

NGÂN HÀNG NHÀ NƯỚC VIỆT NAM

NGÂN HÀNG NHÀ NƯỚC CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
VIỆT NAM Độc lập - Tự do - Hạnh phúc

Số: 35/2006/QĐ-NHNN

Hà Nội, ngày 31 tháng 7 năm 2006

QUYẾT ĐỊNH

**Ban hành Quy định về các nguyên tắc quản lý rủi ro
trong hoạt động ngân hàng điện tử**

THÔNG ĐỌC NGÂN HÀNG NHÀ NƯỚC

Căn cứ Luật Ngân hàng Nhà nước Việt Nam năm 1997; Luật sửa đổi, bổ sung một số điều của Luật Ngân hàng Nhà nước Việt Nam năm 2003;

Căn cứ Luật Các tổ chức tín dụng năm 1997; Luật sửa đổi, bổ sung một số điều của Luật Các tổ chức tín dụng năm 2004;

Căn cứ Luật Giao dịch Điện tử năm 2005;

Căn cứ Nghị định số 52/2003/NĐ-CP ngày 19/5/2003 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Ngân hàng Nhà nước Việt Nam;

Theo đề nghị của Vụ trưởng Vụ Các Ngân hàng và tổ chức tín dụng phi ngân hàng,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy định về các nguyên tắc quản lý rủi ro trong hoạt động ngân hàng điện tử.

Điều 2. Quyết định này có hiệu lực sau 15 ngày, kể từ ngày đăng Công báo.

Điều 3. Chánh Văn phòng, Vụ trưởng Vụ Các Ngân hàng và Tổ chức tín dụng

phi ngân hàng, Thủ trưởng các đơn vị có liên quan thuộc Ngân hàng Nhà nước Việt Nam, Giám đốc Ngân hàng Nhà nước chi nhánh tỉnh, thành phố trực thuộc Trung ương và Chủ tịch Hội đồng quản trị, Tổng Giám đốc (Giám đốc) tổ chức tín dụng chịu trách nhiệm thi hành Quyết định này./.

**KT. THÔNG ĐỐC
PHÓ THÔNG ĐỐC**

Đặng Thanh Bình

NGÂN HÀNG NHÀ NƯỚC CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
VIỆT NAM Độc lập - Tự do - Hạnh phúc

**QUY ĐỊNH VỀ CÁC NGUYÊN TẮC QUẢN LÝ RỦI RO TRONG
HOẠT ĐỘNG NGÂN HÀNG ĐIỆN TỬ**

*(Ban hành kèm theo Quyết định số 35/2006/QĐ-NHNN
ngày 31 tháng 7 năm 2006 của Thống đốc Ngân hàng Nhà nước)*

CHƯƠNG I
NHỮNG QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng

1. Quy định này xác định các nguyên tắc quản lý rủi ro trong hoạt động ngân hàng điện tử.

2. Tổ chức tín dụng và chi nhánh ngân hàng nước ngoài tại Việt Nam (sau đây gọi chung là tổ chức tín dụng) có thực hiện hoạt động ngân hàng điện tử phải tuân thủ các nguyên tắc quản lý rủi ro nêu tại Quy định này.

Điều 2. Mục đích

Các nguyên tắc quản lý rủi ro trong hoạt động ngân hàng điện tử là cơ sở cho các tổ chức tín dụng xây dựng quy định nội bộ về quản lý rủi ro trong hoạt động ngân hàng điện tử.

Điều 3. Giải thích từ ngữ

Trong Quy định này, các từ ngữ dưới đây được hiểu như sau:

1. *Hoạt động ngân hàng điện tử* là hoạt động ngân hàng được thực hiện qua các kênh phân phối điện tử.

2. *Kênh phân phối điện tử* là hệ thống các phương tiện điện tử và quy trình tự

động xử lý giao dịch được tổ chức tín dụng sử dụng để giao tiếp với khách hàng và cung ứng các sản phẩm, dịch vụ ngân hàng cho khách hàng.

3. *Rủi ro trong hoạt động ngân hàng điện tử* là khả năng xảy ra tổn thất khi thực hiện các hoạt động ngân hàng điện tử.

4. *Khách hàng* là các tổ chức, cá nhân có quan hệ giao dịch với tổ chức tín dụng.

5. *Bên thứ ba* là các tổ chức chuyên môn được tổ chức tín dụng thuê hoặc hợp tác với tổ chức tín dụng cung cấp dịch vụ kỹ thuật hỗ trợ cho hoạt động ngân hàng điện tử.

Điều 4. Phạm vi hoạt động ngân hàng điện tử

Tổ chức tín dụng được tiến hành các hoạt động ngân hàng điện tử trong phạm vi nội dung hoạt động quy định tại Giấy phép thành lập và hoạt động và phù hợp với Điều lệ của tổ chức tín dụng.

Điều 5. Nguyên tắc chung

1. Tổ chức tín dụng chịu trách nhiệm về an toàn và hiệu quả của hoạt động ngân hàng điện tử; bảo vệ quyền và lợi ích hợp pháp của tổ chức tín dụng, của khách hàng, lợi ích của Nhà nước và xã hội theo quy định của pháp luật.

2. Để quản lý một cách có hiệu quả những rủi ro phát sinh trong hoạt động ngân hàng điện tử, tổ chức tín dụng cần:

a) Nhận định các rủi ro có thể phát sinh từ những hoạt động ngân hàng điện tử hiện đang thực hiện hoặc dự kiến triển khai;

b) Phân tích và xác định các tác động và hậu quả có thể phát sinh khi rủi ro xảy ra;

c) Phân nhóm các loại rủi ro; xác định phương hướng và biện pháp phòng ngừa rủi ro, đặc biệt lưu ý đến quản lý an ninh mạng và bảo vệ thông tin; xác định mức tổn thất tối đa có thể chấp nhận được trong trường hợp xảy ra rủi ro; không triển khai các loại hình hoạt động ngân hàng điện tử đòi hỏi những biện pháp phòng ngừa rủi ro vượt ngoài khả năng hiện có;

d) Thường xuyên đánh giá, kiểm tra kết quả và hiệu quả của công tác quản lý rủi ro; kiểm toán và cập nhật quy trình quản lý rủi ro.

CHƯƠNG II

CÁC NGUYÊN TẮC QUẢN LÝ RỦI RO TRONG HOẠT ĐỘNG NGÂN HÀNG ĐIỆN TỬ

MỤC 1

QUẢN LÝ RỦI RO TRONG NỘI BỘ TỔ CHỨC TÍN DỤNG

Điều 6. Xây dựng phương án hoạt động ngân hàng điện tử

Trước khi triển khai hoạt động ngân hàng điện tử, tổ chức tín dụng cần xây dựng phương án hoạt động đảm bảo những nội dung cơ bản sau:

1. Cơ sở để quyết định thực hiện hoạt động ngân hàng điện tử như: nhu cầu của thị trường; chiến lược phát triển của tổ chức tín dụng; khả năng đáp ứng của tổ chức tín dụng về vốn, công nghệ, kỹ thuật, khả năng quản trị, kiểm soát rủi ro và nguồn nhân lực.

2. Mục tiêu cụ thể của tổ chức tín dụng khi thực hiện hoạt động ngân hàng điện tử.

3. Những rủi ro có thể phát sinh khi thực hiện hoạt động ngân hàng điện tử và biện pháp quản lý rủi ro tương ứng.

4. Kế hoạch đánh giá định kỳ, tối thiểu một năm một lần, hiệu quả của hoạt động ngân hàng điện tử thông qua các tiêu chí cơ bản như: thu nhập và chi phí từ hoạt động ngân hàng điện-tử; số lượng khách hàng thường xuyên sử dụng các dịch vụ, sản phẩm ngân hàng điện tử; tổng số giao dịch ngân hàng điện tử đã thực hiện và chi phí bình quân cho mỗi giao dịch; các tiêu chí khác phù hợp với thực tế hoạt động của tổ chức tín dụng.

Điều 7. Chính sách quản lý rủi ro

1. Xác định mức độ rủi ro tối đa mà tổ chức tín dụng có thể chấp nhận được;
2. Trách nhiệm cụ thể của từng phòng, ban tham gia hoạt động ngân hàng điện tử;
3. Quy định chế độ báo cáo định kỳ và báo cáo đột xuất khi xảy ra sự cố;
4. Có biện pháp quản lý từng loại rủi ro cụ thể phát sinh trong quá trình cung ứng sản phẩm, dịch vụ ngân hàng điện tử; đồng thời yêu cầu bên thứ ba phải áp dụng các biện pháp tương tự;

5. Nghiên cứu, đánh giá mức độ rủi ro và khả năng kiểm soát rủi ro, triển khai thử nghiệm các sản phẩm mới trước khi cung ứng ra thị trường.

Điều 8. Phân định phạm vi trách nhiệm, quyền hạn

Tổ chức tín dụng phải phân định rõ phạm vi trách nhiệm, quyền hạn của từng bộ phận, từng nhân viên tham gia vào một quy trình của hoạt động ngân hàng điện tử:

1. Xem xét lại và sửa đổi, bổ sung (nếu cần thiết) chế độ phân cấp quyền hạn, trách nhiệm đang áp dụng tại tổ chức tín dụng, đảm bảo phù hợp với đặc điểm và yêu cầu của hoạt động ngân hàng điện tử.

2. Phân định phạm vi trách nhiệm giữa nhân viên nhập dữ liệu và nhân viên kiểm tra dữ liệu.

3. Phân định phạm vi trách nhiệm giữa bộ phận xây dựng hệ thống và bộ phận quản trị hệ thống ngân hàng điện tử.

4. Thường xuyên kiểm tra việc tuân thủ yêu cầu phân cấp trách nhiệm, quyền hạn trong hoạt động ngân hàng điện tử.

Điều 9. Bảo vệ dữ liệu

1. Tổ chức tín dụng phải có các biện pháp thích hợp để đảm bảo dữ liệu của mọi giao dịch ngân hàng điện tử được lưu trữ an toàn, đầy đủ, toàn vẹn và chính xác theo nguyên tắc:

a) Tất cả các dữ liệu, cơ sở dữ liệu của giao dịch ngân hàng điện tử đều được lưu trữ, trong đó cần lưu ý đối với việc mở hoặc đóng tài khoản của khách hàng; giao dịch có liên quan đến kết quả tài chính; sự thay đổi về thẩm quyền truy cập, phạm vi truy cập và giới hạn được phép giao dịch của từng cá nhân trong tổ chức tín dụng và khách hàng.

b) Quy định về việc cấp, đăng ký và bảo mật đối với quyền truy cập của từng nhân viên, cán bộ của tổ chức tín dụng và khách hàng trong hoạt động ngân hàng điện tử.

c) Mọi trường hợp bổ sung, xóa bỏ hoặc thay đổi cơ sở dữ liệu của một tổ chức, cá nhân hoặc hệ thống phải do một đầu mối có thẩm quyền thực hiện. Thông tin về thời điểm xóa bỏ, thay đổi cơ sở dữ liệu và người thực hiện việc xóa bỏ, thay đổi đó phải được lưu lại để phục vụ công tác kiểm tra, kiểm soát.

2. Tổ chức tín dụng phải xây dựng quy trình kiểm soát an toàn dữ liệu trong hoạt động ngân hàng điện tử.

a) Áp dụng các biện pháp kỹ thuật, công nghệ cần thiết để ngăn chặn những trường hợp truy cập trái phép vào các ứng dụng và cơ sở dữ liệu của hoạt động ngân hàng điện tử;

b) Thường xuyên xem xét và kiểm định lại hiệu quả của các biện pháp quản lý an toàn dữ liệu để có những điều chỉnh kịp thời nếu cần thiết.

3. Tổ chức tín dụng phải áp dụng các biện pháp cần thiết nhằm đảm bảo bí mật thông tin hoạt động ngân hàng điện tử. Từng biện pháp cụ thể phải phù hợp với mức độ quan trọng của thông tin được truyền đi hay lưu trữ trong cơ sở dữ liệu.

a) Chỉ những cá nhân có thẩm quyền mới được phép tiếp cận đến dữ liệu mật của tổ chức tín dụng;

b) Mọi thông tin bí mật của tổ chức tín dụng phải được lưu trữ một cách an toàn và phải được bảo vệ khỏi mọi nguy cơ bị sửa đổi, truy cập trái phép hoặc rò rỉ trong quá trình truyền dữ liệu qua các mạng nội bộ hoặc mạng công cộng;

c) Trường hợp được quyền tiếp cận đến những thông tin mật của tổ chức tín dụng, bên thứ ba cũng phải tuân thủ mọi tiêu chuẩn và chế độ kiểm tra, kiểm soát do tổ chức tín dụng quy định;

d) Tổ chức tín dụng phải thực hiện các biện pháp kỹ thuật để lưu trữ từng lượt truy cập thông tin mật và bảo đảm thông tin lưu trữ này không bị sửa đổi.

Điều 10. Kiểm tra, kiểm soát, kiểm toán nội bộ

1. Tổ chức tín dụng phải xây dựng, điều chỉnh quy trình kiểm tra, kiểm soát, kiểm toán nội bộ phù hợp với đặc điểm của hoạt động ngân hàng điện tử.

2. Hệ thống ngân hàng điện tử được kiểm tra, đánh giá thường xuyên và được kiểm soát, kiểm toán nội bộ định kỳ hoặc đột xuất nhằm phát hiện, ngăn ngừa các hành vi truy cập bất hợp pháp hoặc vượt thẩm quyền.

3. Cần lưu ý đến vấn đề bản quyền đối với các phần mềm và ứng dụng sử dụng trong hệ thống ngân hàng điện tử.

4. Dữ liệu liên quan đến một giao dịch ngân hàng điện tử phải được lưu giữ đầy đủ phục vụ công tác kiểm tra, kiểm soát, kiểm toán nội bộ của tổ chức tín dụng. Thời gian lưu trữ chứng từ giao dịch điện tử được thực hiện theo quy định của pháp luật về lưu trữ.

MỤC 2

QUẢN LÝ RỦI RO TRONG GIAO DỊCH VỚI KHÁCH HÀNG

Điều 11. Nguyên tắc giao dịch

1. Bảo mật và bảo đảm tính toàn vẹn và chính xác của những thông tin, dữ liệu, cơ sở dữ liệu của các số liệu giao dịch trong hoạt động ngân hàng điện tử.

2. Phân loại giao dịch, những giao dịch quan trọng phải được người có thẩm quyền tại từng bộ phận kiểm tra, giám sát và phải được kiểm tra, giám sát giữa các bộ phận chức năng trong nội bộ tổ chức tín dụng.

3. Bảo đảm cung cấp cho khách hàng những thông tin chính xác, giúp khách hàng trước khi giao dịch với tổ chức tín dụng có được sự hiểu biết, đánh giá đúng về khả năng và thực trạng của tổ chức tín dụng, về các quyền lợi và nghĩa vụ của mình.

Điều 12. Các nguyên tắc trong quan hệ với khách hàng

1. Tổ chức tín dụng phải quy định cụ thể về trình tự, thủ tục thiết lập quan hệ tiếp nhận và xử lý giao dịch ngân hàng điện tử với khách hàng.

2. Đảm bảo xác minh nhân dạng, quyền tiếp cận thông tin, tài khoản, phạm vi và giới hạn được phép giao dịch của khách hàng.

3. Xác lập và công bố rõ ràng nghĩa vụ, trách nhiệm và quyền hạn của khách hàng khi đưa ra đề nghị giao dịch; đảm bảo ngăn ngừa việc phù nhận hoặc thoái thác giao dịch từ phía khách hàng.

4. Khi ký hợp đồng cung cấp dịch vụ ngân hàng điện tử cho khách hàng và/hoặc trong lần đầu tiên sử dụng dịch vụ ngân hàng điện tử của khách hàng, ngân hàng phải có trách nhiệm công khai và giải thích rõ ràng, đầy đủ những rủi ro khách hàng có thể gặp phải khi sử dụng những dịch vụ này.

5. Ngăn ngừa, phát hiện kịp thời bất kỳ sự giả mạo, sửa đổi những thông tin, dữ liệu kế toán, tài chính và các cam kết liên quan đến quyền lợi, nghĩa vụ của tổ chức tín dụng và khách hàng.

MỤC 3

QUẢN LÝ RỦI RO ĐỐI VỚI BÊN THỨ BA

Điều 13. Đánh giá bên thứ ba

09694454
www.ThuVienPhapLuat.com
Tel: +84-8-3845 6684
LawSoft

Trong trường hợp thuê hoặc hợp tác với bên thứ ba để cung cấp dịch vụ kỹ thuật hỗ trợ cho hoạt động ngân hàng điện tử, tổ chức tín dụng phải:

1. Đánh giá thận trọng và đầy đủ những rủi ro có thể phát sinh; có kế hoạch dự phòng trường hợp dịch vụ do bên thứ ba cung cấp bị gián đoạn.
2. Thẩm định kỹ năng lực kỹ thuật, khả năng tài chính của các bên đối tác. Các bên đối tác phải có đủ năng lực tài chính, uy tín và tiềm năng để chịu trách nhiệm pháp lý và trách nhiệm tài chính có thể phát sinh liên quan đến phần dịch vụ do các bên này cung cấp.
3. Lưu ý đến các vấn đề về an ninh, bảo mật khi nhân viên của bên thứ ba được phép tiếp cận với hệ thống ngân hàng điện tử.
4. Xác định rõ trách nhiệm, quyền hạn và nghĩa vụ của các bên trong hợp đồng thuê, hợp đồng hợp tác; đảm bảo tổ chức tín dụng có quyền kiểm tra, giám sát định kỳ hoặc đột xuất đối với hoạt động cung cấp dịch vụ hỗ trợ kỹ thuật của bên thứ ba và có quyền yêu cầu bên thứ ba thực hiện kiểm toán độc lập khi cần thiết.
5. Thường xuyên đánh giá các vướng mắc, sự cố, các vấn đề tiềm ẩn trong quan hệ với bên thứ ba trong hoạt động ngân hàng điện tử để có biện pháp quản lý rủi ro thích hợp.

Điều 14. Dữ liệu

Trong trường hợp bên thứ ba chịu trách nhiệm quản lý hệ thống xử lý và lưu trữ dữ liệu, tổ chức tín dụng cần đảm bảo:

1. Trong hợp đồng ký kết với bên thứ ba phải quy định rõ việc tổ chức tín dụng có quyền tiếp cận đến những dữ liệu cần thiết;
2. Mọi dữ liệu do bên thứ ba lưu trữ đều phải đáp ứng các tiêu chuẩn và yêu cầu về bảo mật của tổ chức tín dụng.

MỤC 4

QUẢN LÝ RỦI RO TRONG CÁC TRƯỜNG HỢP XẢY RA SỰ CỐ

Điều 15. Phòng ngừa sự cố

1. Xây dựng hệ thống lưu trữ cơ sở dữ liệu và từng bước xây dựng hệ thống dự phòng xử lý giao dịch ngân hàng điện tử.

2. Thực hiện kiểm tra định kỳ và đột xuất để đánh giá: khả năng hoạt động liên tục của hệ thống ngân hàng điện tử; nguồn lực hiện tại và khả năng nâng cấp trong tương lai trên cơ sở có tính đến các yếu tố thị trường đối với thương mại điện tử và tỷ lệ khách hàng dự kiến chấp thuận các dịch vụ và sản phẩm ngân hàng điện tử.

3. Xây dựng các kế hoạch phản ứng khi xảy ra sự cố để có thể kiểm soát, khoanh vùng và giảm thiểu rắc rối phát sinh từ những sự kiện bất ngờ, bao gồm các sự cố phát sinh từ bên ngoài và bên trong hệ thống, trong và ngoài giờ làm việc, tác động vào hệ thống ngân hàng điện tử làm ảnh hưởng đến việc cung cấp các dịch vụ ngân hàng điện tử.

4. Xây dựng quy trình kiểm soát sự cố, xác định người có trách nhiệm nhận thông tin và xử lý thông tin khi hoạt động ngân hàng điện tử phát sinh sự cố. Xác định trước nhân sự của nhóm xử lý sự cố để đề phòng phát sinh những sự cố nghiêm trọng cần phải xử lý ngay. Tổ chức tín dụng có thể thỏa thuận trước với bên thứ ba về việc trưng dụng nhân sự vào nhóm xử lý sự cố khi phát sinh những sự cố nghiêm trọng.

5. Có văn bản quy định rõ phạm vi trách nhiệm của tổ chức tín dụng, bên thứ ba trong trường hợp xảy ra sự cố. Văn bản này phải được cung cấp đầy đủ cho bên thứ ba ngay khi ký kết hợp đồng. Trong trường hợp văn bản nói trên có những nội dung liên quan đến quyền lợi và trách nhiệm của khách hàng trong trường hợp xảy ra sự cố thì những nội dung này phải được công bố cho khách hàng biết khi khách hàng ký kết hợp đồng sử dụng dịch vụ hoặc trong lần đầu tiên khách hàng sử dụng dịch vụ ngân hàng điện tử.

Điều 16. Kiểm soát và khắc phục sự cố

Trong trường hợp hệ thống ngân hàng điện tử xảy ra sự cố, tổ chức tín dụng cần áp dụng các biện pháp sau:

1. Triển khai các biện pháp xử lý sự cố theo quy trình kiểm soát sự cố và phương án xử lý sự cố đã xây dựng.

2. Xác định điểm xảy ra sự cố, nguyên nhân sự cố là do lỗi kỹ thuật hay do yếu tố con người. Khoanh vùng ảnh hưởng và xác định nhóm khách hàng có thể bị ảnh hưởng.

3. Kịp thời có biện pháp tuyên truyền, giải thích cho dân chúng, khách hàng và các đối tượng có liên quan về những sự cố phát sinh đối với hệ thống ngân hàng điện tử.

4. Thu thập, bảo toàn chứng cứ pháp lý để phục vụ việc kiểm tra, xử lý các sự cố đối với hệ thống ngân hàng điện tử và có biện pháp xử lý đối với những tổ chức, cá nhân vi phạm pháp luật.

5. Nhanh chóng khắc phục sự cố, giải quyết các tranh chấp phát sinh có liên quan đến sự cố và bồi thường các thiệt hại thuộc trách nhiệm của mình để tránh các rủi ro có thể xảy ra đối với uy tín của tổ chức tín dụng.

CHƯƠNG III

ĐIỀU KHOẢN THI HÀNH

Điều 17. Quy định nội bộ của tổ chức tín dụng

1. Căn cứ vào tính chất và đặc điểm của kênh phân phối điện tử có liên quan đến hoạt động ngân hàng điện tử, tổ chức tín dụng có trách nhiệm ban hành quy định nội bộ về quản lý rủi ro trong hoạt động ngân hàng điện tử trên cơ sở phù hợp với pháp luật hiện hành và các nguyên tắc nêu tại Quy định này.

2. Trong thời hạn 06 tháng kể từ ngày Quy định này có hiệu lực thi hành, tổ chức tín dụng đã thực hiện hoạt động ngân hàng điện tử phải xây dựng và gửi quy định nội bộ về quản lý rủi ro trong hoạt động ngân hàng điện tử cho Ngân hàng Nhà nước Việt Nam (Thanh tra Ngân hàng Nhà nước, Vụ Các Ngân hàng, Cục Công nghệ tin học ngân hàng, Ngân hàng Nhà nước chi nhánh tỉnh, thành phố trực thuộc Trung ương nơi tổ chức tín dụng có phần đặt trụ sở chính) để phục vụ công tác kiểm tra, giám sát.

3. Trong trường hợp tổ chức tín dụng thay đổi các nội dung tại quy định nội bộ nói trên thì phải thông báo cho Ngân hàng Nhà nước Việt Nam (Thanh tra Ngân hàng Nhà nước, Vụ Các Ngân hàng, Cục Công nghệ tin học ngân hàng, Ngân hàng Nhà nước chi nhánh tỉnh, thành phố trực thuộc Trung ương nơi tổ chức tín dụng có phần đặt trụ sở chính) về những nội dung thay đổi đó.

Điều 18. Báo cáo

1. Chậm nhất vào ngày 20 tháng 01 và ngày 20 tháng 7 hàng năm, tổ chức tín dụng phải gửi báo cáo đến Ngân hàng Nhà nước Việt Nam (Thanh tra Ngân hàng Nhà nước, Vụ Các Ngân hàng, Ngân hàng Nhà nước chi nhánh tỉnh, thành phố

trực thuộc Trung ương nơi tổ chức tín dụng cổ phần đặt trụ sở chính) về hoạt động ngân hàng điện tử và đánh giá về kết quả kiểm soát, xử lý rủi ro đối với hoạt động ngân hàng điện tử trong 06 tháng đầu năm và cả năm.

2. Báo cáo cần phải đảm bảo những nội dung sau:

a) Các sản phẩm, dịch vụ ngân hàng điện tử hiện đang cung ứng;

b) Các bên thứ ba được thuê hoặc cùng hợp tác thực hiện hoạt động ngân hàng điện tử; các hoạt động ngân hàng điện tử có sự tham gia của bên thứ ba và hình thức tham gia của các bên thứ ba này;

c) Số lượng khách hàng sử dụng dịch vụ ngân hàng điện tử và tỷ lệ tăng trưởng khách hàng so với cùng kỳ năm trước;

d) Doanh số hoạt động ngân hàng điện tử;

d) Những sự cố đã phát sinh trong kỳ. Sự cố được báo cáo theo 04 nhóm rủi ro như quy định tại Chương II Quy định này, các thiệt hại và biện pháp xử lý đã áp dụng.

Điều 19. Trách nhiệm của các đơn vị thuộc Ngân hàng Nhà nước

1. Thanh tra Ngân hàng Nhà nước:

a) Thực hiện thanh tra, giám sát việc tuân thủ các nguyên tắc về quản lý rủi ro trong hoạt động ngân hàng điện tử của tổ chức tín dụng theo thẩm quyền.

b) Xử lý theo thẩm quyền và kiến nghị Thống đốc Ngân hàng Nhà nước xử lý các trường hợp vi phạm Quy định này và các quy định khác của pháp luật hiện hành.

2. Ngân hàng Nhà nước chi nhánh tỉnh, thành phố trực thuộc Trung ương:

Thực hiện thanh tra, kiểm tra việc tuân thủ các nguyên tắc về quản lý rủi ro trong hoạt động ngân hàng điện tử của tổ chức tín dụng cổ phần trên địa bàn và xử lý các trường hợp vi phạm theo thẩm quyền.

3. Vụ Các Ngân hàng và tổ chức tín dụng phi ngân hàng:

a) Nghiên cứu, trình Thống đốc Ngân hàng Nhà nước xem xét, sửa đổi bổ sung những quy định về quản lý rủi ro trong hoạt động ngân hàng điện tử tại Quy định này.

b) Phối hợp với Thanh tra Ngân hàng Nhà nước giám sát việc tuân thủ các quy định về quản lý rủi ro trong hoạt động ngân hàng điện tử của các tổ chức tín dụng.

4. Cục Công nghệ tin học ngân hàng:

Phối hợp với Thanh tra Ngân hàng Nhà nước để kiểm tra việc tuân thủ các quy định về quản lý rủi ro trong hoạt động ngân hàng điện tử của các tổ chức tín dụng./.

**KT. THÔNG ĐỌC
PHÓ THÔNG ĐỌC**

Đặng Thanh Bình