TCVN TIÊU CHUẨN QUỐC GIA

TCVN ISO/IEC 27001:2009
ISO/IEC 27001:2005

CÔNG NGHỆ THÔNG TIN - HỆ THỐNG QUẢN LÝ AN TOÀN THÔNG TIN - CÁC YÊU CẦU

Information technology – Information security management system - Requirements

HÀ NỘI – 2009

Mục lục

Lời nói đầu

TCVN ISO/IEC 27001:2009 hoàn toàn tương đương với ISO/IEC 27001:2005.

TCVN ISO/IEC 27001:2009 do Trung tâm Ứng cứu khẩn cấp Máy tính Việt Nam biên soạn, Bộ Thông tin và Truyền thông đề nghị, Tổng cục Tiêu chuẩn Đo lường Chất lượng thẩm định, Bộ Khoa học và Công nghệ công bố.

Công nghệ thông tin - Hệ thống quản lý an toàn thông tin – Các yêu cầu

Information technology – Information security management system - Requirements

1 Phạm vi áp dụng

Tiêu chuẩn này áp dụng rộng rãi cho nhiều loại hình tổ chức (ví dụ: các tổ chức thương mại, cơ quan nhà nước, tổ chức phi lợi nhuận). Tiêu chuẩn này chỉ rõ yêu cầu đối với hoạt động thiết lập; triển khai; điều hành; giám sát; soát xét; duy trì và cải tiến một hệ thống quản lý an toàn thông tin (ISMS) để đảm bảo an toàn thông tin trước những rủi ro có thể xảy ra với các hoạt động của tổ chức. Tiêu chuẩn này cũng chỉ rõ các yêu cầu khi triển khai các biện pháp quản lý an toàn đã được chọn lọc phù hợp với nhu cầu của tổ chức hoặc bộ phận của tổ chức.

Hệ thống ISMS được thiết kế các biện pháp đảm bảo an toàn thông tin phù hợp và đầy.đủ để bảo vệ các tài sản thông tin và đem lại sự tin tưởng của các bên liên quan như đối tác, khách hàng...

Các yêu cầu trình bày trong tiêu chuẩn này mang tính tổng quát và nhằm ứng dụng rộng rãi cho nhiều loại hình tổ chức khác nhau. Điều 4, 5, 6, 7 và 8 của tiêu chuẩn là bắt buộc nếu tổ chức công bố phù hợp với tiêu chuẩn này; các loại trừ đối với các biện pháp quản lý, nếu cần thiết để thoả mãn các tiêu chí chấp nhận rủi ro, cần có lý do chính đáng và có bằng chứng chứng minh các rủi ro liên đới đã được chấp nhận bởi người có trách nhiệm.

2 Tài liệu viện dẫn

ISO/IEC 17799:2005, Information technology – Security techniques – Code of practice for information security management *(Công nghệ thông tin – Các kỹ thuật an toàn – Quy phạm thực hành quản lý an toàn thông tin).*

3 Thuật ngữ và định nghĩa

Tiêu chuẩn này sử dụng các thuật ngữ và định nghĩa sau:

3.1

Tài sản (asset)

Bất kỳ thứ gì có giá trị đối với tổ chức.

3.2

Tính sẵn sàng (availability)

Tính chất đảm bảo mọi thực thể được phép có thể truy cập và sử dụng theo yêu cầu.

3.3

Tính bảo mật (confidentiality)

Tính chất đảm bảo thông tin không sẵn sàng và phơi bày trước cá nhân, thực thể và các tiến trình không được phép.

3.4

An toàn thông tin (information security)

Sự duy trì tính bảo mật, tính toàn vẹn và tính sẵn sàng của thông tin; ngoài ra còn có thể bao hàm một số tính chất khác như xác thực, kiểm soát được, không từ chối và tin cậy.

3.5

Sự kiện an toàn thông tin (information security event)

Một sự kiện đã được xác định trong một hệ thống, dịch vụ hay trạng thái mạng chỉ ra khả năng vi phạm chính sách an toàn thông tin, sự thất bại của hệ thống bảo vệ, hoặc một vấn đề chưa biết gây ảnh hưởng đến an toàn thông tin.

3.6

Sự cố an toàn thông tin (information security incident)

Một hoặc một chuỗi các sự kiện an toàn thông tin không mong muốn có khả năng làm tổn hại các hoạt động của cơ quan tổ chức và đe dọa an toàn thông tin.

3.7

Hệ thống quản lý an toàn thông tin (information security management system)

ISMS

Hệ thống quản lý an toàn thông tin là một phần của hệ thống quản lý toàn diện, dựa trên các rủi ro có thể xuất hiện trong hoạt động của tổ chức để thiết lập, triển khai, điều hành, giám sát, soát xét, duy trì và cải tiến an toàn thông tin.

CHÚ THÍCH: Hệ thống quản lý toàn diện bao gồm cơ cấu, chính sách, kế hoạch hoạt động, trách nhiệm, quy định, thủ tục, quy trình và tài nguyên của tổ chức.

3.8

Tính toàn vẹn (integrity)

Tính chất đảm bảo sự chính xác và đầy đủ của các tài sản.

3.9

Rủi ro tồn đọng (residual risk)

Rủi ro còn lại sau quá trình xử lý rủi ro.

3.10

Chấp nhận rủi ro (risk acceptance)

Quyết định chấp nhận rủi ro.

3.11

Phân tích rủi ro (risk analysis)

Sử dụng thông tin một cách có hệ thống nhằm xác định các nguồn gốc và ước đoán rủi ro.

3.12

Đánh giá rủi ro (risk assessment)

Quá trình tổng thể gồm phân tích rủi ro và ước lượng rủi ro.

3.13

Ước lượng rủi ro (risk evaluation)

Quá trình so sánh rủi ro đã ước đoán với chỉ tiêu rủi ro đã có nhằm xác định mức độ nghiêm trọng của rủi ro.

3.14

Quản lý rủi ro (risk management)

Các hoạt động phối hợp nhằm điều khiển và quản lý một tổ chức trước các rủi ro có thể xảy ra.

3.15

Xử lý rủi ro (risk treatment)

Quá trình lựa chọn và triển khai các biện pháp hạn chế rủi ro.

3.16

Thông báo áp dụng (statement of applicability)

Thông báo bằng văn bản mô tả mục tiêu quản lý và biện pháp quản lý thích hợp áp dụng cho hệ thống ISMS của tổ chức.

CHÚ THÍCH: Các mục tiêu quản lý và biện pháp quản lý được xây dựng dựa trên kết quả của các quá trình đánh giá rủi ro và xử lý rủi ro, các yêu cầu về pháp lý hoặc quy định, các nghĩa vụ trong hợp đồng và các yêu cầu về nghiệp vụ của tổ chức để đảm bảo an toàn thông tin.

4 Hệ thống quản lý an toàn thông tin

4.1 Các yêu cầu chung

Tổ chức phải thiết lập, triển khai, điều hành, giám sát, soát xét, duy trì và cải tiến một hệ thống quản lý an toàn thông tin (ISMS) đã được tài liệu hóa trong bối cảnh các hoạt động nghiệp vụ chung của tổ chức và những rủi ro phải đối mặt.

4.2 Thiết lập và quản lý hệ thống ISMS

4.2.1 Thiết lập hệ thống ISMS

Để thiết lập hệ thống ISMS, tổ chức cần thực hiện như sau:

a) Xác định phạm vi và các giới hạn của hệ thống ISMS theo đặc thù công việc, tổ chức, địa điểm, tài sản và công nghệ. Khi loại trừ các biện pháp quản lý khỏi phạm vi áp dụng (xem 1) cần phải đưa ra lý do và các thông tin chi tiết.

b) Xây dựng và hoạch định chính sách ISMS theo đặc thù công việc, tổ chức. địa điểm, tài sản và công nghệ. Chính sách này:

1) bao gồm khuôn khổ để xây dựng các mục tiêu và thiết lập một định hướng và nguyên tắc chung cho các hành động đảm bảo an toàn thông tin;
2) tuân thủ quy định pháp lý, các yêu cầu nghiệp vụ và cam kết về an toàn thông tin đã có;
3) thiết lập và duy trì hệ thống ISMS như một phần trong chiến lược quản lý rủi ro chung của tổ chức;
4) thiết lập tiêu chí xác định các rủi ro sẽ được ước lượng (xem 4.2.1c);
5) cần phải được ban quản lý phê duyệt.

CHÚ THÍCH: trong tiêu chuẩn này, chính sách ISMS được xem xét như là một danh mục đầy đủ các chính sách an toàn thông tin. Các chính sách này có thể được mô tả trong cùng một tài liệu.

c) Xác định phương pháp tiếp cận đánh giá rủi ro của tổ chức.

1) Xác định hệ phương pháp đánh giá rủi ro phù hợp với hệ thống ISMS và các quy định, luật pháp, yêu cầu và cam kết đã có cần phải tuân thủ.
2) Xây dựng các tiêu chí cho việc chấp nhận rủi ro và vạch rõ các mức rủi ro có thể chấp nhận được (xem 5.1f).

Hệ phương pháp đánh giá rủi ro được lựa chọn phải đảm bảo các đánh giá rủi ro đưa ra các kết quả có thể so sánh và tái tạo được.

CHÚ THÍCH: Có nhiều hệ phương pháp đánh giá rủi ro khác nhau. Ví dụ về các hệ phương pháp đánh giá rủi ro được nêu ra trong tài liệu ISO/IEC TR 13335-3 "Information technology – Guidelines for the management of IT Security – Techniques for the management of IT Security".

d) Xác định các rủi ro.

1) Xác định tất cả các tài sản trong phạm vi hệ thống ISMS và *đối tượng quản lý* [1] các tài sản này.

2) Xác định các mối đe doạ đối với tài sản.

3) Xác định các điểm yếu có thể bị khai thác bởi các mối đe doạ trên.

4) Xác định các tác động làm mất tính chất bí mật, toàn vẹn và sẵn sàng của tài sản.

e) Phân tích và ước lượng các rủi ro.

1) 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 bảo mật, toàn vẹn hay sẵn sàng của các tài sản.

2) 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 điểm yếu đã dự đoán. Đồng thời đánh giá các tác động tới tài sản và các biện pháp bảo vệ đang thực hiện.

3) Ước đoán các mức độ của rủi ro.

4) 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 4.2.1.c)2.

f) Xác định và đánh giá các lựa chọn cho việc xử lý rủi ro.

Các hành động có thể thực hiện bao gồm:

1) áp dụng các biện pháp quản lý thích hợp;

2) 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 (xem 4.2.1c)2);

3) tránh các rủi ro;

4) chuyển giao các rủi ro các bên tham gia khác, như bảo hiểm, nhà cung cấp...

g) Lựa chọn các mục tiêu quản lý và biện pháp quản lý để xử lý các rủi ro.

Các mục tiêu quản lý và biện pháp quản lý phải được lựa chọn và thực hiện để đáp ứng các yêu cầu được xác định bởi quá trình đánh giá rủi ro và xử lý rủi ro. Việc lựa chọn này phải xem xét đến tiêu chí chấp nhận rủi ro (xem 4.2.1c)2) cũng như các yêu cầu về pháp lý, quy định và cam kết phải tuân thủ.

Các mục tiêu quản lý và biện pháp quản lý trong Phụ lục A có thể được lựa chọn như là một phần thích hợp để bảo đảm các yêu cầu đã xác định.

Các yêu cầu quản lý và biện pháp quản lý trong Phụ lục A là chưa thực sự đầy đủ. Tùy trường hợp có thể lựa chọn thêm các mục tiêu quản lý và biện pháp quản lý cần thiết khác.

[1] Thuật ngữ "đối tượng quản lý" trong ngữ cảnh này dùng để chỉ một cá nhân hay thực thể đã phê chuẩn trách nhiệm quản lý trong việc điều khiển sản xuất, phát triển, duy trì, sử dụng và đảm bảo an toàn của tài sản. Thuật ngữ này không dùng để chỉ những người có quyền sở hữu tài sản.

CHÚ THÍCH: Phụ lục A là một danh sách toàn diện các mục tiêu quản lý và biện pháp quản lý có khả năng thích hợp đối với nhiều tổ chức. Người sử dụng tiêu chuẩn này có thể sử dụng Phụ lục A như là điểm khởi đầu trong việc lựa chọn biện pháp quản lý để đảm bảo không có các biện pháp quan trọng bị bỏ sót.

h) Trình ban quản lý phê chuẩn các rủi ro tồn đọng đã đề xuất.

i) Trình ban quản lý cho phép triển khai và vận hành hệ thống ISMS.

j) Chuẩn bị thông báo áp dụng.

Thông báo áp dụng hệ thống ISMS bao gồm:

1) các mục tiêu quản lý và biện pháp quản lý đã được lựa chọn trong 4.2.1g) và lý do cho các lựa chọn này;

2) các mục tiêu quản lý và biện pháp quản lý đang được thực hiện (xem 4.2.1e)2));

3) các mục tiêu quản lý và biện pháp quản lý trong Phụ lục A đã loại trừ và giải trình cho việc loại trừ này.

CHÚ THÍCH: Thông báo áp dụng cung cấp thông tin tóm tắt về các quyết định liên quan đến việc xử lý rủi ro. Việc giải trình các biện pháp và mục tiêu quản lý trong Phụ lục A đã được loại trừ giúp cho phép kiểm tra chéo, tránh khả năng bỏ sót.

4.2.2 Triển khai và điều hành hệ thống ISMS

Quá trình triển khai và điều hành hệ thống ISMS cần thực hiện như sau:

a) Lập kế hoạch xử lý rủi ro trong đó xác định các hành động quản lý thích hợp, các tài nguyên, các trách nhiệm và mức độ ưu tiên quản lý các rủi ro an toàn thông tin (xem 5).

b) Triển khai kế hoạch xử lý rủi ro nhằm đạt được mục tiêu quản lý đã xác định trong đó bao gồm cả việc xem xét kinh phí đầu tư cũng như phân bổ các vai trò, trách nhiệm.

c) Triển khai các biện pháp quản lý được lựa chọn trong 4.2.1g) để đáp ứng các mục tiêu quản lý.

d) Xác định cách đánh giá hiệu lực của các biện pháp quản lý hoặc nhóm các biện pháp quản lý đã lựa chọn và chỉ ra các phương pháp đánh giá này sẽ được sử dụng như thế nào trong việc đánh giá hiệu lực của các biện pháp quản lý nhằm tạo ra những kết quả có thể so sánh được và tái tạo được (xem 4.2.3c).

CHÚ THÍCH: Việc đánh giá hiệu lực của các biện pháp quản lý đã lựa chọn cho phép người quản lý và nhân viên xác định các biện pháp quản lý đã đạt được mục tiêu quản lý theo kế hoạch như thế nào.

e) Triển khai các chương trình đào tạo nâng cao nhận thức (xem 5.2.2).

f) Quản lý hoạt động của hệ thống ISMS.

g) Quản lý các tài nguyên dành cho hệ thống ISMS (xem 5.2).

h) Triển khai các thủ tục và các biện pháp quản lý khác có khả năng nhanh chóng phát hiện các sự kiện an toàn thông tin và phản ứng với các sự cố an toàn thông tin (xem 4.2.3a)).

4.2.3 Giám sát và soát xét hệ thống ISMS

Tổ chức thực hiện các hành động sau đây:

a) Tiến hành giám sát, soát xét các thủ tục và các biện pháp quản lý khác nhằm:

1) nhanh chóng phát hiện ra các lỗi trong kết quả xử lý;
2) nhanh chóng xác định các tấn công, lỗ hổng và sự cố an toàn thông tin;
3) cho phép ban quản lý xác định các hoạt động an toàn thông tin giao cho người hoặc thực hiện bằng công nghệ thông tin đã được thực hiện như mong muốn;
4) hỗ trợ phát hiện các sự kiện an toàn thông tin và do đó ngăn chặn sớm các sự cố an toàn thông tin bằng cách sử dụng các dấu hiệu cần thiết;
5) xác định hiệu lực của các hành động xử lý vi phạm an toàn thông tin đã thực hiện.

b) Thường xuyên soát xét hiệu lực của hệ thống ISMS (bao gồm việc đáp ứng các chính sách và mục tiêu quản lý của ISMS, và soát xét việc thực hiện các biện pháp quản lý an toàn thông tin) trong đó xem xét đến các kết quả kiểm toán an toàn thông tin, các sự cố đã xảy ra, các kết quả đánh giá hiệu lực, các đề xuất và thông tin phản hồi thu thập được từ các bên liên quan.

c) Đánh giá hiệu lực của các biện pháp quản lý để xác minh các yêu cầu về an toàn thông tin đã được đáp ứng.

d) Soát xét các đánh giá rủi ro đã tiến hành theo kế hoạch và soát xét các rủi ro tồn đọng cũng như mức độ rủi ro có thể chấp nhận được. Trong đó lưu ý các thay đổi trong:

1) tổ chức;
2) công nghệ;
3) mục tiêu và các quá trình nghiệp vụ;
4) các mối đe doạ an toàn thông tin đã xác định;
5) hiệu lực của các biện pháp quản lý đã thực hiện;
6) các sự kiện bên ngoài, như thay đổi trong môi trường pháp lý hay quy định, thay đổi trong các nghĩa vụ hợp đồng, thay đổi về hoàn cảnh xã hội.

e) Thực hiện việc kiểm toán nội bộ hệ thống ISMS một cách định kỳ (xem 6).

CHÚ THÍCH: Kiểm toán nội bộ đôi khi còn được gọi là kiểm toán của bên thứ nhất và được thực hiện bởi chính tổ chức hoặc đại diện của tổ chức.

f) Thực hiện soát xét của ban quản lý đối với hệ thống ISMS một cách thường xuyên để đảm bảo phạm vi đặt ra vẫn phù hợp và xác định các cải tiến cần thiết cho hệ thống ISMS (xem 7.1).

g) Cập nhật kế hoạch bảo đảm an toàn thông tin theo sát thay đổi của tình hình thực tế thu được qua

các hoạt động giám sát và đánh giá.

h) Ghi chép, lập tài liệu về các hành động và sự kiện có khả năng ảnh hưởng đến hiệu lực hoặc hiệu suất của hệ thống ISMS (xem 4.3.3).

4.2.4 Duy trì và cải tiến hệ thống ISMS

Tổ chức cần thường xuyên thực hiện:

a) Triển khai các cải tiến đã được xác định cho hệ thống ISMS.

b) Tiến hành các hành động khắc phục và phòng ngừa thích hợp (xem 8.2 và 8.3). Vận dụng kinh nghiệm đã có cũng như tham khảo từ các tổ chức khác.

c) Thông báo và thống nhất với các bên liên quan về các hành động và cải tiến của hệ thống ISMS.

d) Đảm bảo việc cải tiến phải đạt được các mục tiêu đã đặt ra.

4.3 Các yêu cầu về hệ thống tài liệu

4.3.1 Khái quát

Hệ thống tài liệu bao gồm các hồ sơ xử lý nhằm đảm bảo truy lại được các quyết định xử lý, chính sách và đảm bảo các kết quả đã ghi nhận là có thể tái tạo lại được.

Điều quan trọng là cần nêu rõ được sự liên quan giữa các biện pháp quản lý đã chọn với kết quả của các quy trình đánh giá và xử lý rủi ro cũng như với các chính sách và mục tiêu của hệ thống ISMS đã được đặt ra.

Hệ thống tài liệu của ISMS cần phải bao gồm:

a) các thông báo dạng văn bản về chính sách (xem 4.2.1b) và mục tiêu của hệ thống ISMS;

b) phạm vi của hệ thống ISMS (xem 4.2.1a);

c) các thủ tục và biện pháp quản lý hỗ trợ cho hệ thống ISMS;

d) mô tả về hệ phương pháp đánh giá rủi ro (xem 4.2.1c));

e) báo cáo đánh giá rủi ro (xem 4.2.1c) tới 4.2.1g));

f) kế hoạch xử lý rủi ro (xem 4.2.2b));

g) các thủ tục dạng văn bản cần thiết của tổ chức để đảm bảo hiệu quả của việc lập kế hoạch, điều hành và quản lý các quy trình bảo đảm an toàn thông tin và mô tả phương thức đánh giá hiệu lực của các biện pháp quản lý đã áp dụng (xem 4.2.3c);

h) các hồ sơ cần thiết được mô tả trong 4.3.3 của tiêu chuẩn này;

i) thông báo áp dụng.

CHÚ THÍCH 1: Cụm từ "thủ tục dạng văn bản" trong ngữ cảnh của tiêu chuẩn này có nghĩa là các thủ tục đã được thiết lập, biên soạn thành tài liệu, triển khai và duy trì.

CHÚ THÍCH 2: Quy mô của tài liệu về hệ thống ISMS giữa các tổ chức là khác nhau và phụ thuộc vào:

- quy mô và loại hình hoạt động của tổ chức;
- phạm vi và độ phức tạp của các yêu cầu an toàn thông tin và của hệ thống đang được quản lý.

CHÚ THÍCH 3: Các hồ sơ và tài liệu có thể được biểu diễn dưới bất kỳ hình thức và phương tiện nào phù hợp.

4.3.2 Biện pháp quản lý tài liệu

Các tài liệu cần thiết của hệ thống ISMS cần phải được bảo vệ và quản lý. Một thủ tục dạng văn bản phải được thiết lập để xác định các hành động quản lý cần thiết nhằm:

a) phê duyệt thoả đáng các tài liệu trước khi ban hành;

b) soát xét tài liệu và tiến hành các sửa đổi cần thiết để có thể phê duyệt lại;

c) đảm bảo nhận biết được các thay đổi và tình trạng sửa đổi hiện hành của tài liệu;

d) đảm bảo rằng các phiên bản tài liệu thích hợp luôn có sẵn ở nơi cần sử dụng;

e) đảm bảo rằng các tài liệu phải rõ ràng, dễ đọc và dễ nhận biết;

f) đảm bảo tài liệu phải sẵn sàng đối với người cần, được chuyển giao, lưu trữ và hủy bỏ theo các thủ tục phù hợp.

g) đảm bảo các tài liệu có nguồn gốc bên ngoài được nhận biết;

h) đảm bảo việc phân phối tài liệu phải được quản lý;

i) tránh việc vô tình sử dụng phải các tài liệu đã bị thay thế;

j) áp dụng các biện pháp định danh phù hợp đối với các tài liệu cần lưu trữ.

4.3.3 Biện pháp quản lý hồ sơ

Các hồ sơ phải được thiết lập và duy trì để cung cấp các dẫn chứng thể hiện sự phù hợp với các yêu cầu và sự hoạt động hiệu quả của hệ thống ISMS. Các hồ sơ phải được bảo vệ và quản lý. Hệ thống ISMS phải chú ý đến các yêu cầu về pháp lý hoặc quy định liên quan và các nghĩa vụ trong hợp đồng. Hồ sơ phải dễ đọc, dễ nhận biết và có thể truy xuất được. Các biện pháp quản lý cần thiết để định danh, lưu trữ, bảo vệ, truy xuất, định thời gian duy trì và sắp xếp hồ sơ phải được ghi thành văn bản và triển khai.

Các hồ sơ phải được lưu giữ khi thực hiện quy trình nêu tại 4.2 và trong các sự cố an toàn thông tin quan trọng liên quan đến hệ thống ISMS.

VÍ DỤ: hồ sơ là một quyển sách ghi chép về các khách đến, báo cáo kiểm toán...

5 Trách nhiệm của ban quản lý

5.1 Cam kết của ban quản lý

Ban quản lý phải chứng minh cam kết của mình trong việc thiết lập, triển khai, điều hành, giám sát,

soát xét, duy trì và cải tiến hệ thống quản lý an toàn thông tin bằng việc:

a) thiết lập chính sách cho hệ thống ISMS;

b) đảm bảo rằng các mục tiêu và kế hoạch của hệ thống ISMS đã được xây dựng;

c) thiết lập các vai trò và trách nhiệm về an toàn thông tin;

d) trao đổi với tổ chức về tầm quan trọng của việc đảm bảo các mục tiêu an toàn thông tin và việc tuân thủ các chính sách an toàn thông tin, các trách nhiệm trước pháp luật và sự cần thiết tiếp tục cải tiến;

e) cung cấp đầy đủ tài nguyên cho các quá trình thiết lập, triển khai, điều hành, giám sát, soát xét, duy trì và cải tiến hệ thống ISMS (xem 5.2.1);

f) xác định các tiêu chí chấp nhận rủi ro và mức độ rủi ro có thể chấp nhận được;

g) đảm bảo việc kiểm toán nội bộ hệ thống ISMS được thực hiện (xem 6);

h) triển khai việc soát xét của ban quản lý đối với hệ thống ISMS (xem 7).

5.2 Quản lý nguồn lực

5.2.1 Cấp phát nguồn lực

Tổ chức phải xác định và cung cấp các nguồn lực cần thiết cho việc:

a) thiết lập, triển khai, điều hành, giám sát, soát xét, duy trì và cải tiến hệ thống ISMS;

b) đảm bảo các thủ tục an toàn thông tin hỗ trợ cho các yêu cầu nghiệp vụ;

c) xác định và áp dụng các yêu cầu pháp lý, quy định và các nghĩa vụ về an toàn thông tin trong hợp đồng;

d) duy trì đầy đủ an toàn thông tin bằng cách áp dụng đúng tất cả các biện pháp quản lý đã được triển khai;

e) thực hiện soát xét và có các biện pháp xử lý khi cần thiết;

f) nâng cao hiệu lực của hệ thống ISMS khi cần thiết.

5.2.2 Đào tạo, nhận thức và năng lực

Tổ chức phải đảm bảo những người có trách nhiệm trong hệ thống ISMS phải có đầy đủ năng lực để thực hiện các nhiệm vụ được giao bằng cách:

a) xác định các kỹ năng cần thiết đối với nhân viên thực hiện các công việc có tác động đến hệ thống ISMS;

b) cung cấp các khóa đào tạo hoặc tuyển chọn người đã có năng lực để có thể thỏa mãn yêu cầu;

c) đánh giá mức độ hiệu quả của các hoạt động đã thực hiện;

d) lưu giữ hồ sơ về việc học vấn, quá trình đào tạo, các kỹ năng, kinh nghiệm và trình độ chuyên môn

(xem 4.3.3).

Tổ chức cũng cần đảm bảo rằng mọi cá nhân liên quan đều nhận thức được tầm quan trọng của các hoạt động đảm bảo an toàn thông tin và hiểu cách góp phần để đạt được các mục tiêu của hệ thống ISMS.

6 Kiểm toán nội bộ hệ thống ISMS

Tổ chức phải thực hiện kiểm toán nội bộ hệ thống ISMS theo kế hoạch để xác định các mục tiêu quản lý, biện pháp quản lý, quy trình, thủ tục trong hệ thống ISMS có:

a) tuân thủ các yêu cầu của tiêu chuẩn này và các quy định pháp lý liên quan;

b) tuân thủ các các yêu cầu đảm bảo an toàn thông tin đã xác định;

c) được triển khai và duy trì hiệu quả;

d) hoạt động diễn ra đúng như mong muốn.

Các chương trình kiểm toán phải được lên kế hoạch, có xem xét đến hiện trạng và tầm quan trọng của các quy trình và phạm vi được kiểm toán. Các tiêu chí, phạm vi, tần suất và phương pháp kiểm toán phải được xác định. Việc lựa chọn người tiến hành kiểm toán (kiểm toán viên) và việc thực hiện kiểm toán phải đảm bảo tính khách quan, công bằng cho quá trình kiểm toán. Kiểm toán viên không kiểm toán công việc của mình.

Các trách nhiệm và yêu cầu cho việc lập kế hoạch và thực hiện kiểm toán, báo cáo kết quả và lưu giữ hồ sơ (xem 4.3.3) phải được xác định trong một thủ tục dạng văn bản.

Ban quản lý chịu trách nhiệm cho phạm vi đang được kiểm toán phải đảm bảo thời gian trì hoãn để loại bỏ những điểm không phù hợp và nguyên nhân của chúng. Các hoạt động tiếp theo sẽ bao gồm việc thẩm tra các hoạt động đã thực hiện và lập báo cáo về kết quả thẩm tra này (xem 8).

CHÚ THÍCH: Tiêu chuẩn ISO 19011:2002, *"Guidelines for quality and/or environmental management systems auditing"* cung cấp hướng dẫn hữu ích cho việc triển khai kiểm toán nội bộ hệ thống ISMS.

7 Soát xét của ban quản lý đối với hệ thống ISMS

7.1 Khái quát

Ban quản lý phải soát xét hệ thống ISMS của tổ chức theo kế hoạch đã đặt ra (ít nhất một lần trong năm) để luôn đảm bảo tính phù hợp, đầy đủ và hiệu quả. Việc soát xét này bao gồm đánh giá khả năng có thể cải tiến và sự cần thiết phải thay đổi của hệ thống ISMS, bao gồm các chính sách an toàn thông tin và mục tiêu an toàn thông tin. Kết quả của việc soát xét phải được lập thành tài liệu rõ ràng và các hồ sơ phải được lưu giữ (xem 4.3.3).

7.2 Đầu vào của việc soát xét

Đầu vào cho ban quản lý tiến hành việc soát xét hệ thống ISMS bao gồm:

a) các kết quả kiểm toán và soát xét hệ thống ISMS;

b) thông tin phản hồi từ các bên liên quan;

c) các kỹ thuật, sản phẩm hoặc thủ tục có thể được sử dụng trong tổ chức nhằm nâng cao hiệu quả và hiệu suất của hệ thống ISMS;

d) hiện trạng của các hành động phòng ngừa và hành động khắc phục;

e) các lỗ hổng hoặc nguy cơ mất an toàn thông tin không được giải quyết thoả đáng trong lần đánh giá rủi ro trước;

f) các kết quả đánh giá hiệu lực của hệ thống;

g) các hoạt động tiếp theo lần soát xét trước của ban quản lý;

h) các thay đổi có ảnh hưởng đến hệ thống ISMS;

i) các kiến nghị nhằm cải tiến hệ thống.

7.3 Đầu ra của việc soát xét

Ban quản lý sau khi soát xét hệ thống ISMS cần đưa ra các quyết định và hành động liên quan sau đây:

a) Nâng cao hiệu lực của hệ thống ISMS.

b) Cập nhật kế hoạch đánh giá và xử lý rủi ro.

c) Sửa đổi các thủ tục và biện pháp quản lý cần thiết có ảnh hưởng đến an toàn thông tin nhằm đối phó lại với các sự kiện từ bên trong và bên ngoài có thể gây tác động đến hệ thống ISMS, bao gồm những thay đổi về:

1) các yêu cầu trong hoạt động nghiệp vụ;
2) các yêu cầu an toàn thông tin;
3) các quy trình nghiệp vụ có ảnh hưởng tới các yêu cầu trong hoạt động nghiệp vụ hiện tại của tổ chức;
4) các yêu cầu về pháp lý và quy định;
5) các nghĩa vụ theo các hợp đồng đã ký kết;
6) mức độ rủi ro và/hoặc tiêu chí chấp nhận rủi ro.

d) Các nhu cầu cần thiết về nguồn lực.

e) Cải tiến về phương thức đánh giá hiệu lực của các biện pháp quản lý.

8 Cải tiến hệ thống ISMS

8.1 Cải tiến thường xuyên

Tổ chức phải thường xuyên nâng cao tính hiệu lực của hệ thống ISMS thông qua việc sử dụng chính sách an toàn thông tin, các mục tiêu đảm bảo an toàn thông tin, các kết quả kiểm toán, kết quả phân tích các sự kiện đã giám sát, các hành động phòng ngừa và khắc phục cũng như các kết quả soát xét của ban quản lý (xem 7).

8.2 Hành động khắc phục

Tổ chức phải thực hiện hành động loại bỏ các nguyên nhân của các vi phạm đối với yêu cầu của hệ thống ISMS. Các thủ tục dạng văn bản cho các hành động khắc phục phải xác định rõ các yêu cầu đối với việc:

a) xác định các vi phạm;

b) tìm ra nguyên nhân của các vi phạm trên;

c) đánh giá sự cần thiết của các hành động ngăn chặn các vi phạm này xuất hiện trở lại;

d) quyết định và triển khai các hành động khắc phục cần thiết;

e) lập hồ sơ kết quả thực hiện các hành động trên (xem 4.3.3);

f) soát xét lại các hành động khắc phục đã thực hiện.

8.3 Hành động phòng ngừa

Tổ chức cần xác định các hành động để loại trừ các nguyên nhân gây ra các vi phạm tiềm ẩn đối với các yêu cầu của hệ thống ISMS để phòng ngừa các vi phạm này xảy ra. Các hành động phòng ngừa cần được thực hiện phù hợp với các tác động mà các vi phạm này có thể gây ra. Các thủ tục dạng văn bản cho các hành động phòng ngừa cần xác định rõ các yêu cầu đối với việc:

a) xác định các vi phạm tiềm ẩn và nguyên nhân gây ra chúng;

b) đánh giá sự cần thiết của các hành động ngăn chặn các vi phạm này xuất hiện;

c) quyết định và triển khai các hành động trên;

d) lập hồ sơ về kết quả của các hành động đã thực hiện (xem 4.3.3);

e) soát xét lại các hành động phòng ngừa đã thực hiện.

Tổ chức cần nhận biết các rủi ro đã thay đổi và xác định các hành động phòng ngừa phù hợp đáp ứng lại các thay đổi này. Mức ưu tiên của các hành động phòng ngừa phải được xác định dựa trên kết quả của quá trình đánh giá rủi ro.

CHÚ THÍCH: Hành động nhằm ngăn chặn các vi phạm thường hiệu quả và kinh tế hơn hành động khắc phục sự cố do các vi phạm gây ra.

Phụ lục A

(Quy định)

Các mục tiêu quản lý và biện pháp quản lý

Các mục tiêu và biện pháp quản lý trong bảng A.1 được xây dựng từ điều 5 đến 15 trong tiêu chuẩn quốc tế ISO/IEC 17799:2005. Nội dung trong bảng A.1 là chưa hoàn toàn đầy đủ nên tổ chức có thể tham khảo thêm các mục tiêu và biện pháp quản lý khác. Việc lựa chọn các mục tiêu và biện pháp quản lý trong bảng A.1 sẽ được coi như một phần trong quá trình thiết lập hệ thống ISMS (xem 4.2.1).

Điều 5 đến 15 trong tiêu chuẩn quốc tế ISO/IEC 17799:2005 cung cấp các khuyến cáo và hướng dẫn triển khai thực tế cho các biện pháp quản lý trong bảng A.1.

Bảng A.1 - Các mục tiêu và biện pháp quản lý

A.5 Chính sách an toàn		
A.5.1 Chính sách an toàn thông tin *Mục tiêu:* Nhằm cung cấp định hướng quản lý và hỗ trợ bảo đảm an toàn thông tin thỏa mãn với các yêu cầu trong hoạt động nghiệp vụ, môi trường pháp lý và các quy định phải tuân thủ.		
A.5.1.1	Tài liệu chính sách an toàn thông tin	*Biện pháp quản lý* Một tài liệu về chính sách an toàn thông tin cần phải được phê duyệt bởi ban quản lý và được cung cấp, thông báo tới mọi nhân viên cũng như các bên liên quan.
A.5.1.2	Soát xét lại chính sách an toàn thông tin	*Biện pháp quản lý* Chính sách an toàn thông tin cần thường xuyên được soát xét theo kế hoạch hoặc khi có những thay đổi lớn xuất hiện để luôn đảm bảo sự phù hợp, đầy đủ và thực sự có hiệu lực.
A.6 Tổ chức đảm bảo an toàn thông tin		
A.6.1 Tổ chức nội bộ *Mục tiêu:* Nhằm quản lý an toàn thông tin bên trong tổ chức.		
A.6.1.1	Cam kết của ban quản lý về bảo đảm an toàn thông tin	*Biện pháp quản lý* Ban quản lý phải chủ động hỗ trợ bảo đảm an toàn thông tin trong tổ chức bằng các định hướng rõ ràng, các cam kết có thể thấy được, các nhiệm vụ rõ ràng và nhận thức rõ trách nhiệm về bảo đảm an toàn thông tin.

A.6.1.2	Phối hợp bảo đảm an toàn thông tin	*Biện pháp quản lý* Các hoạt động bảo đảm an toàn thông tin cần phải được phối hợp bởi các đại diện của các bộ phận trong tổ chức với vai trò và nhiệm vụ cụ thể.
A.6.1.3	Phân định trách nhiệm bảo đảm an toàn thông tin	*Biện pháp quản lý* Tất cả các trách nhiệm bảo đảm an toàn thông tin cần phải được xác định một cách rõ ràng.
A.6.1.4	Quy trình trao quyền cho phương tiện xử lý thông tin	*Biện pháp quản lý* Một quy trình trao quyền quản lý cho phương tiện xử lý thông tin phải được xác định rõ và triển khai.
A.6.1.5	Các thỏa thuận về bảo mật	*Biện pháp quản lý* Các yêu cầu về bảo mật hoặc các thoả thuận không tiết lộ phản ánh nhu cầu của tổ chức đối với việc bảo vệ thông tin phải được xác định rõ và soát xét thường xuyên.
A.6.1.6	Liên lạc với những cơ quan/tổ chức có thẩm quyền	*Biện pháp quản lý* Phải duy trì liên lạc thoả đáng với các cơ quan có thẩm quyền liên quan.
A.6.1.7	Liên lạc với các nhóm chuyên gia	*Biện pháp quản lý* Phải giữ liên lạc với các nhóm chuyên gia hoặc các diễn đàn và hiệp hội an toàn thông tin.
A.6.1.8	Tự soát xét về an toàn thông tin	*Biện pháp quản lý* Cách tiếp cận quản lý an toàn thông tin của tổ chức và việc triển khai của tổ chức (chẳng hạn như: các mục tiêu và biện pháp quản lý, các chính sách, các quá trình và các thủ tục đảm bảo an toàn thông tin) phải được tự soát xét định kỳ hoặc khi xuất hiện những thay đổi quan trọng liên quan đến an toàn thông tin.
A.6.2 Các bên tham gia bên ngoài		
Mục tiêu: Nhằm duy trì an toàn đối với thông tin và các phương tiện xử lý thông tin của tổ chức được truy cập, xử lý, truyền tới hoặc quản lý bởi các bên tham gia bên ngoài tổ chức.		

A.6.2.1	Xác định các rủi ro liên quan đến các bên tham gia bên ngoài	*Biện pháp quản lý* Các rủi ro đối thông tin và phương tiện xử lý thông tin của tổ chức từ các quy trình nghiệp vụ liên quan đến các bên tham gia bên ngoài phải được nhận biết và triển khai biện pháp quản lý thích hợp trước khi cấp quyền truy cập.
A.6.2.2	Giải quyết an toàn khi làm việc với khách hàng	*Biện pháp quản lý* Tất cả các yêu cầu về an toàn phải được giải quyết trước khi cho phép khách hàng truy cập tới các tài sản hoặc thông tin của tổ chức.
A.6.2.3	Giải quyết an toàn trong các thỏa thuận với bên thứ ba	*Biện pháp quản lý* Các thỏa thuận với bên thứ ba liên quan đến truy cập, xử lý, truyền thông hoặc quản lý thông tin hay phương tiện xử lý thông tin của tổ chức, hoặc các sản phẩm, dịch vụ phụ trợ của các phương tiện xử lý thông tin phải bao hàm tất cả các yêu cầu an toàn liên quan.
A.7 Quản lý tài sản		
A.7.1 Trách nhiệm đối với tài sản *Mục tiêu:* Nhằm hoàn thành và duy trì các biện pháp bảo vệ thích hợp đối với tài sản của tổ chức.		
A.7.1.1	Kiểm kê tài sản	*Biện pháp quản lý* Mọi tài sản cần được xác định rõ ràng và cần thực hiện, duy trì việc kiểm kê mọi tài sản quan trọng.
A.7.1.2	Quyền sở hữu tài sản	*Biện pháp quản lý* Mọi thông tin và tài sản gắn với phương tiện xử lý thông tin phải được quản lý, kiểm soát bởi bộ phận được chỉ định của tổ chức.
A.7.1.3	Sử dụng hợp lý tài sản	*Biện pháp quản lý* Các quy tắc cho việc sử dụng hợp lý thông tin và tài sản gắn với phương tiện xử lý thông tin phải được xác định, ghi thành văn bản và triển khai.
A.7.2 Phân loại thông tin *Mục tiêu:* Nhằm đảm bảo thông tin sẽ có mức độ bảo vệ thích hợp.		

A.7.2.1	Hướng dẫn phân loại	*Biện pháp quản lý* Thông tin cần được phân loại theo giá trị, yêu cầu pháp lý, độ nhạy cảm và quan trọng đối với tổ chức.
A.7.2.2	Gán nhãn và quản lý thông tin	*Biện pháp quản lý* Các thủ tục cần thiết cho việc gán nhãn và quản lý thông tin cần được phát triển và triển khai phù hợp với lược đồ phân loại thông tin đã được tổ chức chấp nhận.
A.8 Đảm bảo an toàn tài nguyên con người		
***A.8.1 Trước khi tuyển dụng*[2]** *Mục tiêu:* Đảm bảo rằng các nhân viên, người của nhà thầu và bên thứ ba hiểu rõ trách nhiệm của mình và phù hợp với vai trò được giao, đồng thời giảm thiểu các rủi ro về việc đánh cắp, gian lận hoặc lạm dụng chức năng, quyền hạn.		
A.8.1.1	Các vai trò và trách nhiệm	*Biện pháp quản lý* Các vai trò và trách nhiệm đảm bảo an toàn của các nhân viên, người của nhà thầu và bên thứ ba cần được xác định và ghi thành văn bản phù hợp với chính sách an toàn thông tin của tổ chức.
A.8.1.2	Thẩm tra	*Biện pháp quản lý* Việc xác minh lai lịch của mọi ứng viên tuyển dụng, người của nhà nhà thầu và bên thứ ba phải được thực hiện phù hợp với pháp luật, quy định, đạo đức và phù hợp với các yêu cầu của công việc, phân loại thông tin được truy cập và các rủi ro có thể nhận thấy được.
A.8.1.3	Điều khoản và điều kiện tuyển dụng	*Biện pháp quản lý* Như một phần của các ràng buộc trong hợp đồng, các nhân viên, người của nhà thầu và bên thứ ba phải đồng ý và ký vào các điều khoản và điều kiện của hợp đồng tuyển dụng. Việc này làm rõ trách nhiệm của người được tuyển dụng và tổ chức tuyển dụng đối với an toàn thông tin.

[2] Thuật ngữ "tuyển dụng" ở đây bao hàm tất cả các tình huống khác nhau như : tuyển dụng người (tạm thời hay dài hạn), bổ nhiệm nhân sự, thay đổi việc, chỉ định thầu và việc chấm dứt những bố trí này.

A.8.2 Trong thời gian làm việc		
Mục tiêu: Đảm bảo rằng mọi nhân viên của tổ chức, người của nhà thầu và bên thứ ba nhận thức được các mối nguy cơ và các vấn đề liên quan tới an toàn thông tin, trách nhiệm và nghĩa vụ pháp lý của họ, và được trang bị các kiến thức, điều kiện cần thiết nhằm hỗ trợ chính sách an toàn thông tin của tổ chức trong quá trình làm việc, và giảm thiểu các rủi ro do con người gây ra.		
A.8.2.1	Trách nhiệm ban quản lý	*Biện pháp quản lý* Ban quản lý cần phải yêu cầu các nhân viên, người của nhà thầu và bên thứ ba chấp hành an toàn thông tin phù hợp với các các thủ tục và các chính sách an toàn thông tin đã được thiết lập của tổ chức.
A.8.2.2	Nhận thức, giáo dục và đào tạo về an toàn thông tin	*Biện pháp quản lý* Tất cả các nhân viên trong tổ chức, người của nhà thầu và bên thứ ba cần phải được đào tạo nhận thức và cập nhật thường xuyên những thủ tục, chính sách đảm bảo an toàn thông tin của tổ chức như một phần công việc bắt buộc.
A.8.2.3	Xử lý kỷ luật	*Biện pháp quản lý* Phải có hình thức xử lý kỷ luật đối với các nhân viên vi phạm về an toàn thông tin.
A.8.3 Chấm dứt hoặc thay đổi công việc		
Mục tiêu: Nhằm đảm bảo rằng các nhân viên của tổ chức, người của nhà thầu và bên thứ ba nghỉ việc hoặc thay đổi vị trí một cách có tổ chức.		
A.8.3.1	Trách nhiệm kết thúc hợp đồng	*Biện pháp quản lý* Các trách nhiệm trong việc kết thúc hoặc thay đổi nhân sự cần được xác định và phân định rõ ràng.
A.8.3.2	Bàn giao tài sản	*Biện pháp quản lý* Tất cả các nhân viên, người của nhà thầu và bên thứ ba cần trả lại các tài sản của tổ chức mà họ quản lý khi kết thúc hợp đồng hoặc thuyên chuyển công tác khác theo các điều khoản đã thống nhất.

A.8.3.3	Hủy bỏ quyền truy cập	*Biện pháp quản lý* Các quyền truy cập thông tin của mọi nhân viên, người của nhà thầu, bên thứ ba và các phương tiện xử lý thông tin phải được hủy bỏ khi họ kết thúc hợp đồng hoặc thuyên chuyển công tác.
A.9 Đảm bảo an toàn vật lý và môi trường		
A.9.1 Các khu vực an toàn *Mục tiêu:* Nhằm ngăn chặn sự truy cập vật lý trái phép, làm hư hại và cản trở thông tin và tài sản của tổ chức.		
A.9.1.1	Vành đai an toàn vật lý	*Biện pháp quản lý* Các vành đai an toàn (như tường, cổng ra/vào có kiểm soát bằng thẻ hoặc bàn tiếp tân...) phải được sử dụng để bảo vệ các khu vực chứa thông tin và phương tiện xử lý thông tin.
A.9.1.2	Kiểm soát cổng truy cập vật lý	*Biện pháp quản lý* Các khu vực bảo mật cần được bảo vệ bằng các biện pháp kiểm soát truy cập thích hợp nhằm đảm bảo chỉ những người có quyền mới được phép truy cập.
A.9.1.3	Bảo vệ các văn phòng, phòng làm việc và vật dụng	*Biện pháp quản lý* Biện pháp bảo vệ an toàn vật lý cho các văn phòng, phòng làm việc và vật dụng cần được thiết kế và áp dụng.
A.9.1.4	Bảo vệ chống lại các mối đe dọa từ bên ngoài và từ môi trường	*Biện pháp quản lý* Biện pháp bảo vệ vật lý chống lại những nguy cơ do cháy nổ, ngập lụt, động đất, tình trạng náo loạn và các dạng thảm họa khác do thiên nhiên và do con người gây ra cần được thiết kế và áp dụng.
A.9.1.5	Làm việc trong các khu vực an toàn	*Biện pháp quản lý* Biện pháp bảo vệ vật lý và các hướng dẫn làm việc trong các khu vực an toàn cần được thiết kế và áp dụng.

A.9.1.6	Các khu vực truy cập tự do, phân phối, chuyển hàng	*Biện pháp quản lý* Các điểm truy cập mà người truy nhập không cần cấp phép như khu vực chung, phân phối, chuyển hàng.. phải được quản lý và, nếu có thể, được cách ly khỏi các phương tiện xử lý thông tin để tránh tình trạng truy nhập trái phép.
A.9.2 Đảm bảo an toàn trang thiết bị *Mục tiêu:* Nhằm ngăn ngừa sự mất mát, hư hại, đánh cắp hoặc lợi dụng tài sản, và sự gián đoạn hoạt động của tổ chức.		
A.9.2.1	Bố trí và bảo vệ thiết bị	*Biện pháp quản lý* Thiết bị phải được bố trí tại các địa điểm an toàn hoặc được bảo vệ nhằm giảm thiểu các rủi ro do các đe doạ, hiểm hoạ từ môi trường hay các truy cập trái phép.
A.9.2.2	Các tiện ích hỗ trợ	*Biện pháp quản lý* Thiết bị phải được bảo vệ khỏi sự cố về nguồn điện cũng như các sự gián đoạn hoạt động có nguyên nhân từ các tiện ích hỗ trợ.
A.9.2.3	An toàn cho dây cáp	*Biện pháp quản lý* Dây dẫn nguồn điện và cáp truyền thông mang dữ liệu hoặc các hỗ trợ các dịch vụ thông tin phải được bảo vệ khỏi sự xâm phạm hoặc làm hư hại.
A.9.2.4	Duy trì thiết bị	*Biện pháp quản lý* Các thiết bị cần được duy trì một cách thích hợp nhằm đảm bảo luôn sẵn sàng và toàn vẹn.
A.9.2.5	An toàn cho thiết bị hoạt động bên ngoài nhà	*Biện pháp quản lý* Phải đảm bảo an toàn cho các thiết bị ngoài nhà, chú ý đến các rủi ro khác nhau khi thiết bị làm việc bên ngoài tổ chức.
A.9.2.6	An toàn khi loại bỏ và tái sử dụng thiết bị	*Biện pháp quản lý* Tất cả các bộ phận của thiết bị có chứa các phương tiện lưu trữ thông tin phải được kiểm tra nhằm đảm bảo rằng tất cả dữ liệu nhạy cảm và phần mềm có bản quyền phải được xóa bỏ hoặc ghi đè trước khi loại bỏ hoặc tái sử dụng thiết bị cho mục đích khác.

A.9.2.7	Di dời tài sản	*Biện pháp quản lý* Thiết bị, thông tin hoặc phần mềm không được mang ra ngoài trước khi được phép.
A.10 Quản lý truyền thông và điều hành		
A.10.1 Các thủ tục và trách nhiệm điều hành *Mục tiêu:* Nhằm đảm bảo sự điều hành các phương tiện xử lý thông tin đúng đắn và an toàn.		
A.10.1.1	Các thủ tục vận hành được ghi thành văn bản	*Biện pháp quản lý* Các thủ tục vận hành cần được ghi thành văn bản, duy trì và luôn sẵn sàng đối với mọi người cần dùng đến.
A.10.1.2	Quản lý thay đổi	*Biện pháp quản lý* Các thay đổi trong các phương tiện xử lý thông tin và hệ thống xử lý thông tin phải được kiểm soát.
A.10.1.3	Phân tách nhiệm vụ	*Biện pháp quản lý* Các nhiệm vụ và phạm vi trách nhiệm phải được phân tách nhằm giảm thiểu khả năng sửa đổi bất hợp lệ hoặc không mong muốn hay lạm dụng các tài sản của tổ chức.
A.10.1.4	Phân tách các chức năng phát triển, kiểm thử và điều hành	*Biện pháp quản lý* Các chức năng phát triển, kiểm thử và vận hành cần được phân tách nhằm giảm thiểu các rủi ro của việc truy cập hoặc thay đổi trái phép đối với hệ thống điều hành.
A.10.2 Quản lý chuyển giao dịch vụ của bên thứ ba *Mục tiêu:* Nhằm triển khai và duy trì mức độ an toàn thông tin và việc chuyển giao dịch vụ phù hợp với thỏa thuận chuyển giao dịch vụ của bên thứ ba.		
A.10.2.1	Chuyển giao dịch vụ	*Biện pháp quản lý* Cần phải đảm bảo rằng các biện pháp kiểm soát an toàn, các định nghĩa dịch vụ và mức độ chuyển giao dịch vụ trong thỏa thuận chuyển giao dịch vụ của bên thứ ba được triển khai, vận hành và duy trì bởi bên thứ ba.

A.10.2.2	Giám sát và soát xét các dịch vụ của bên thứ ba	*Biện pháp quản lý* Các dịch vụ, báo cáo và hồ sơ do bên thứ ba cung cấp phải được giám sát và soát xét một cách thường xuyên và việc kiểm toán phải được tiến hành một cách thường xuyên.
A.10.2.3	Quản lý thay đổi đối với các dịch vụ của bên thứ ba	*Biện pháp quản lý* Các thay đổi về cung cấp dịch vụ bao gồm việc duy trì và cải tiến các chính sách, thủ tục, biện pháp quản lý an toàn thông tin hiện hành cần phải được quản lý, chú ý đến tính quan trọng của hệ thống và quy trình nghiệp vụ liên quan cũng như việc đánh giá lại các rủi ro.
A.10.3 Lập kế hoạch và chấp nhận hệ thống *Mục tiêu:* Giảm thiểu rủi ro do sự đổ vỡ hệ thống.		
A.10.3.1	Quản lý năng lực hệ thống	*Biện pháp quản lý* Việc sử dụng tài nguyên phải được giám sát, điều chỉnh và có dự đoán các yêu cầu về năng lực hệ thống trong tương lai nhằm đảm bảo hiệu suất cần thiết.
A.10.3.2	Chấp nhận hệ thống	*Biện pháp quản lý* Tiêu chí chấp nhận các hệ thống thông tin mới, các cải tiến và các phiên bản mới cần được thiết lập và các kiểm tra hệ thống thích hợp cần được tiến hành trong quá trình phát triển và trước khi được chấp nhận.
A.10.4 Bảo vệ chống lại các mã độc và mã di động *Mục tiêu:* Nhằm bảo vệ tính toàn vẹn của phần mềm và thông tin.		
A.10.4.1	Quản lý chống lại mã độc	*Biện pháp quản lý* Các biện pháp quản lý trong việc phát hiện, ngăn chặn và phục hồi nhằm chống lại các đoạn mã độc và các thủ tục tuyên truyền nâng cao nhận thức của người sử dụng phải được thực hiện.
A.10.4.2	Kiểm soát các mã di động	*Biện pháp quản lý* Đối với các mã di động hợp lệ, việc cài đặt phải đảm bảo phù hợp với các chính sách an toàn đã được đặt ra. Ngược lại, các đoạn mã di động trái phép sẽ bị ngăn chặn.

A.10.5 Sao lưu *Mục tiêu:* Nhằm duy trì sự toàn vẹn và sẵn sàng của thông tin cũng như các phương tiện xử lý thông tin.		
A.10.5.1	Sao lưu thông tin	*Biện pháp quản lý* Thông tin và phần mềm cần được sao lưu và các bản sao cần được kiểm tra thường xuyên phù hợp với chính sách sao lưu đã được chấp thuận.
A.10.6 Quản lý an toàn mạng *Mục tiêu:* Nhằm đảm bảo an toàn cho thông tin trên mạng và an toàn cho cơ sở hạ tầng hỗ trợ.		
A.10.6.1	Kiểm soát mạng	*Biện pháp quản lý* Các mạng cần phải được quản lý và kiểm soát một cách thỏa đáng nhằm bảo vệ khỏi các mối đe dọa và duy trì an toàn cho các hệ thống, ứng dụng sử dụng mạng và thông tin đang được truyền trên mạng.
A.10.6.2	An toàn cho các dịch vụ mạng	*Biện pháp quản lý* Các tính năng an toàn, các mức độ dịch vụ và các yêu cầu quản lý của tất cả các dịch vụ mạng phải được xác định và ghi rõ trong các thỏa thuận về dịch vụ mạng, bất kể dịch vụ là do nội bộ cấp hay thuê khoán.
A.10.7 Quản lý phương tiện *Mục tiêu:* Nhằm ngăn ngừa sự tiết lộ, sửa đổi, xoá bỏ hoặc phá hoại bất hợp pháp các tài sản và sự gián đoạn các hoạt động nghiệp vụ.		
A.10.7.1	Quản lý các phương tiện có thể di dời	*Biện pháp quản lý* Cần phải có các thủ tục sẵn sàng cho việc quản lý phương tiện có thể di dời.
A.10.7.2	Loại bỏ phương tiện	*Biện pháp quản lý* Các phương tiện cần được loại bỏ một cách an toàn và bảo mật khi không còn cần thiết theo các thủ tục xử lý chính thức.

A.10.7.3	Các thủ tục xử lý thông tin	*Biện pháp quản lý* Các thủ tục cho việc xử lý và lưu trữ thông tin phải được thiết lập nhằm bảo vệ thông tin khỏi sự tiết lộ hoặc sử dụng bất hợp pháp.
A.10.7.4	An toàn cho các tài liệu hệ thống	*Biện pháp quản lý* Các tài liệu hệ thống cần được bảo vệ khỏi sự truy cập trái phép.
A.10.8 Trao đổi thông tin *Mục tiêu:* Nhằm duy trì an toàn cho các thông tin và phần mềm được trao đổi trong nội bộ tổ chức hoặc với các thực thể bên ngoài.		
A.10.8.1	Các chính sách và thủ tục trao đổi thông tin	*Biện pháp quản lý* Các chính sách, thủ tục và biện pháp quản lý chính thức cần phải sẵn có để bảo vệ sự trao đổi thông tin thông qua hệ thống truyền thông.
A.10.8.2	Các thỏa thuận trao đổi	*Biện pháp quản lý* Các thỏa thuận cần được thiết lập cho việc trao đổi thông tin và phần mềm giữa tổ chức và các thực thể bên ngoài.
A.10.8.3	Vận chuyển phương tiện vật lý	*Biện pháp quản lý* Phương tiện chứa thông tin cần được bảo vệ khỏi sự truy cập trái phép, sự lạm dụng hoặc làm sai lạc khi vận chuyển vượt ra ngoài phạm vi địa lý của tổ chức.
A.10.8.4	Thông điệp điện tử	*Biện pháp quản lý* Thông tin bao hàm trong các thông điệp điện tử cần được bảo vệ một cách thỏa đáng.
A.10.8.5	Các hệ thống thông tin nghiệp vụ	*Biện pháp quản lý* Các chính sách, các thủ tục cần được phát triển và triển khai nhằm bảo vệ thông tin gắn với sự kết nối giữa các các hệ thống thông tin nghiệp vụ.
A.10.9 Các dịch vụ thương mại điện tử *Mục tiêu:* Nhằm đảm bảo an toàn cho các dịch vụ thương mại điện tử và việc sử dụng an toàn các dịch vụ này.		

A.10.9.1	Thương mại điện tử	*Biện pháp quản lý* Thông tin trong thương mại điện tử truyền qua các mạng công cộng cần phải được bảo vệ khỏi các hoạt động gian lận, các tranh cãi về giao kèo và sự tiết lộ, sửa đổi trái phép.
A.10.9.2	Các giao dịch trực tuyến	*Biện pháp quản lý* Thông tin trong các giao dịch trực tuyến cần được bảo vệ khỏi việc truyền không đầy đủ, sai địa chỉ, bị sửa đổi thông điệp trái phép, bị tiết lộ hoặc nhân bản thông điệp một cách trái phép.
A.10.9.3	Thông tin công khai	*Biện pháp quản lý* Tính toàn vẹn của thông tin công khai trên các hệ thống công cộng cần phải được bảo vệ nhằm ngăn chặn sự sửa đổi trái phép.
A.10.10 Giám sát *Mục tiêu:* Nhằm phát hiện các hoạt động xử lý thông tin trái phép		
A.10.10.1	Ghi nhật ký kiểm toán	*Biện pháp quản lý* Việc ghi lại tất cả các hoạt động của người dùng, các lỗi ngoại lệ và các sự kiện an toàn thông tin cần phải được thực hiện và duy trì trong một khoảng thời gian đã được thỏa thuận nhằm trợ giúp cho việc điều tra cũng như giám sát điều khiển truy cập về sau.
A.10.10.2	Giám sát việc sử dụng hệ thống	*Biện pháp quản lý* Các thủ tục giám sát việc sử dụng các phương tiện xử lý thông tin cần được thiết lập và kết quả giám sát cần phải được xem xét thường xuyên.
A.10.10.3	Bảo vệ các thông tin nhật ký	*Biện pháp quản lý* Các chức năng ghi nhật ký cũng như thông tin nhật ký cần được bảo vệ khỏi sự giả mạo và truy cập trái phép.
A.10.10.4	Nhật ký người điều hành và người quản trị	*Biện pháp quản lý* Tất cả hoạt động của người quản trị cũng như người điều hành hệ thống cần phải được ghi lại.

A.10.10.5	Nhật ký lỗi	*Biện pháp quản lý* Các lỗi cần được ghi lại và phân tích và có các hoạt động xử lý cần thiết.
A.10.10.6	Đồng bộ thời gian	*Biện pháp quản lý* Đồng hồ trên các hệ thống xử lý thông tin trong tổ chức hoặc trong một phạm vi an toàn cần được đồng bộ với một nguồn thời gian chính xác đã được đồng ý lựa chọn.
A.11 Quản lý truy cập		
A.11.1 Yêu cầu nghiệp vụ cho quản lý truy cập *Mục tiêu:* Quản lý các truy cập thông tin.		
A.11.1.1	Chính sách quản lý truy cập	*Biện pháp quản lý* Chính sách quản lý truy cập cần được thiết lập, ghi thành văn bản và soát xét dựa trên các yêu cầu bảo mật và nghiệp vụ cho các truy cập.
A.11.2 Quản lý truy cập người sử dụng *Mục tiêu:* Nhằm đảm bảo người dùng hợp lệ được truy cập và ngăn chặn những người dùng không hợp lệ truy cập trái phép đến hệ thống thông tin.		
A.11.2.1	Đăng ký thành viên	*Biện pháp quản lý* Cần thiết phải có một thủ tục chính thức về đăng ký và hủy đăng ký thành viên để thực hiện cấp phát hoặc thu hồi quyền truy cập đến tất cả các hệ thống và dịch vụ thông tin.
A.11.2.2	Quản lý đặc quyền	*Biện pháp quản lý* Việc cấp phát và sử dụng các đặc quyền cần phải được giới hạn và kiểm soát.
A.11.2.3	Quản lý mật khẩu người sử dụng	*Biện pháp quản lý* Việc cấp phát mật khẩu người dùng cần được kiểm soát thông qua một quy trình quản lý chính thức.
A.11.2.4	Soát xét các quyền truy cập của người dùng	*Biện pháp quản lý* Ban quản lý cần định kỳ soát xét các quyền truy cập của người dùng theo một quy trình chính thức.

A.11.3 Các trách nhiệm của người dùng		
Mục tiêu: Nhằm ngăn chặn những người dùng trái phép truy cập, làm tổn hại hoặc lấy cắp thông tin cũng như các phương tiện xử lý thông tin.		
A.11.3.1	Sử dụng mật khẩu	*Biện pháp quản lý* Người dùng phải được yêu cầu tuân thủ quy tắc thực hành an toàn tốt trong việc lựa chọn và sử dụng mật khẩu.
A.11.3.2	Các thiết bị không được quản lý	*Biện pháp quản lý* Người dùng cần đảm bảo rằng các thiết bị không được quản lý phải được bảo vệ thích hợp.
A.11.3.3	Chính sách giữ sạch bàn và màn hình làm việc	*Biện pháp quản lý* Chính sách bàn làm việc sạch không có giấy và các phương tiện lưu trữ di động và chính sách màn hình sạch cho các phương tiện xử lý thông tin phải được thực hiện.
A.11.4 Quản lý truy cập mạng		
Mục tiêu: Nhằm ngăn chặn các truy cập trái phép các dịch vụ mạng.		
A.11.4.1	Chính sách sử dụng các dịch vụ mạng	*Biện pháp quản lý* Người dùng chỉ được cung cấp quyền truy cập đến các dịch vụ mà họ đã được cho phép.
A.11.4.2	Xác thực người dùng cho các kết nối bên ngoài	*Biện pháp quản lý* Các biện pháp xác thực thích hợp cần được sử dụng để quản lý truy cập bởi các người dùng từ xa.
A.11.4.3	Định danh thiết bị trong các mạng	*Biện pháp quản lý* Định danh thiết bị tự động cần được xem xét như là một biện pháp để xác thực kết nối từ các vị trí và thiết bị cụ thể.
A.11.4.4	Bảo vệ cổng cấu hình và chẩn đoán từ xa	*Biện pháp quản lý* Các truy cập lôgíc hoặc vật lý tới các cổng dùng cho việc cấu hình và chẩn đoán cần được kiểm soát.
A.11.4.5	Phân tách trên mạng	*Biện pháp quản lý* Các nhóm người dùng, dịch vụ và hệ thống thông tin cần được phân tách trên các mạng.

A.11.4.6	Quản lý kết nối mạng	*Biện pháp quản lý* Đối với các mạng chia sẻ, đặc biệt là các mạng mở rộng ra ngoài tổ chức, số lượng người dùng có thể kết nối vào mạng phải được giới hạn, phù hợp với các chính sách quản lý truy cập và các yêu cầu trong ứng dụng nghiệp vụ (xem 11.1)
A.11.4.7	Quản lý định tuyến mạng	*Biện pháp quản lý* Quản lý định tuyến mạng cần được triển khai nhằm đảm bảo các kết nối máy tính và luồng thông tin không vi phạm các chính sách quản lý truy cập của các ứng dụng nghiệp vụ.
A.11.5 Quản lý truy cập hệ thống điều hành *Mục tiêu:* Nhằm ngăn chặn các truy cập trái phép tới hệ thống điều hành		
A.11.5.1	Các thủ tục đăng nhập an toàn	*Biện pháp quản lý* Truy cập đến hệ thống điều hành cần được kiểm soát bởi thủ tục đăng nhập an toàn.
A.11.5.2	Định danh và xác thực người dùng	*Biện pháp quản lý* Tất cả người dùng đều phải có một định danh duy nhất (định danh người dùng – User ID) để sử dụng cho mục đích cá nhân. Một kỹ thuật xác thực thích hợp cần được chọn nhằm chứng thực đặc điểm nhận dạng của người dùng.
A.11.5.3	Hệ thống quản lý mật khẩu	*Biện pháp quản lý* Các hệ thống quản lý mật khẩu phải có khả năng tương tác và bảo đảm chất lượng của mật khẩu.
A.11.5.4	Sử dụng các tiện ích hệ thống	*Biện pháp quản lý* Việc sử dụng chương trình tiện ích có khả năng ảnh hưởng đến việc quản lý hệ thống và các chương trình ứng dụng khác phải được giới hạn và kiểm soát chặt chẽ.
A.11.5.5	Thời gian giới hạn của phiên làm việc	*Biện pháp quản lý* Các phiên làm việc không hoạt động cần được ngắt sau một khoảng thời gian trễ nhất định.

A.11.5.6	Giới hạn thời gian kết nối	*Biện pháp quản lý* Cần hạn chế về thời gian kết nối để làm tăng độ an toàn cho các ứng dụng có mức rủi ro cao.
A.11.6 Điều khiển truy cập thông tin và ứng dụng *Mục tiêu:* Nhằm ngăn chặn các truy cập trái phép đến thông tin lưu trong các hệ thống ứng dụng.		
A.11.6.1	Hạn chế truy cập thông tin	*Biện pháp quản lý* Truy cập của người sử dụng và nhân viên hỗ trợ tới thông tin và các chức năng của hệ thống ứng dụng cần được hạn chế phù hợp với chính sách quản lý truy cập đã được xác định.
A.11.6.2	Cách ly hệ thống nhạy cảm	*Biện pháp quản lý* Các hệ thống nhạy cảm cần có môi trường máy tính cách ly.
A.11.7 Tính toán qua thiết bị di động và làm việc từ xa *Mục tiêu:* Nhằm đảm bảo an toàn thông tin khi sử dụng các phương tiện tính toán di động và làm việc từ xa.		
A.11.7.1	Tính toán và truyền thông qua thiết bị di động	*Biện pháp quản lý* Một chính sách chính thức cần được chuẩn bị và các biện pháp an toàn thông tin thích hợp cần được chấp nhận nhằm bảo vệ khỏi các rủi ro khi sử dụng tính toán và truyền thông di động.
A.11.7.2	Làm việc từ xa	*Biện pháp quản lý* Một chính sách, các kế hoạch điều hành và các thủ tục cần được phát triển và triển khai cho các hoạt động làm việc từ xa.
A.12 Tiếp nhận, phát triển và duy trì các hệ thống thông tin		
A.12.1 Yêu cầu đảm bảo an toàn cho các hệ thống thông tin *Mục tiêu:* Nhằm đảm bảo rằng an toàn thông tin là một phần không thể thiếu của các hệ thống thông tin.		
A.12.1.1	Phân tích và đặc tả các yêu cầu về an toàn	*Biện pháp quản lý* Các thông báo về yêu cầu nghiệp vụ đối với các hệ thống thông tin mới hoặc được cải tiến từ hệ thống thông tin có sẵn cần chỉ rõ các yêu cầu về biện pháp quản lý an toàn thông tin.

A.12.2 Xử lý đúng trong các ứng dụng		
Mục tiêu: Nhằm ngăn chặn các lỗi, mất mát, sửa đổi hoặc sử dụng trái phép thông tin trong các ứng dụng.		
A.12.2.1	Kiểm tra tính hợp lệ của dữ liệu nhập vào	*Biện pháp quản lý* Dữ liệu nhập vào các ứng dụng cần được kiểm tra tính hợp lệ để đảm bảo các dữ liệu này là chính xác và thích hợp.
A.12.2.2	Kiểm soát việc xử lý nội bộ	*Biện pháp quản lý* Việc kiểm tra tính hợp lệ cần được tích hợp trong các ứng dụng nhằm phát hiện thông tin sai lệch do các lỗi trong quá trình xử lý hoặc các hành vi có chủ ý.
A.12.2.3	Tính toàn vẹn thông điệp	*Biện pháp quản lý* Các yêu cầu bảo đảm tính xác thực và bảo vệ sự toàn vẹn thông điệp trong các ứng dụng cần được xác định. Bên cạnh đó các biện pháp quản lý phù hợp cũng cần được xác định và triển khai.
A.12.2.4	Kiểm tra tính hợp lệ của dữ liệu đầu ra	*Biện pháp quản lý* Dữ liệu xuất ra từ một ứng dụng cần được kiểm tra nhằm đảm bảo rằng quá trình xử lý thông tin chính xác và thích hợp trong mọi trường hợp.
A.12.3 Quản lý mã hóa		
Mục đích: Nhằm bảo vệ tính bảo mật, xác thực hoặc toàn vẹn của thông tin bằng các biện pháp mã hóa.		
A.12.3.1	Chính sách sử dụng các biện pháp quản lý mã hóa	*Biện pháp quản lý* Một chính sách về việc sử dụng các biện pháp quản lý mã hóa để bảo vệ thông tin cần được xây dựng và triển khai.
A.12.3.2	Quản lý khóa	*Biện pháp quản lý* Việc quản lý khóa cần sẵn sàng để hỗ trợ cho các kỹ thuật mã hóa được sử dụng trong tổ chức.
A.12.4 An toàn cho các tệp tin hệ thống		
Mục tiêu: Nhằm đảm bảo an toàn cho các tệp tin hệ thống.		

A.12.4.1	Quản lý các phần mềm điều hành	*Biện pháp quản lý* Cần phải có các thủ tục sẵn sàng cho việc quản lý quá trình cài đặt các phần mềm trên hệ thống điều hành.
A.12.4.2	Bảo vệ dữ liệu kiểm tra hệ thống	*Biện pháp quản lý* Dữ liệu kiểm tra cần được lựa chọn, bảo vệ và kiểm soát một cách thận trọng.
A.12.4.3	Quản lý truy cập đến mã nguồn của chương trình	*Biện pháp quản lý* Việc truy cập đến mã nguồn của chương trình cần được giới hạn chặt chẽ.
A.12.5 Bảo đảm an toàn trong các quy trình hỗ trợ và phát triển *Mục tiêu:* Nhằm duy trì an toàn của thông tin và các phần mềm hệ thống ứng dụng		
A.12.5.1	Các thủ tục quản lý thay đổi	*Biện pháp quản lý* Việc thực thi các thay đổi phải được quản lý bằng việc áp dụng các thủ tục quản lý thay đổi chính thức.
A.12.5.2	Soát xét kỹ thuật các ứng dụng sau thay đổi của hệ thống điều hành.	*Biện pháp quản lý* Khi hệ điều hành thay đổi, các ứng dụng nghiệp vụ quan trọng cần được soát xét và kiểm tra lại nhằm đảm bảo không xảy ra các ảnh hưởng bất lợi tới hoạt động cũng như an toàn của tổ chức.
A.12.5.3	Hạn chế thay đổi các gói phần mềm	*Biện pháp quản lý* Việc sửa đổi các gói phần mềm là không được khuyến khích, cần hạn chế và chỉ thực hiện đối với các thay đổi rất cần thiết. Trong trường hợp này, mọi thay đổi cần phải được quản lý chặt chẽ.
A.12.5.4	Sự rò rỉ thông tin	*Biện pháp quản lý* Các điều kiện có thể gây rò rỉ thông tin cần phải được ngăn chặn.
A.12.5.5	Phát triển phần mềm thuê khoán	*Biện pháp quản lý* Việc phát triển các phần mềm thuê khoán cần phải được quản lý và giám sát bởi tổ chức.

A.12.6 Quản lý các điểm yếu về kỹ thuật		
Mục tiêu: Nhằm giảm thiểu các mối nguy hiểm xuất phát từ việc tin tặc khai thác các điểm yếu kỹ thuật đã được công bố.		
A.12.6.1	Quản lý các điểm yếu về mặt kỹ thuật	*Biện pháp quản lý* Thông tin kịp thời về các điểm yếu kỹ thuật của các hệ thống thông tin đang được sử dụng cần phải được thu thập. Tổ chức cần công bố đánh giá về các điểm yếu này và thực hiện các biện pháp thích hợp để giải quyết các rủi ro liên quan.
A.13 Quản lý các sự cố an toàn thông tin		
A.13.1 Báo cáo về các sự kiện an toàn thông tin và các nhược điểm		
Mục tiêu: Nhằm đảm bảo các sự kiện an toàn thông tin và các nhược điểm liên quan tới các hệ thống thông tin được trao đổi để các hành động khắc phục được tiến hành kịp thời.		
A.13.1.1	Báo cáo các sự kiện an toàn thông tin	*Biện pháp quản lý* Các sự kiện an toàn thông tin cần được báo cáo thông qua các kênh quản lý thích hợp theo cách nhanh nhất có thể.
A.13.1.2	Báo cáo các nhược điểm về an toàn thông tin	*Biện pháp quản lý* Mọi nhân viên, nhà thầu và bên thứ ba của các hệ thống và dịch vụ thông tin cần được yêu cầu ghi lại và báo cáo bất kỳ nhược điểm nào về an toàn đã thấy được hoặc cảm thấy nghi ngờ trong các hệ thống hoặc dịch vụ.
A.13.2 Quản lý các sự cố an toàn thông tin và cải tiến		
Mục tiêu: Nhằm đảm bảo một cách tiếp cận hiệu quả và nhất quán được áp dụng trong việc quản lý các sự cố an toàn thông tin.		
A.13.2.1	Các trách nhiệm và thủ tục	*Biện pháp quản lý* Các trách nhiệm và thủ tục quản lý cần được thiết lập nhằm đảm bảo sự phản ứng nhanh chóng, hiệu quả, đúng trình tự khi xảy ra các sự cố an toàn thông tin.
A.13.2.2	Rút bài học kinh nghiệm từ các sự cố an toàn thông tin	*Biện pháp quản lý* Cần phải có các cơ chế sẵn sàng nhằm cho phép các lượng hóa và giám sát các kiểu, số lượng và chi phí của các sự cố an toàn thông tin.

A.13.2.3	Thu thập chứng cứ	*Biện pháp quản lý* Khi một hành động nhằm chống lại một người hay một tổ chức sau khi có một sự cố an toàn thông tin xảy ra, liên quan đến pháp luật (có thể là dân sự hay hình sự), chứng cứ cần được thu thập, giữ lại và được trình bày sao cho phù hợp với quy định pháp lý.
A.14 Quản lý sự liên tục của hoạt động nghiệp vụ		
A.14.1 Các khía cạnh an toàn thông tin trong quản lý sự liên tục của hoạt động nghiệp vụ *Mục tiêu:* Chống lại các gián đoạn trong hoạt động nghiệp vụ và bảo vệ các quy trình hoạt động trọng yếu khỏi các ảnh hưởng do lỗi hệ thống thông tin hay các thảm hoạ và đảm bảo khả năng khôi phục các hoạt động bình thường đúng lúc.		
A.14.1.1	Tính đến an toàn thông tin trong các quy trình quản lý sự liên tục của hoạt động nghiệp vụ	*Biện pháp quản lý* Một quy trình được quản lý cần được xây dựng và duy trì nhằm đảm bảo các hoạt động của cơ quan/tổ chức không bị gián đoạn. Nội dung quy trình này phải đề cập các yêu cầu về an toàn thông tin cần thiết để đảm bảo các hoạt động liên tục của tổ chức.
A.14.1.2	Đánh giá rủi ro và sự liên tục trong hoạt động của tổ chức	*Biện pháp quản lý* Các sự kiện có thể gây ra sự gián đoạn của hoạt động của tổ chức cần được xác định cùng với xác suất, ảnh hưởng cũng như hậu quả của chúng đối với an toàn thông tin.
A.14.1.3	Xây dựng và triển khai các kế hoạch về tính liên tục, trong đó bao gồm vấn đề bảo đảm an toàn thông tin.	*Biện pháp quản lý* Các kế hoạch phải được phát triển và triển khai nhằm duy trì hoặc khôi phục các hoạt động điều hành và đảm bảo tính sẵn sàng của thông tin ở mức độ yêu cầu và đáp ứng yêu cầu về thời gian xử lý các gián đoạn và hư hỏng trong các quá trình nghiệp vụ quan trọng.
A.14.1.4	Khung hoạch định sự liên tục trong hoạt động nghiệp vụ	*Biện pháp quản lý* Một khung hoạch định các kế hoạch đảm bảo liên tục trong hoạt động nghiệp vụ cần được duy trì để mọi kế hoạch được thực hiện một cách nhất quán và đạt được các yêu cầu về đảm bảo an toàn thông tin cũng như xác định được các mức độ ưu tiên cho việc kiểm tra và duy trì.

A.14.1.5	Kiểm tra, duy trì và đánh giá lại các kế hoạch đảm bảo sự liên tục trong hoạt động của tổ chức.	*Biện pháp quản lý* Các kế hoạch đảm bảo sự liên tục trong hoạt động đơn vị cần được kiểm tra và cập nhật thường xuyên nhằm luôn đảm bảo tính cập nhật và hiệu quả.
A.15 Sự tuân thủ		
A.15.1 Sự tuân thủ các quy định pháp lý *Mục tiêu:* Nhằm tránh sự vi phạm pháp luật, quy định, nghĩa vụ theo các hợp đồng đã ký kết, các yêu cầu về bảo đảm an toàn thông tin.		
A.15.1.1	Xác định các điều luật hiện đang áp dụng được	*Biện pháp quản lý* Tất cả yêu cầu về pháp lý; quy định; nghĩa vụ trong hợp đồng đã ký và cách tiếp cận của tổ chức để đáp ứng những yêu cầu này phải được xác định rõ ràng, ghi thành văn bản và được cập nhật thường xuyên.
A.15.1.2	Quyền sở hữu trí tuệ (IPR)	*Biện pháp quản lý* Các thủ tục phù hợp cần được triển khai nhằm đảm bảo sự phù hợp với các yêu cầu pháp lý, các quy định và cam kết theo hợp đồng trong việc sử dụng các tài liệu có quyền sở hữu trí tuệ và các sản phẩm phần mềm độc quyền.
A.15.1.3	Bảo vệ các hồ sơ tổ chức	*Biện pháp quản lý* Các hồ sơ quan trọng cần được bảo vệ khỏi sự mất mát, phá hủy hoặc làm sai lệnh, phù hợp với pháp luật, quy định, các nghĩa vụ trong hợp đồng đã ký.
A.15.1.4	Bảo vệ dữ liệu và sự riêng tư của thông tin cá nhân	*Biện pháp quản lý* Việc bảo vệ dữ liệu và tính riêng tư cần được đảm bảo theo yêu cầu của pháp lý, quy định và cả các điều khoản trong hợp đồng nếu có.
A.15.1.5	Ngăn ngừa việc lạm dụng phương tiện xử lý thông tin	*Biện pháp quản lý* Cần phải ngăn chặn người dùng khỏi việc sử dụng các phương tiện xử lý thông tin vào mục đích không được phép.
A.15.1.6	Quy định về quản lý mã hóa	*Biện pháp quản lý* Quản lý mã hóa cần được áp dụng phù hợp với các thỏa thuận, luật pháp và các quy định liên quan.

A.15.2 Sự tuân thủ các chính sách và tiêu chuẩn an toàn, và tương thích kỹ thuật *Mục tiêu:* Nhằm đảm bảo sự tuân thủ của hệ thống với các chính sách và tiêu chuẩn an toàn của tổ chức.		
A.15.2.1	Sự tuân thủ các chính sách và tiêu chuẩn an toàn	*Biện pháp quản lý* Người quản lý cần đảm bảo rằng mọi thủ tục đảm bảo an toàn trong phạm vi trách nhiệm của mình đều được thực hiện chính xác để đạt được kết quả phù hợp với các chính sách cũng như các tiêu chuẩn an toàn.
A.15.2.2	Kiểm tra sự tương thích kỹ thuật	*Biện pháp quản lý* Các hệ thống thông tin cần được kiểm tra thường xuyên sự tuân thủ các tiêu chuẩn thực hiện an toàn.
A.15.3 Xem xét việc kiểm toán các hệ thống thông tin *Mục tiêu:* Nhằm tối ưu hóa hiệu quả và giảm thiểu những ảnh hưởng xấu tới quá trình kiểm toán các hệ thống thông tin.		
A.15.3.1	Các biện pháp quản lý kiểm toán các hệ thống thông tin	*Biện pháp quản lý* Các yêu cầu kiểm toán và các hoạt động kiểm tra các hệ thống điều hành cần được hoạch định thận trọng và thống nhất để hạn chế rủi ro hoặc sự đổ vỡ của các quy trình hoạt động nghiệp vụ.
A.15.3.2	Bảo vệ các công cụ kiểm toán hệ thống thông tin	*Biện pháp quản lý* Truy cập đến các công cụ kiểm toán hệ thống thông tin cần được bảo vệ khỏi mọi sự lạm dụng hoặc lợi dụng.

Phụ lục B

(Tham khảo)

Cách tiếp cận theo quy trình

B.1 Khái quát

Tiêu chuẩn này đưa ra một mô hình cho việc thiết lập, triển khai, điều hành, giám sát, soát xét, duy trì và cải tiến hệ thống quản lý an toàn thông tin (ISMS). Việc chấp nhận một hệ thống ISMS sẽ là một quyết định chiến lược của tổ chức. Thiết kế và triển khai ISMS của một tổ chức phụ thuộc vào các nhu cầu và mục tiêu khác nhau, các yêu cầu về an toàn cần phải đạt, các quy trình đang được sử dụng và quy mô, cấu trúc của tổ chức. Các yếu tố này và hệ thống hỗ trợ cần luôn được cập nhật và thay đổi. Việc đầu tư và triển khai một hệ thống ISMS cần phải có tỷ trọng phù hợp với nhu cầu của tổ chức.

Tiêu chuẩn này có thể sử dụng để đánh giá sự tuân thủ của các bộ phận bên trong tổ chức cũng như các bên liên quan bên ngoài tổ chức.

B.2 Cách tiếp cận theo quy trình

Tiêu chuẩn này chấp nhận cách tiếp cận theo quy trình khi thiết lập, triển khai, điều hành, giám sát, soát xét, duy trì và cải tiến hệ thống ISMS của tổ chức.

Một tổ chức cần xác định và quản lý rất nhiều hoạt động để vận hành một cách hiệu quả. Bất cứ hoạt động nào sử dụng các tài nguyên và được quản lý để có thể chuyển hoá các đầu vào thành đầu ra đều có thể được coi là một quy trình, Thông thường đầu ra của một quy trình này là đầu vào của một quy trình tiếp theo.

Việc áp dụng một hệ thống các quy trình trong tổ chức, cùng với sự nhận biết tương tác giữa các quy trình như vậy, và sự quản lý chúng, có thể coi như "cách tiếp cận theo quy trình".

Cách tiếp cận theo quy trình cho quản lý an toàn thông tin được trình bày trong tiêu chuẩn này nhằm khuyến khích người sử dụng nhấn mạnh các điểm quan trọng của:

a) việc hiểu các yêu cầu an toàn thông tin của tổ chức và các sự cần thiết phải thiết lập chính sách và mục tiêu cho an toàn thông tin,

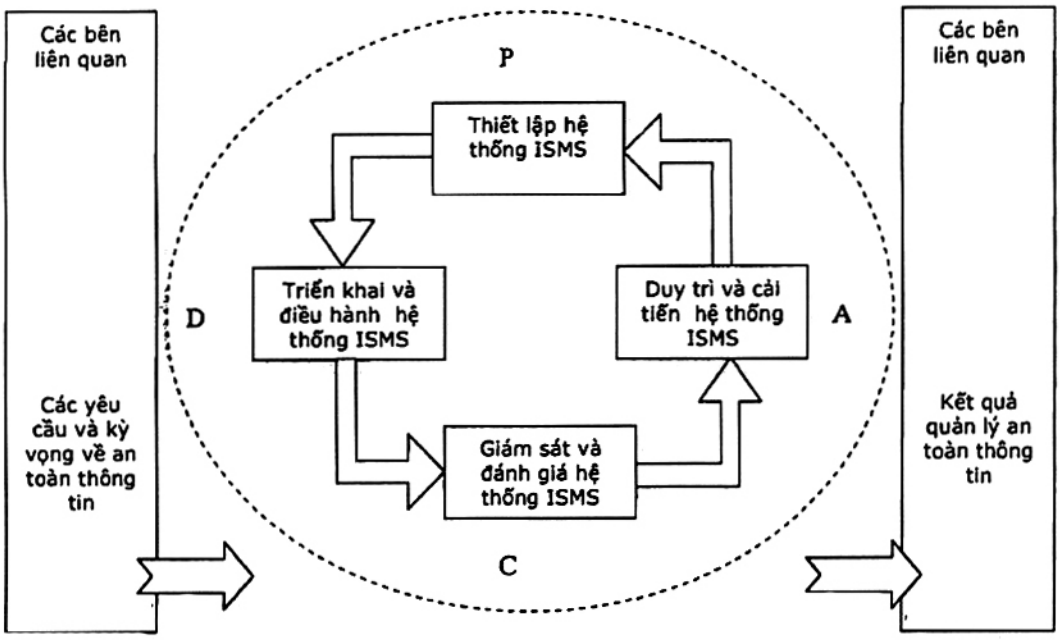
b) việc triển khai và điều hành các biện pháp quản lý rủi ro an toàn thông tin của tổ chức trước tất cả các rủi ro chung có thể xảy ra với tổ chức;

c) việc giám sát và soát xét hiệu suất và hiệu quả của hệ thống ISMS;

d) việc thường xuyên cải tiến dựa trên các khuôn khổ mục tiêu đã đặt ra.

Tiêu chuẩn này chấp nhận mô hình "Lập kế hoạch – Thực hiện – Kiểm tra - Hành động" (PDCA) để áp dụng cho tất cả các quy trình trong hệ thống ISMS. Hình 1 mô tả cách hệ thống ISMS lấy đầu vào là các yêu cầu và kỳ vọng về an toàn thông tin của các bên liên quan, sau khi tiến hành các quy trình và

hành động cần thiết sẽ đáp ứng an toàn thông tin theo như các yêu cầu và kỳ vọng đã đặt ra. Hình 1 cũng chỉ ra các liên hệ giữa các quy trình được biểu diễn trong các điều 4, 5, 6, 7 và 8 của tiêu chuẩn.



Hình 1 - Áp dụng mô hình PDCA cho các quy trình hệ thống ISMS

P (Lập kế hoạch) - Thiết lập ISMS	Thiết lập các chính sách, mục tiêu, quy trình và thủ tục liên quan đến việc quản lý các rủi ro và nâng cao an toàn thông tin nhằm đem lại các kết quả phù hợp với các chính sách và mục tiêu chung của tổ chức.
D (Thực hiện) - Triển khai và điều hành ISMS	Triển khai và vận hành các chính sách, biện pháp quản lý, quy trình và thủ tục của hệ thống ISMS.
C (Kiểm tra) - giám sát và soát xét ISMS	Xác định hiệu quả việc thực hiện quy trình dựa trên chính sách, mục tiêu mà hệ thống ISMS đã đặt ra và kinh nghiệm thực tiễn và báo cáo kết quả cho ban quản lý để soát xét.
A (Hành động) - Duy trì và cải tiến ISMS	Tiến hành các hành động khắc phục và hành động phòng ngừa dựa trên các kết quả của việc kiểm toán nội bộ hệ thống ISMS, soát xét của ban quản lý hoặc các thông tin liên quan khác nhằm liên tục hoàn thiện hệ thống ISMS.

Phụ lục C

(Tham khảo)

Sự tương ứng giữa ISO 9001:2000, ISO 14001:2004 và tiêu chuẩn này

Bảng C.1 chỉ ra sự tương ứng giữa ISO 9001:2000, ISO 14001:2004 và tiêu chuẩn này.

Bảng C.1 – Sự tương ứng giữa ISO 9001:2000, ISO 14001:2004 và tiêu chuẩn này

TCVN ISO/IEC 27001:2009	ISO 9001:2000	ISO 14001:2004
1 Phạm vi	**1 Scope** 1.1 General 1.2 Application	**1 Scope**
2 Tài liệu viện dẫn	**2 Normative references**	**2 Normative references**
3 Thuật ngữ và định nghĩa	**3 Terms and definitions**	**3 Terms and definitions**
4 Hệ thống quản lý an toàn thông tin	**4 Quality management system**	**4 EMS requirements**
4.1 Các yêu cầu chung	4.1 General requirements	4.1 General requirements
4.2 Thiết lập và quản lý hệ thống ISMS		
4.2.1 Thiết lập ISMS		
4.2.2 Triển khai và điều hành hệ thống ISMS		4.4 Implementation and operation
4.2.3 Giám sát và soát xét hệ thống ISMS	8.2.3 Monitoring and measurement of processes 8.2.4 Monitoring and measurement of product	4.5.1 Monitoring and measurement
4.2.4 Duy trì và cải tiến hệ thống ISMS		
4.3 Các yêu cầu về hệ thống tài liệu	4.2 Documentation requirements	
4.3.1 Khái quát	4.2.1 General 4.2.2 Quality manual	
4.3.2 Biện pháp quản lý tài liệu	4.2.3 Control of documents	4.4.5 Documentation control
4.3.3 Biện pháp quản lý hồ sơ	4.2.4 Control of records	4.5.4 Control of records

5 Trách nhiệm của ban quản lý 5.1 Cam kết của ban quản lý	**5 Management responsibility** 5.1 Management commitment 5.2 Customer focus 5.3 Quality policy 5.4 Planning 5.5 Responsibility, authority and communication	 4.2 Environmental policy 4.3 Planning
5.2 Quản lý nguồn lực 5.2.1 Cấp phát nguồn lực 5.2.2 Đào tạo, nhận thức và năng lực	**6 Resource management** 6.1 Provision of resources 6.2 Human resources 6.2.2 Competence, awareness and training 6.3 Infrastructure 6.4 Work environment	 4.4.2 Competence, training, and awareness
6 Kiểm toán nội bộ hệ thống ISMS	8.2.2 Internal Audit	4.5.5 Internal audit
7 Soát xét của ban quản lý đối với hệ thống ISMS 7.1 Khái quát 7.2 Đầu vào cho việc soát xét 7.3 Đầu ra của việc soát xét	**5.6 Management review** 5.6.1 General 5.6.2 Review input 5.6.3 Review output	**4.6 Management review**
8 Cải tiến hệ thống ISMS 8.1 Cải tiến thường xuyên	**8.5 Improvement** 8.5.1 Continual improvement	
8.2 Hành động khắc phục	8.5.3 Corrective actions	4.5.3 Non-conformity, corrective action and preventive action
8.3 Hành động phòng ngừa	8.5.3 Preventive actions	
Phụ lục A Các mục tiêu và biện pháp quản lý	**Annex A Control objectives and controls**	**Annex A Guidance on the use of this International Standard**
Phụ lục B Tiêu chuẩn hệ thống ISMS và cách tiếp cận theo quy trình 1 Khái quát 2 Cách tiếp cận theo quy trình	**0 Introduction** 0.1 General 0.2 Process approach	**Introduction**
Phụ lục C Sự tương ứng giữa ISO 9001:2000, ISO 14001:2004 và tiêu chuẩn này	**Annex A Correspondence between ISO 9001:2000 and ISO 14001:1996**	**Annex B Correspondence between ISO 14001:2004 and ISO 9001:2000**

Thư mục tài liệu tham khảo

Tiêu chuẩn kỹ thuật

[1] ISO 9001:2000, Quality management systems - Requirements

[2] ISO/IEC 13335-1:2004, Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management.

[3] ISO/IEC TR 13335-3:1998, Information technology - Guidelines for the management of IT Security - Part 3: Techniques for the management of IT security

[4] ISO/IEC TR 13335-4:2000, Information technology - Guidelines for the management of IT Security - Part 4: Selection of safeguards

[5] ISO 14001:2004, Environmental management systems - Requirements with guidance for use

[6] ISO/IEC TR 18044:2004, Information technology - Security techniques - Information security incident management

[7] ISO 19011:2002, Guidelines for quality and/or environmental management systems auditing

[8] ISO/IEC Guide 62:1996, General requirements for bodies operating assessment and certification/registration of quality systems

[9] ISO/IEC Guide 73:2002, Risk management - Vocabulary - Guidelines for use in standards

[10] TCVN ISO 9001:2000, Hệ thống quản lý chất lượng - Các yêu cầu

[11] TCVN 7562: 2005, Công nghệ thông tin – Mã thực hành quản lý an toàn thông tin.

Các tài liệu khác

[1] OECD, Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security. Paris: OECD, July 2002. www.oecd.org

[2] NIST SP 800-30, Risk Management Guide for Information Technology Systems

[3] Deming W.E., Out of the Crisis, Cambridge, Mass: MIT, Center for Advanced Engineering Study, 1986