NGÂN HÀNG NHÀ NƯỚC
Số: 35/2006/QĐ-NHNN

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

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

THỐNG ĐỐC 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. THỐNG ĐỐC
PHÓ THỐNG ĐỐC

(Đã ký)

Đặng Thanh Bình

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

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

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:

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

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.

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.

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

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

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.

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:

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.

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

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.

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

Xác định mức độ rủi ro tối đa mà tổ chức tín dụng có thể chấp nhận được;

Trách nhiệm cụ thể của từng phòng, ban tham gia hoạt động ngân hàng điện tử;

Quy định chế độ báo cáo định kỳ và báo cáo đột xuất khi xảy ra sự cố;

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;

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:

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.

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

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

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

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, xoá 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 xoá bỏ, thay đổi cơ sở dữ liệu và người thực hiện việc xoá bỏ, thay đổi đó phải được lưu lại để phục vụ công tác kiểm tra, kiểm soát.

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;