QUẢN LÝ RỦI RO DOANH NGHIỆP THEO BỘ TIÊU CHUẨN ISO/IEC 27000

ThS. Nguyễn Thị Xuân

Tổ NCPT An toàn thông tin

Tóm tắt: *Trong bối cảnh công nghệ thông tin phát triển như vũ bão, hầu hết các tổ chức, doanh nghiệp hoạt động lệ thuộc gần như hoàn toàn vào mạng máy tính và cơ sở dữ liệu. Vấn đề đặt ra ở đây là rủi ro trong tổ chức, doanh nghiệp sẽ được quản lý như thế nào. Một biện pháp quản lý rủi ro hiệu quả đó là tuân thủ hướng dẫn quản lý rủi ro trong bộ tiêu chuẩn quốc tế ISO/IEC 27000. Trong bộ tiêu chuẩn trên, có 2 tiêu chuẩn đề cập tới vấn đề quản lý rủi ro: Tiêu chuẩn ISO/IEC 27001 chỉ rõ những yêu cầu đối với hoạt động thiết lập; triển khai; điều hành; giám sát; soát xét; bảo trì và nâng cấp một ISMS để đảm bảo an toàn thông tin trước những rủi ro có thể xảy ra với tổ chức. Còn ISO/IEC 27005 là hướng dẫn quản lý rủi ro an ninh thông tin được thiết kế nhằm hỗ trợ triển khai an toàn thông tin một cách thỏa đáng dựa trên phương thức tiếp cận quản lý rủi ro.*

1. GIỚI THIỆU

Có thể nói rằng bộ ISO 27000 là một phần của hệ thống quản lý chung trong tổ chức, được thực hiện dựa trên nguyên tắc tiếp cận các rủi ro trong hoạt động, để thiết lập, áp dụng, thực hiện, theo dõi, xem xét, duy trì và cải tiến đảm bảo an toàn thông tin của tổ chức.

Bộ tiêu chuẩn ISO/IEC 27000 ra đời đánh dấu một bước phát triển trong lĩnh vực quản lý bảo mật hệ thống thông tin. Nó có thể áp dụng được cho các tổ chức với quy mô và loại hình khác nhau. Việc áp dụng mô hình hệ thống quản lý an ninh thông tin (ISMS), đánh giá các rủi ro an toàn thông tin trong tổ chức, sau đó triển khai các biện pháp quản lý an toàn thông tin sẽ giúp cho các tổ chức kiến trúc một mô hình quản lý hệ thống tiên tiến với những giải pháp an ninh tổng thể, chi phí hợp lý và hiệu quả.

2. SƠ LƯỢC VỀ BỘ TIÊU CHUẨN ISO/IEC 27000

Tiền thân là BS 7799 - chuẩn về an ninh thông tin do Viện Tiêu chuẩn Anh quốc (British Standard Institude) phát hành lần đầu năm 1995.

Tháng 10/2000, tổ chức Tiêu chuẩn hóa quốc tế (ISO) đã tiếp nhận BS 7799, chỉnh sửa và xuất bản dưới tên gọi ISO/IEC 17799:2000; 17799 được chỉnh sửa và bổ sung năm 2005, sau đó đổi tên thành bộ ISO/IEC 27000.

Từ năm 2005 đến nay, bộ tiêu chuẩn ISO/IEC 27000 liên tục được cập nhật. Hiện nay đã có 16 tiêu chuẩn trong bộ tiêu chuẩn này đã được ban hành, và một số khác hiện đang được xây dựng:

- ISO/IEC 27000:2012 - Information security management systems - Overview and vocabulary: tiêu chuẩn về các nguyên tắc và từ vựng.
- ISO/IEC 27001:2013 - Information security management systems - Requirements: tiêu chuẩn về các yêu cầu hệ thống quản lý thông tin.
- ISO/IEC 27002:2013 - Code of practice for information security management: tiêu chuẩn về mã thực hành hệ thống quản lý an ninh thông tin.
- ISO/IEC 27003:2010 - Information security management system implementation guidance: tiêu chuẩn về hướng dẫn áp dụng hệ thống quản lý an ninh thông tin.
- ISO/IEC 27004:2009 - Information security management - Measurement: tiêu chuẩn về đo lường hệ thống quản lý an ninh thông tin.
- ISO/IEC 27005:2011 - Information security risk management: tiêu chuẩn về

quản lý rủi ro hệ thống quản lý an ninh thông tin.

- ISO/IEC 27006:2011 - Requirements for bodies providing audit and certification of information security management systems: dành cho các tổ chức đánh giá và chứng nhận ISMS.
- ISO/IEC 27007:2011 Information technology - Security techniques - Guidelines for information security management systems auditing: tiêu chuẩn về hướng dẫn kiểm toán các hệ thống quản lý an ninh thông tin.
- IEC TR 27008:2011 - Guidelines for auditors on information security management systems controls: hướng dẫn cho kiểm toán viên về các biện pháp điều khiển hệ thống quản lý an ninh thông tin.
- ISO/IEC 27010:2012 - Information security management for inter-sector and inter-organisational communications: quản lý an ninh thông tin cho ngành truyền thông nội bộ
- ISO/IEC 27011:2008 - Information security management guidelines for telecommunications organizations based on ISO/IEC 27002: hướng dẫn quản lý an ninh thông tin cho tổ chức viễn thông dựa trên 27002.
- ISO/IEC 27031:2011 Guidelines for information and communications technology readiness for business continuity: hướng dẫn sẵn sàng công nghệ thông tin và truyền thông cho liên tục doanh nghiệp.
- ISO/IEC 27033-1:2009 - Network security overview and concepts: tổng quan và khái niệm an ninh mạng.
- ISO/IEC 27034-1:2011 - Information technology - Security techniques - Application security - Overview and concepts: công nghệ thông tin - kỹ thuật an ninh - an ninh ứng dụng - Tổng quan và khái niệm.
- ISO/IEC 27035:2011 - Information security incident management: quản lý sự cố an ninh thông tin.
- ISO 27799:2008 - Information security management in health using ISO/IEC 27002: quản lý an ninh thông tin trong lĩnh vực y tế sử dụng 27002.
- …

3. QUẢN LÝ RỦI RO DOANH NGHIỆP TUÂN THEO CHUẨN ISO/IEC 27000

Trong bộ tiêu chuẩn trên, tiêu chuẩn ISO/IEC 27001 chính là những yêu cầu bắt buộc đối với tổ chức khi xây dựng, vận hành và duy trì ISMS. Các tiêu chuẩn khác được coi như những hướng dẫn chi tiết cho tiêu chuẩn ISO/IEC 27001.

Xét về khía cạnh quản lý rủi ro, tiêu chuẩn ISO/IEC 27001 chỉ rõ những yêu cầu đối với hoạt động thiết lập; triển khai; điều hành; giám sát; soát xét; bảo trì và nâng cấp một ISMS để đảm bảo an toàn thông tin trước những rủi ro có thể xảy ra với tổ chức. Còn ISO/IEC 27005 là hướng dẫn quản lý rủi ro an ninh thông tin được thiết kế nhằm hỗ trợ triển khai an toàn thông tin một cách thỏa đáng dựa trên phương thức tiếp cận quản lý rủi ro.

3.1. Quản lý rủi ro chỉ ra trong ISO/IEC 27001

a) Xác định các rủi ro:

- Xác định tất cả các tài sản (assets) trong phạm vi hệ thống ISMS và đối tượng quản lý các tài sản này.
- Xác định các mối đe doạ (threats) đối với tài sản.
- Xác định các điểm yếu (vulnerabilities) có thể bị khai thác bởi các mối đe doạ trên.
- Xác định các tác động (impacts) làm mất tính chất bí mật, toàn vẹn và sẵn sàng của tài sản.

b) Phân tích và ước lượng rủi ro:

- Đánh giá các ảnh hưởng tới hoạt động của tổ chức có thể gây ra do sự cố về an toàn thông tin, chú ý đến các hậu quả của việc mất tính bí mật, toàn vẹn hay sẵn sàng của các tài sản.
- Đánh giá các khả năng thực tế có thể xảy ra sự cố an toàn thông tin bắt nguồn từ các mối đe dọa và nguy cơ đã dự đoán. Đồng thời đánh giá các tác động tới tài sản và các biện pháp bảo vệ đang thực hiện.
- Ước đoán các mức độ của rủi ro.
- Xác định rủi ro là chấp nhận được hay phải có biện pháp xử lý dựa trên các tiêu chí chấp nhận rủi ro đã được thiết lập trong mục 4.2.1.c.2.

c) Xác định và đánh giá các lựa chọn cho việc xử lý rủi ro:

- Áp dụng các biện pháp quản lý thích hợp.
- Chấp nhận rủi ro với điều kiện chúng hoàn toàn thỏa mãn các chính sách và tiêu chí chấp nhận rủi ro của tổ chức.
- Tránh các rủi ro.
- Chuyển giao các rủi ro các bộ phận khác (như bảo hiểm, nhà cung cấp...).

3.2. Quản lý rủi ro chỉ ra trong ISO/IEC 27005

Tiến trình quản lý rủi ro bao gồm các bước sau:

- Thiết lập ngữ cảnh
- Đánh giá rủi ro an toàn thông tin
- Ước tính/ ước lượng rủi ro
- Xử lý rủi ro
- Chấp nhận rủi ro
- Tài liệu hóa/ truyền thông và tư vấn rủi ro
- Giám sát và soát xét rủi ro

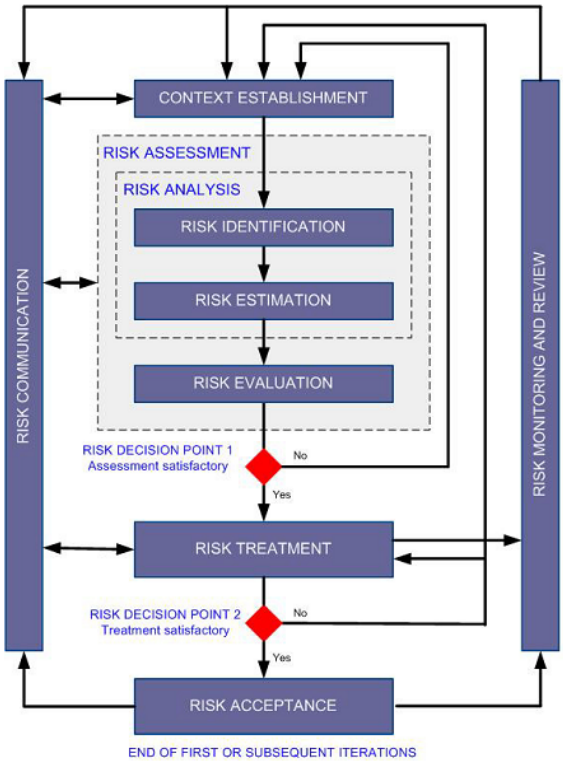

Figure 1 — Information security risk management process

Hình 1. Quy trình quản lý rủi ro an ninh thông tin

Ngoài ra có các phụ lục A đến G là các chỉ dẫn và ví dụ cụ thể cho các nội dung đánh giá đã nêu trong quy trình trên.

4. KẾT LUẬN

Với việc áp dụng chuẩn ISO/IEC 27001 và 27005 vào quản lý rủi ro an ninh thông tin trong doanh nghiệp, yêu cầu tổ chức, doanh nghiệp cần tiến hành khảo sát hiện trạng hệ thống, xác định tất cả các tài sản trong phạm vi ISMS: Liệt kê tất cả các tài sản (mô hình thiết kế, thành phần chức năng, quy trình nghiệp vụ,…). Sau đó tiến hành phân tích lượng hóa rủi ro, đánh giá rủi ro và lựa chọn các phương án xử lý rủi ro đối với tài sản của tổ chức: Xác định giá trị, những rủi ro xuất hiện (rủi ro về sở hữu tài sản, những điểm yếu, các mối đe dọa, mất độ tin cậy, tính toàn vẹn, tính sẵn sàng).

5. TÀI LIỆU THAM KHẢO:

1. *ISO/IEC 27000:2009* - Information technology - Security techniques - *Information security management systems - Overview and vocabulary.*
2. *ISO/IEC 27001:2005 - Information technology - Security techniques Information security management systems – Requirements.*
3. *ISO/IEC 27005:2011 - Information technology - Security techniques Information security risk management.*

Thông tin tác giả: **Nguyễn Thị Xuân**

Năm sinh: 1979

Lý lịch khoa học:

- Tốt nghiệp Đại học Công nghệ thông tin, trường Đại học Công nghệ, Đại học Quốc gia Hà Nội năm 2001.
- Tốt nghiệp Cao học Công nghệ thông tin, trường Đại học Công nghệ, Đại học Quốc gia Hà Nội năm 2008.
- Hiện đang công tác tại tổ Nghiên cứu Phát triển An toàn thông tin thuộc Viện công nghệ Thông tin và Truyền thông – CDiT, Học viện Công nghệ Bưu chính Viễn thông.

Lĩnh vực nghiên cứu hiện nay: Tiêu chuẩn quản lý an toàn hệ thống thông tin, giải pháp và công nghệ bảo mật.

Email: xuannt@ptit.edu.vn ; xuannt@cdit.com.vn