian lận và thay đổi hồ sơ. Do đó, ngân hàng cần đảm bảo có các biện pháp phù hợp để đảm bảo tính chính xác, đầy đủ và tin cậy của các giao dịch ngân hàng điện tử, hồ sơ và thông tin được lưu chuyển qua mạng Internet, cơ sở dữ liệu tại chỗ hoặc nội bộ của ngân hàng, hoặc được lưu chuyển/lưu trữ tại nhà cung cấp dịch vụ bên thứ ba thay mặt ngân hàng[29]. Các thông lệ chung được sử dụng để duy trì toàn vẹn dữ liệu trong môi trường ngân hàng điện tử bao gồm:

- Giao dịch ngân hàng điện tử cần được thực hiện làm sao để không bị thay đổi trong toàn bộ qui trình xử lý.

- Hồ sơ ngân hàng điện tử cần được lưu trữ, truy cập và sửa đổi thế nào để không bị thay đổi.

- Qui trình giao dịch ngân hàng điện tử và lưu giữ hồ sơ cần được thiết kế bảo vệ như thế nào để có thể phát hiện ra các thay đổi bất hợp pháp.

- Cần có chính sách kiểm soát thay đổi phù hợp, bao gồm qui trình theo dõi và kiểm tra nhằm bảo vệ chống lại bất kỳ thay đổi nào trong hệ thống ngân hàng điện tử có tác động vô tình hay hữu ý đến các biện pháp kiểm soát mức độ tin cậy của dữ liệu.

- Bất kỳ việc thay đổi nào liên quan đến các giao dịch hoặc hồ sơ ngân hàng điện tử cần bị phát hiện trong quá trình thực hiện chức năng xử lý giao dịch, theo dõi và lưu giữ hồ sơ.

Nguyên tắc 9: Ngân hàng cần đảm bảo phải lưu giữ đầy đủ tập tin lưu giữ bằng chứng phục vụ đánh giá độc lập đối với tất cả các giao dịch ngân hàng điện tử.

Việc sử dụng mạng Internet để cung cấp các dịch vụ tài chính càng gây nhiều khó khăn trong việc áp dụng và thực thi kiểm soát nội bộ và duy trì đầy đủ các tập tin lưu giữ bằng chứng phục vụ đánh giá độc lập nếu các biện pháp này không được áp dụng trong môi trường ngân hàng điện tử. Ngân hàng không chỉ gặp khó khăn trong vấn đề phải có những biện pháp kiểm soát nội bộ hữu hiệu trong môi trường tự động hóa cao mà còn liên quan đến việc làm sao các biện pháp kiểm soát đó có thể được kiểm toán độc lập, đặc biệt trong các tình huống và ứng dụng ngân hàng điện tử quan trọng.

[29] Ngân hàng cần đảm bảo hệ thống lưu giữ hồ sơ được thiết kế và cài đặt phù hợp cho phép khôi phục các hồ sơ này trong trường hợp bị thay đổi hoặc phá hủy.

Môi trường kiểm soát nội bộ của ngân hàng có thể bị suy yếu nếu không có khả năng duy trì đầy đủ các tập tin lưu giữ bằng chứng phục vụ kiểm toán đối với các hoạt động ngân hàng điện tử. Điều này là do hầu hết, nếu không phải là tất cả các hồ sơ và bằng chứng hỗ trợ cho giao dịch điện tử đều ở dạng điện tử. Để quyết định được việc lưu trữ đầy đủ các tập tin lưu giữ bằng chứng phục vụ kiểm toán, các loại hình giao dịch ngân hàng điện tử sau đây cần được xem xét:

- Việc mở, sửa đổi và đóng tài khoản của một khách hàng.
- Bất kỳ giao dịch nào có hậu quả về tài chính.
- Bất kỳ việc cấp phép nào cho một khách hàng vượt hạn mức.
- Bất kỳ việc cấp quyền, sửa đổi hoặc rút quyền truy cập hệ thống.

Phụ lục IV đề cập một số thông lệ tốt nhất nhằm giúp đảm bảo rằng cần lưu trữ bằng chứng rõ ràng phục vụ kiểm toán đối với các giao dịch ngân hàng điện tử.

Nguyên tắc 10: Ngân hàng cần có biện pháp phù hợp trong việc bảo toàn tính bảo mật của thông tin ngân hàng điện tử quan trọng. Các biện pháp sử dụng để bảo toàn tính bảo mật cần tương xứng với mức độ nhạy cảm của các thông tin được lưu chuyển và/hoặc lưu trữ tại các cơ sở dữ liệu.

Bảo mật là việc đảm bảo rằng thông tin quan trọng vẫn giữ được tính riêng tư đối với ngân hàng và không bị đối tượng bất hợp pháp làm lộ hoặc sử dụng. Việc sử dụng sai mục đích hoặc công bố dữ liệu bất hợp pháp sẽ gây rủi ro pháp lý và rủi ro uy tín cho ngân hàng. Dịch vụ ngân hàng điện tử đã tạo thêm nhiều khó khăn về an ninh cho ngân hàng vì điều này đã làm tăng nguy cơ rủi ro về dữ liệu khi được lưu chuyển trên mạng công cộng hoặc lưu trữ tại cơ sở dữ liệu có thể bị truy cập bởi người hoặc đối tượng bất hợp pháp hoặc sử dụng theo cách mà khách hàng cung cấp thông tin không mong muốn. Ngoài ra, việc sử dụng nhiều dịch vụ của nhà cung cấp càng làm tăng rủi ro bị lộ thông tin cho bên thứ ba.

Để giải quyết các vấn đề khó khăn trong việc đảm bảo tính bảo mật về thông tin ngân hàng điện tử quan trọng, ngân hàng cần đảm bảo rằng:

- Chỉ có người, đại lý hoặc hệ thống có thẩm quyền và được cấp phép đầy đủ mới có thể truy cập vào tất cả hồ sơ hoặc dữ liệu bảo mật của ngân hàng.
- Tất cả dữ liệu bảo mật của ngân hàng được lưu giữ và bảo vệ một cách an toàn chống lại việc tiếp cận và sửa đổi bất hợp pháp trong quá trình lưu chuyển trên hệ thống nội bộ, hệ thống riêng hoặc công cộng.
- Tiêu chuẩn, biện pháp kiểm soát sử dụng và bảo vệ dữ liệu của ngân hàng cần phải được áp dụng khi bên thứ ba truy cập vào dữ liệu thông qua quan hệ thuê ngoài.
- Tất cả mọi truy cập vào hệ thống dữ liệu hạn chế truy cập đều phải được ghi lại và có biện pháp kiểm soát để đảm bảo rằng các tập tin ghi lại thông tin truy cập không bị thay đổi.

C. Quản trị Rủi to Pháp lý và Rủi ro Uy tín (Nguyên tắc 11-14)

Luật pháp và qui chế liên quan đến bảo vệ khách hàng và tính riêng tư là khác nhau giữa các quốc gia. Tuy nhiên, ngân hàng nói chung có trách nhiệm rõ ràng trong việc cung cấp cho khách hàng một mức độ bảo vệ phù hợp liên quan đến việc công bố thông tin, bảo vệ dữ liệu khách hàng và cung cấp dịch vụ liên tục tương đương với mức độ mà khách hàng sử dụng các dịch vụ ngân hàng qua kênh cung cấp dịch vụ ngân hàng truyền thống.

Nguyên tắc 11: Ngân hàng cần đảm bảo cung cấp đầy đủ thông tin trên trang chủ để cho phép các khách hàng tiềm năng có đủ thông tin để kết luận về danh tính và trạng thái pháp lý của ngân hàng trước khi tiến hành giao dịch ngân hàng điện tử.

Nhằm giảm thiểu rủi ro pháp lý và rủi ro uy tín liên quan đến các hoạt động ngân hàng điện tử được cung cấp trong và ngoài nước, ngân hàng cần đảm bảo cung cấp đầy đủ thông tin trên trang chủ để cho phép khách hàng có đủ thông tin kết luận về danh tính và trạng thái pháp lý của ngân hàng trước khi tiến hành giao dịch ngân hàng điện tử..

Ví dụ về thông tin mà ngân hàng có thể cung cấp trên trang chủ bao gồm:

- Tên của ngân hàng và địa chỉ của hội sở (và văn phòng tại địa phương nếu cần thiết).
- Danh tính của (các) cơ quan giám sát ngân hàng chính, chịu trách nhiệm giám sát hội sở ngân hàng.
- Làm thế nào khách hàng có thể liên hệ với trung tâm dịch vụ khách hàng của ngân hàng về vấn đề dịch vụ, khiếu nại, nghi ngờ sử dụng tài khoản sai mục đích, v.v.
- Làm thế nào khách hàng có thể truy cập và sử dụng chương trình thanh tra hoặc các chương trình khiếu nại.
- Làm thế nào khách hàng có thể truy cập thông tin về đền bù quốc gia đang áp dụng hoặc bảo đảm tiền gửi và mức độ bảo vệ mà họ được hưởng (hoặc các đường dẫn đến trang web cung cấp các thông tin đó).
- Thông tin cần thiết khác hoặc thông tin buộc phải đăng tải theo qui định pháp luật[30].

Nguyên tắc 12: Ngân hàng cần có biện pháp đảm bảo tuân thủ qui định của luật pháp về tính riêng tư của khách hàng, theo đó ngân hàng cung cấp các dịch vụ và sản phẩm ngân hàng điện tử.

Duy trì sự riêng tư của thông tin khách hàng là một trách nhiệm quan trọng của ngân hàng. Việc tiết lộ sai mục đích hoặc không được phép về dữ liệu bảo mật của khách hàng sẽ gây ra rủi ro về pháp lý và uy tín đối với ngân hàng. Nhằm giải quyết các vấn đề liên quan tới việc bảo toàn sự riêng tư về thông tin khách hàng, ngân hàng cần đảm bảo rằng:

- Chính sách và tiêu chuẩn của ngân hàng về sự riêng tư của khách hàng là dựa trên và tuân thủ tất cả các qui định về sự riêng tư và luật pháp áp dụng tại quốc gia mà ngân hàng đang cung cấp dịch vụ và sản phẩm ngân hàng điện tử.

[30] Ví dụ, ngân hàng không muốn cung cấp thông tin về quốc gia mà tại đó ngân hàng có ý định cung cấp dịch vụ ngân hàng điện tử hoặc ngược lại, thông tin về quốc gia mà ngân hàng không muốn cung cấp dịch vụ đó.

- Khách hàng biết về chính sách riêng tư của ngân hàng và các vấn đề liên quan đến riêng tư khác trong việc sử dụng các dịch vụ và sản phẩm ngân hàng điện tử.

- Khách hàng có thể từ chối ("gạch bỏ") không cho phép ngân hàng chia sẻ với bên thứ ba vì các mục đích tiếp thị đối với bất kỳ thông tin nào liên quan đến nhu cầu cá nhân, lĩnh vực quan tâm, tình hình tài chính hoặc hoạt động ngân hàng của khách hàng.

- Không được sử dụng dữ liệu khách hàng cho các mục đích khác trừ phi được phép hoặc ngoài các mục đích mà khách hàng cho phép sử dụng[31].

- Bên thứ ba cần phải đáp ứng các tiêu chuẩn của ngân hàng về dữ liệu khách hàng khi truy cập dữ liệu khách hàng thông qua các quan hệ thuê ngoài.

Phụ lục V mô tả một số thông lệ tốt nhất giúp duy trì sự riêng tư của thông tin khách hàng sử dụng dịch vụ ngân hàng điện tử.

Nguyên tắc 13: Ngân hàng cần có năng lực phù hợp, qui trình kế hoạch dự phòng và duy trì kinh doanh giúp đảm bảo sự hoạt động liên tục của hệ thống và dịch vụ ngân hàng điện tử.

Để bảo vệ ngân hàng trước các rủi ro kinh doanh, rủi ro pháp lý và rủi ro uy tín, dịch vụ ngân hàng điện tử cần được cung cấp trên cơ sở nhất quán và kịp thời theo kỳ vọng của khách hàng. Để thực hiện được điều này, ngân hàng cần có khả năng cung cấp dịch vụ ngân hàng điện tử cho người sử dụng đầu cuối từ nguồn sơ cấp (có nghĩa là các ứng dụng và hệ thống trong nội bộ ngân hàng) hoặc nguồn thứ cấp (có nghĩa là các ứng dụng và hệ thống của nhà cung cấp dịch vụ). Việc duy trì hoạt động liên tục cũng phụ thuộc vào khả năng của các hệ thống dự phòng nhằm phòng tránh các cuộc tấn công từ chối dịch vụ hoặc các sự kiện khác dẫn tới việc gián đoạn kinh doanh.

Vấn đề duy trì khả năng hoạt động liên tục của hệ thống và ứng dụng ngân hàng điện tử có thể là to lớn trong trường hợp có nhu cầu giao dịch cao, đặc biệt trong các giai đoạn cao điểm. Ngoài ra, kỳ vọng ở mức độ cao của khách hàng liên quan tới thời gian chu kỳ xử lý giao dịch ngắn và khả năng cung cấp dịch vụ liên tục (24 X 7) cũng nâng tầm quan trọng của công tác xây dựng kế hoạch dự phòng, khả năng hoạt động liên tục và kế hoạch duy trì kinh doanh. Để cung cấp các dịch vụ ngân hàng điện tử một cách liên tục theo đúng kỳ vọng của khách hàng, ngân hàng cần đảm bảo rằng:

- Phân tích năng lực hệ thống ngân hàng điện tử hiện tại và khả năng nâng cấp trong tương lai dựa trên sự thay đổi tổng thể trên thị trường và tỷ lệ khách hàng dự kiến chấp nhận sử dụng dịch vụ và sản phẩm ngân hàng điện tử[32].

[31] Tại một số quốc gia, luật pháp và qui định không bắt buộc ngân hàng phải có sự đồng ý của khách hàng trong việc sử dụng dữ liệu của họ cho mục đích nội bộ. Tuy nhiên, luật có thể buộc ngân hàng cho khách hàng lựa chọn quyền từ chối cho phép ngân hàng chia sẻ thông tin đó với bên thứ ba hoặc bên phối thuộc. Tại các quốc gia khác, ngân hàng có quyền không cho ngân hàng sử dụng các thông tin của họ cho mục đích nội bộ hoặc bên ngoài.

[32] Cần liên tục đánh giá năng lực hiện tại và tương lai của hệ thống cung cấp dịch vụ ngân hàng điện tử quan trọng.

- Xây dựng khả năng xử lý giao dịch ngân hàng điện tử dự kiến, kiểm tra trong trường hợp chịu sức ép và cần đánh giá định kỳ.

- Có kế hoạch dự phòng và duy trì kinh doanh hợp lý đối với các hệ thống cung cấp và xử lý ngân hàng điện tử quan trọng và được kiểm tra thường xuyên.

Phụ lục VI đề cập một số thông lệ tốt nhất liên quan đến năng lực, kế hoạch dự phòng và duy trì kinh doanh.

Nguyên tắc 14: Ngân hàng cần xây dựng các kế hoạch xử lý tình huống phù hợp nhằm quản lý, ngăn chặn và giảm thiểu các vấn đề xảy ra từ các sự kiện bất ngờ, bao gồm các cuộc tấn công từ bên trong và bên ngoài có thể làm ảnh hưởng đến khả năng cung cấp hệ thống và dịch vụ ngân hàng điện tử.

Cơ chế xử lý tình huống hiệu quả là quan trọng trong việc giảm thiểu rủi ro tác nghiệp, rủi ro pháp lý và rủi ro uy tín nảy sinh từ các sự kiện bất ngờ như các cuộc tấn công từ bên trong và bên ngoài có thể làm ảnh hưởng đến việc cung cấp hệ thống và dịch vụ ngân hàng điện tử. Ngân hàng cần xây dựng các kế hoạch xử lý tình huống phù hợp bao gồm các chiến lược truyền thông nhằm đảm bảo duy trì kinh doanh, kiểm soát rủi ro uy tín và hạn chế trách nhiệm liên quan đến việc gián đoạn dịch vụ ngân hàng điện tử, bao gồm cả các vấn đề xuất phát từ các hệ thống và nghiệp vụ đã thuê ngoài.

Nhằm đảm bảo đối phó với các sự kiện bất thường xảy ra, ngân hàng cần xây dựng:

- Kế hoạch xử lý tình huống nhằm giải quyết việc phục hồi các hệ thống và dịch vụ ngân hàng điện tử trong mọi tình huống, nghiệp vụ kinh doanh và địa điểm địa lý. Báo cáo phân tích tình huống cần tính tới khả năng xảy ra rủi ro và tác động tới ngân hàng. Hệ thống ngân hàng điện tử do bên thứ ba cung cấp dịch vụ nhận triển khai là một phần không thể tách rời của các kế hoạch này.

- Cơ chế xác định một sự kiện hoặc khủng hoảng ngay khi xảy ra, đánh giá mức độ và kiểm soát rủi ro uy tín có liên quan đến bất kỳ sự gián đoạn dịch vụ nào[33].

- Một chiến lược truyền thông nhằm giải quyết hợp lý các vấn đề về thị trường bên ngoài và báo giới có thể nảy sinh trong trường hợp đột nhập an ninh, tấn công trực tuyến và/hoặc trục trặc trong hệ thống ngân hàng điện tử.

- Một qui trình cảnh báo rõ ràng cho cơ quan luật pháp phù hợp trong trường hợp bị đột nhập an ninh hoặc gián đoạn dịch vụ.

- Nhóm xử lý tình huống có thẩm quyền hoạt động trong trường hợp khẩn cấp và được đào tạo đầy đủ trong việc phát hiện tình huống /hệ thống xử lý và hiểu rõ tầm quan trọng của các kết quả có liên quan.

- Một chuỗi mệnh lệnh rõ ràng áp dụng cho cả các hoạt động nội bộ và thuê ngoài, nhằm đảm bảo triển khai hành động khẩn trương đối với tính chất quan trọng của sự

[33] Theo dõi bộ phận hỗ trợ kỹ thuật và các hoạt động hỗ trợ khách hàng và việc đánh giá thường xuyên việc khiếu nại của khách hàng có thể giúp xác định các lỗ hổng bằng việc phát hiện thông tin và báo cáo thông qua các biện pháp kiểm soát an ninh đã được thiết lập và các hoạt động đột nhập thực tế.

kiện. Ngoài ra, cần xây dựng các thủ tục liên hệ nội bộ và với các cấp quản lý và bao gồm việc thông báo cho Hội đồng Quản trị trong trường hợp cần thiết.

- Một qui trình đảm bảo tất cả các bên có liên quan, bao gồm khách hàng tại ngân hàng, đối tác và khu vực truyền thông được thông báo kịp thời trong trường hợp có sự gián đoạn dịch vụ ngân hàng điện tử có tính chất nghiêm trọng và các hoạt động phục hồi kinh doanh.

- Một qui trình thu thập và bảo quản bằng chứng pháp lý phục vụ cho việc đánh giá phân tích sau khi xảy ra bất kỳ sự kiện nào liên quan đến ngân hàng điện tử cũng như giúp khởi tố những kẻ tấn công.

Phụ lục I

THÔNG LỆ KIỂM SOÁT AN NINH HIỆU QUẢ TRONG NGÂN HÀNG ĐIỆN TỬ

1. Cần xây dựng và duy trì mức độ an ninh và các đặc quyền cấp phép đặc biệt phân bổ cho tất cả người sử dụng trong hệ thống và ứng dụng ngân hàng điện tử, bao gồm tất cả các khách hàng, người sử dụng trong nội bộ ngân hàng và các nhà cung cấp dịch vụ thuê ngoài. Các biện pháp kiểm soát truy cập hợp lý cũng cần được thiết kế để hỗ trợ việc phân công nhiệm vụ phù hợp[34].

2. Dữ liệu và hệ thống ngân hàng điện tử cần được phân loại tùy theo mức độ nhạy cảm, tầm quan trọng và được bảo vệ thích hợp. Các cơ chế phù hợp như mã hóa, kiểm soát truy cập và kế hoạch phục hồi dữ liệu cần được sử dụng nhằm bảo vệ tất cả các hệ thống ngân hàng điện tử, máy chủ, cơ sở dữ liệu và các ứng dụng có độ nhạy cảm và nguy cơ rủi ro cao.

3. Cần giảm thiểu lưu trữ các dữ liệu nhạy cảm hoặc có nguy cơ rủi ro cao trên các hệ thống máy để bàn và máy xách tay, cần bảo vệ các dữ liệu một cách hợp lý bằng kỹ thuật mã hóa, kiểm soát truy cập và kế hoạch phục hồi dữ liệu.

4. Cần có các biện pháp kiểm soát ở mức vật lý nhằm loại trừ truy cập bất hợp pháp[35] vào tất cả các hệ thống, máy chủ, cơ sở dữ liệu và ứng dụng ngân hàng điện tử quan trọng.

5. Cần áp dụng các kỹ thuật phù hợp nhằm loại trừ các mối đe dọa từ bên ngoài đối với các hệ thống ngân hàng điện tử, bao gồm việc sử dụng:

   - Phần mềm quét virus tại tất cả các điểm truy cập vào hệ thống quan trọng (v.d máy chủ truy cập từ xa, máy chủ proxy thư điện tử) và trên từng hệ thống máy để bàn.

   - Phần mềm phát hiện đột nhập và các công cụ đánh giá an ninh khác nhằm định kỳ kiểm tra thăm dò mạng, máy chủ và tường lửa nhằm phát hiện các yếu điểm và/hoặc vi phạm các chính sách và kiểm soát an ninh.

   - Kiểm tra xâm nhập các hệ thống nội bộ và bên ngoài.

6. Cần áp dụng qui trình đánh giá an ninh chặt chẽ đối với tất cả các cán bộ công nhân viên và các nhà cung cấp dịch vụ đang nắm giữ các vị trí nhạy cảm.

[34] Các định nghĩa về an ninh và các tiêu chuẩn chất lượng và việc phụ thuộc vào chương trình xác thực có thể do ngân hàng tự xây dựng hoặc xây dựng tiêu chuẩn (có nghĩa là trong ngành công nghiệp ngân hàng quốc gia nâng cao và duy trì mức độ an ninh của các hoạt động ngân hàng). Các ngân hàng cũng có thể lựa chọn xây dựng quyền truy cập theo phương thức tập trung hoặc phân tán. Ví dụ, có thể chỉ có duy nhất một bộ phận cấp phép chịu trách nhiệm trao quyền truy cập cho các đối tượng, nhóm hoặc chức năng trong một ngân hàng, hoặc có thể có một số bộ phận cấp phép được thành lập nhằm giải quyết các nhu cầu đa dạng trong các nghiệp vụ kinh doanh chủ yếu.

[35] Điều này bao gồm các biện pháp kiểm soát bảo vệ chống lại truy cập bất hợp pháp của các nhóm đối tượng bên ngoài như khách vãng lai, nhà thầu hoặc kỹ thuật viên có thể tiếp cận những khu vực làm việc mặc dù họ không trực tiếp liên quan đến dịch vụ ngân hàng điện tử.

Phụ lục II

THÔNG LỆ TỐT NHẤT TRONG QUẢN LÝ THUÊ NGOÀI DỊCH VỤ VÀ HỆ THỐNG NGÂN HÀNG ĐIỆN TỬ

1. Các ngân hàng cần áp dụng các qui trình phù hợp trong việc đánh giá quyết định thuê ngoài dịch vụ và hệ thống ngân hàng điện tử.

   - Ban (tổng) giám đốc ngân hàng cần xác định rõ mục tiêu chiến lược, lợi ích và chi phí liên quan đến các hợp đồng thuê ngoài dịch vụ ngân hàng điện tử với bên thứ ba.

   - Quyết định thuê ngoài một chức năng hoặc dịch vụ ngân hàng điện tử quan trọng cần nhất quán với các chiến lược kinh doanh của ngân hàng và dựa trên nhu cầu kinh doanh được xác định rõ ràng và việc nhận thức được các rủi ro cụ thể nảy sinh từ việc thuê ngoài.

   - Tất cả các bộ phận trong ngân hàng có liên quan cần hiểu phương thức mà (các) nhà cung cấp dịch vụ sẽ hỗ trợ chiến lược phát triển dịch vụ ngân hàng điện tử và phù hợp với cơ cấu hoạt động của ngân hàng.

2. Ngân hàng cần triển khai phân tích rủi ro phù hợp và tính tuân thủ trước khi lựa chọn một nhà cung cấp dịch vụ ngân hàng điện tử và luôn đánh giá định kỳ trong thời gian sau này.

   - Ngân hàng cần cân nhắc xây dựng các qui trình đánh giá đề xuất của các nhà cung cấp dịch vụ ngân hàng điện tử và các tiêu chí nhằm lựa chọn giữa các đề xuất đó.

   - Sau khi đã xác định được một nhà cung cấp dịch vụ, ngân hàng cần tiến hành đánh giá tính tuân thủ phù hợp, bao gồm việc đánh giá rủi ro liên quan đến tiềm lực tài chính, uy tín, chính sách và biện pháp kiểm soát quản trị rủi ro và khả năng thực hiện nghĩa vụ của nhà cung cấp dịch vụ.

   - Sau đó, ngân hàng cần thường xuyên theo dõi và, khi cần thiết,[36] thực hiện đánh giá tính tuân thủ đối với khả năng của nhà cung cấp dich vụ trong việc thực hiện dịch vụ và các nghĩa vụ quản trị rủi ro có liên quan trong toàn bộ thời gian ký hợp đồng.

   - Ngân hàng cần đảm bảo có đủ nguồn lực phù hợp như đã cam kết trong việc giám sát việc thuê ngoài hỗ trợ cho ngân hàng điện tử.

   - Trách nhiệm trong việc giám sát các hợp đồng ngân hàng điện tử thuê ngoài cần được phân bổ rõ ràng.

[36] Việc đánh giá liên tục tính tuân thủ cần dựa trên tính chất của các hoạt đông thuê ngoài và mức độ của hệ thống cũng như các thay đổi về quản trị rủi ro theo từng thời kỳ, bao gồm cả việc nhà cung cấp dịch vụ ký kết bất kỳ hợp đồng phụ nào khác.

- Ngân hàng cần chuẩn bị một chiến lược rút lui phù hợp nhằm quản trị rủi ro trong trường hợp cần phải chấm dứt quan hệ thuê ngoài.

3. Ngân hàng cần áp dụng các qui trình phù hợp nhằm đảm bảo tính chất hợp lý của các hợp đồng liên quan đến ngân hàng điện tử. Các hợp đồng liên quan đến thuê ngoài các hoạt động ngân hàng điện tử cần giải quyết, ví dụ như sau[37]:

   - Trách nhiệm theo hợp đồng của các bên liên quan cũng như trách nhiệm ra quyết định, bao gồm bất kỳ hợp đồng thầu phụ nào khác đối với bất kỳ dịch vụ cụ thể nào cũng phải được xác định rõ ràng.

   - Trách nhiệm cung cấp thông tin và nhận thông tin từ nhà cung cấp dịch vụ phải được xác định rõ ràng. Thông tin do nhà cung cấp dịch vụ cung cấp phải kịp thời và đầy đủ để ngân hàng có thể đánh giá mức độ dịch vụ và rủi ro. Cần phải xác định rõ phương thức và qui trình thông báo cho ngân hàng về gián đoạn dịch vụ, đột nhập an ninh và các sự kiện khác dẫn tới rủi ro nghiêm trọng cho ngân hàng.

   - Các điều khoản giải quyết cụ thể vấn đề bảo hiểm, quyền sở hữu dữ liệu lưu trữ tại các máy chủ hoặc cơ sở dữ liệu của nhà cung cấp dịch vụ và quyền của ngân hàng trong việc phục hồi các dữ liệu đó trong trường hợp hết hạn hoặc chấm dứt hợp đồng cần phải được qui định rõ ràng.

   - Cần qui định khả năng thực hiện kỳ vọng trong các trường hợp bình thường và dự phòng.

   - Cần qui định các biện pháp và bảo hành phù hợp, ví dụ được đề cập trong các điều khoản về kiểm toán nhằm đảm bảo rằng nhà cung cấp dịch vụ tuân thủ các chính sách của ngân hàng.

   - Cần có những điều khoản qui định việc can thiệp theo trình tự, kịp thời và kiểm chứng trong trường hợp cung cấp dịch vụ không đủ tiêu chuẩn.

   - Đối với các hợp đồng thuê ngoài tại nước ngoài, cần phải xác định rõ sẽ áp dụng luật và qui định của quốc gia nào đối với việc bảo vệ quyền riêng tư và các biện pháp khác bảo vệ khách hàng.

   - Cần qui định rõ quyền của ngân hàng trong việc tiến hành đánh giá độc lập và/hoặc kiểm toán về an ninh, kiểm soát nội bộ, kế hoạch duy trì kinh doanh và kế hoạch dự phòng.

4. Ngân hàng cần đảm bảo sẽ tiến hành các đợt kiểm toán nội bộ và/hoặc kiểm toán bên ngoài định kỳ đối với các hoạt động thuê ngoài với mức độ ít nhất là tương đương như các hoạt động đó được nội bộ tự thực hiện[38].

[37] Như đối với các hợp đồng pháp lý khác của ngân hàng, luật sư pháp lý hoặc phòng pháp lý cần xem xét tất cả các điều khoản và điều kiện trong hợp đồng thuê ngoài ngân hàng điện tử.

[38] Nếu ngân hàng không có bộ phận kiểm toán đặc biệt trong nội bộ thì ít nhất cũng phải bố trí cán bộ không tham gia vào công tác quản trị các quan hệ thuê ngoài thực hiện việc đánh giá hiệu quả trong việc giám sát các hợp đồng thuê ngoài.

- Đối với các quan hệ thuê ngoài liên quan đến các dịch vụ/ứng dụng ngân hàng điện tử quan trọng hoặc phức tạp về mặt công nghệ thì ngân hàng cần có bên thứ ba có kinh nghiệm kỹ thuật thực hiện đánh giá định kỳ một cách độc lập.

5. Ngân hàng cần xây dựng các kế hoạch dự phòng phù hợp đối với các hoạt động ngân hàng điện tử đã được thuê ngoài.

- Ngân hàng cần xây dựng và định kỳ kiểm tra kế hoạch dự phòng của tất cả các hệ thống và dịch vụ ngân hàng điện tử quan trọng đã thuê bên thứ ba.

- Kế hoạch dự phòng cần giải quyết các tình huống xấu nhất có thể xảy ra nhằm đảm bảo duy trì dịch vụ ngân hàng điện tử trong trường hợp gián đoạn ảnh hưởng đến các hoạt động đã được thuê ngoài.

- Ngân hàng cần xác định một nhóm công tác chịu trách nhiệm quản lý phục hồi và đánh giá tác động tài chính của sự kiện gián đoạn các dịch vụ ngân hàng điện tử đã được thuê ngoài.

6. Ngân hàng cung cấp dịch vụ ngân hàng điện tử cho bên thứ ba cần đảm bảo rằng hoạt động, trách nhiệm và nghĩa vụ là rõ ràng để đối tượng được cung cấp dịch vụ có thể tiến hành các đánh giá tuân thủ hiệu quả và giám sát thường xuyên quan hệ đó.

- Ngân hàng có trách nhiệm cung cấp cho đối tượng được cung cấp dịch vụ các thông tin cần thiết nhằm xác định, kiểm soát và theo dõi bất kỳ rủi ro nào liên quan tới thỏa thuận dịch vụ ngân hàng điện tử.

Phụ lục III

THÔNG LỆ CẤP PHÉP HIỆU QUẢ TRONG ỨNG DỤNG NGÂN HÀNG ĐIỆN TỬ

1. Việc cấp phép cụ thể và các đặc quyền truy cập cần được thực hiện đối với tất cả đối tượng, đại lý hoặc các hệ thống thực hiện các hoạt động ngân hàng điện tử.

2. Tất cả các hệ thống ngân hàng điện tử cần được xây dựng nhằm đảm bảo rằng các hệ thống này liên kết với một cơ sở dữ liệu cấp phép có hiệu lực.

3. Không đại lý hoặc hệ thống đơn lẻ nào có quyền thay đổi thẩm quyền của chính họ hoặc thay đổi các đặc quyền truy cập trong một cơ sở dữ liệu cấp phép ngân hàng điện tử[39].

4. Bất kỳ việc bổ sung của một cá nhân, đại lý hoặc hệ thống hoặc bất kỳ thay đổi về đặc quyền truy cập trong cơ sở dữ liệu cấp phép ngân hàng điện tử cần được cấp phép phù hợp bởi một nguồn được chứng thực là có đầy đủ thẩm quyền cần thiết và tuân thủ theo qui trình giám sát phù hợp và kịp thời và ghi lại bằng chứng phục vụ đánh giá độc lập.

5. Cần xây dựng các biện pháp phù hợp nhằm chống lại sự thay đổi cơ sở dữ liệu cấp phép trong ngân hàng điện tử. Bất kỳ sự thay đổi nào cần được phát hiện thông qua các qui trình giám sát liên tục. Cần lưu giữ đầy đủ tập tin lưu bằng chứng thể hiện sự thay đổi đó.

6. Không sử dụng bất kỳ cơ sở dữ liệu cấp phép ngân hàng điện tử nào đã bị thay đổi cho đến khi được thay thế bởi một cơ sở dữ liệu đã được kiểm chứng.

7. Cần có các biện pháp kiểm soát nhằm ngăn ngừa thay đổi đối với các mức độ cấp phép trong các phiên giao dịch ngân hàng điện tử và cần ghi lại bất kỳ hành động nào nhằm thay đổi cấp phép và việc này cần phải được báo cáo cho Ban (tổng) giám đốc.

[39] Vì điều này có thể không khả thi đối với người sử dụng quản trị hệ thống nên cần phải có các biện pháp kiểm soát nội bộ chặt chẽ và sự phân công nhiệm vụ nhằm theo dõi các hoạt động của các tài khoản người sử dụng đó.

Phụ lục IV

THÔNG LỆ TỐT NHẤT VỀ THEO DÕI BẰNG CHỨNG PHỤC VỤ KIỂM TOÁN TRONG HỆ THỐNG NGÂN HÀNG ĐIỆN TỬ

1. Cần lưu giữ đầy đủ các bản ghi đối với tất cả các giao dịch ngân hàng điện tử giúp xây dựng đầy đủ bằng chứng phục vụ kiểm toán và hỗ trợ cho việc giải quyết các tranh chấp.

2. Các hệ thống ngân hàng điện tử cần được thiết kế và cài đặt làm sao để ghi lại và duy trì các bằng chứng pháp lý nhằm duy trì kiểm soát bằng chứng, tránh việc giả mạo và thu thập các bằng chứng giả.

3. Trong trường hợp nhà cung cấp dịch vụ bên thứ ba chịu trách nhiệm về hệ thống xử lý và theo dõi kiểm toán liên quan:

    - Ngân hàng cần đảm bảo có thể truy cập vào hệ thống theo dõi bằng chứng kiểm toán do nhà cung cấp dịch vụ duy trì.

    - Các bằng chứng kiểm toán do nhà cung cấp dịch vụ chịu trách nhiệm duy trì phải đúng tiêu chuẩn của ngân hàng.

Phụ lục V

THÔNG LỆ TỐT NHẤT GIÚP DUY TRÌ SỰ RIÊNG TƯ CỦA THÔNG TIN KHÁCH HÀNG SỬ DỤNG DỊCH VỤ NGÂN HÀNG ĐIỆN TỬ

1. Các ngân hàng cần sử dụng các kỹ thuật mã hóa phù hợp, các giao thức cụ thể hoặc các biện pháp kiểm soát khác nhằm đảm bảo tính chất bảo mật các dữ liệu của khách hàng sử dụng dịch vụ ngân hàng điện tử.

2. Các ngân hàng cần xây dựng các qui trình và các biện pháp kiểm soát phù hợp nhằm thường xuyên đánh giá cơ sở hạ tầng an ninh của khách hàng và các giao thức phục vụ cho dịch vụ ngân hàng điện tử.

3. Các ngân hàng cần đảm bảo rằng các nhà cung cấp dịch vụ là bên thứ ba áp dụng các chính sách về riêng tư và bảo mật tương ứng với các chính sách tại ngân hàng.

4. Các ngân hàng cần triển khai các bước phù hợp nhằm thông báo với các khách hàng sử dụng dịch vụ ngân hàng điện tử về sự riêng tư và bảo mật các thông tin của khách hàng. Các bước này bao gồm:

   - Thông báo cho khách hàng về chính sách riêng tư của ngân hàng, có thể được đăng tải trên trang chủ của ngân hàng. Việc sử dụng từ ngữ rõ ràng và ngắn gọn trong các thông báo là cần thiết nhằm đảm bảo cho khách hàng hiểu rõ về chính sách riêng tư. Phần mô tả dài dòng về pháp lý, tuy nội dung vẫn chính xác nhưng trong thực tế, hầu hết khách hàng đều không đọc phần này.

   - Hướng dẫn khách hàng về sự cần thiết phải bảo vệ mật khẩu, mã số nhận dạng cá nhân (PINs) và các dữ liệu cá nhân và/hoặc dữ liệu ngân hàng.

   - Cung cấp cho khách hàng thông tin tổng quát về vấn đề an ninh đối với máy tính cá nhân, bao gồm các lợi ích khi sử dụng phần mềm chống virus, kiểm soát truy cập máy tính và tường lửa cá nhân đối với các kết nối Internet tĩnh.

Phụ lục VI

THÔNG LỆ TỐT NHẤT VỀ NĂNG LỰC, LẬP KẾ HOẠCH DUY TRÌ KINH DOANH VÀ LẬP KẾ HOẠCH DỰ PHÒNG TRONG NGÂN HÀNG ĐIỆN TỬ

1. Cần xác định và đánh giá tất cả các dịch vụ và ứng dụng ngân hàng điện tử, bao gồm những ứng dụng do nhà cung cấp dịch vụ là bên thứ ba cung cấp.

2. Cần thực hiện công tác đánh giá rủi ro đối với từng dịch vụ và ứng dụng ngân hàng điện tử quan trọng, bao gồm bất kỳ rủi ro tiềm tàng nào dẫn đến việc gián đoạn kinh doanh hoặc gây ra rủi ro tín dụng, thị trường, thanh khoản, pháp lý, hoạt động và uy tín của ngân hàng.

3. Cần xây dựng các chỉ tiêu hoạt động đối với từng dịch vụ và ứng dụng ngân hàng điện tử, và cần theo dõi các mức độ dịch vụ dựa trên các chỉ tiêu này. Cần thực hiện các biện pháp cần thiết nhằm đảm bảo rằng các hệ thống ngân hàng điện tử có thể xử lý được khối lượng giao dịch ít hoặc nhiều và việc hoạt động và năng lực hệ thống phải nhất quán với kỳ vọng phát triển ngân hàng điện tử trong tương lai của ngân hàng.

4. Cần xem xét xây dựng các phương thức xử lý lựa chọn để quản lý các nhu cầu khi các hệ thống ngân hàng điện tử có dấu hiệu đạt tới mức năng lực đã xác định.

5. Cần xây dựng các kế hoạch duy trì kinh doanh ngân hàng điện tử nhằm giải quyết vấn đề phụ thuộc vào các nhà cung cấp dịch vụ là bên thứ ba và bất kỳ sự phụ thuộc nào từ bên ngoài trong việc cần phục hồi.

6. Các kế hoạch ngân hàng điện tử dự phòng cần đưa ra một qui trình phục hồi hoặc thay thế khả năng xử lý ngân hàng điện tử, phục hồi thông tin hỗ trợ giao dịch và bao gồm các biện pháp cần áp dụng để khôi phục lại các hệ thống và ứng dụng ngân hàng điện tử quan trọng trong trường hợp gián đoạn kinh doanh.