TCVN TIÊU CHUẨN QUỐC GIA

TCVN ISO/IEC 27001:2019
ISO/IEC 27001:2013

Xuất bản lần 2

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

Information technology - Security techniques - Infomation security management systems - Requirements

HÀ NỘI – 2019

Lời nói đầu

TCVN ISO/IEC 27001:2019 thay thế TCVN ISO/IEC 27001:2009.

TCVN ISO/IEC 27001:2019 hoàn toàn tương đương với ISO/IEC 27001:2013; ISO/IEC 27001:2013/Cor.1:2014, ISO/IEC 27001:2013/Cor.2:2015.

TCVN ISO/IEC 27001:2019 do Viện Khoa học Kỹ thuật Bưu điện 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.

0 Lời giới thiệu

0.1 Tổng quan

Tiêu chuẩn này quy định các yêu cầu đối với hoạt động thiết lập, triển khai, duy trì và cải tiến liên tục hệ thống quản lý an toàn thông tin. Việc chấp nhận một hệ thống quản lý an toàn thông tin là quyết định chiến lược của tổ chức. Việc thiết lập và thực hiện một hệ thống quản lý an toàn thông tin của tổ chức chịu ảnh hưởng bởi nhu cầu và mục tiêu của tổ chức, các yêu cầu về an toàn, các quy trình của tổ chức được sử dụng và bởi quy mô và cấu trúc của tổ chức. Tất cả những yếu tố ảnh hưởng này dự kiến sẽ thay đổi theo thời gian.

Hệ thống quản lý an toàn thông tin đảm bảo tính bảo mật, tính toàn vẹn và tính sẵn sàng của thông tin bằng cách áp dụng quy trình quản lý rủi ro và mang lại niềm tin cho các bên liên quan rằng các rủi ro được quản lý đầy đủ.

Điều quan trọng là hệ thống quản lý an toàn thông tin là một phần và được tích hợp các quy trình của tổ chức và với cấu trúc quản lý tổng thể và an toàn thông tin được xem xét trong thiết kế các quy trình, các hệ thống thông tin và các kiểm soát. Dự kiến rằng việc triển khai một hệ thống quản lý an toàn thông tin sẽ có quy mô phù hợp với nhu cầu của tổ chức.

Tiêu chuẩn này có thể được sử dụng bởi các phòng ban nội bộ và bên ngoài để đánh giá khả năng của tổ chức trong việc đáp ứng các yêu cầu an toàn thông tin của chính tổ chức.

Thứ tự yêu cầu được trình bày trong tiêu chuẩn này không phản ánh tầm quan trọng của chúng hay hàm ý thứ tự mà chúng sẽ được thực hiện. Các danh mục được liệt kê chỉ nhằm mục đích tham khảo.

ISO/IEC 27000 mô tả tổng quan và từ vựng của các hệ thống quản lý an toàn thông tin, tham khảo bộ tiêu chuẩn hệ thống quản lý an toàn thông tin (bao gồm ISO/IEC 27003, ISO/IEC 27004 và ISO/IEC 27005), với các thuật ngữ và định nghĩa liên quan.

0.2 Tương thích với các tiêu chuẩn hệ thống quản lý khác

Tiêu chuẩn này áp dụng cấu trúc cấp cao, cùng tiêu đề điều con, đoạn văn, thuật ngữ chung và định nghĩa cốt lõi được xác định trong Phụ lục SL của Các chỉ dẫn ISO/IEC, Phần 1, Phần Bổ sung ISO hợp nhất, và do đó duy trì sự tương thích với các tiêu chuẩn hệ thống quản lý khác đã áp dụng Phụ lục SL.

Cách tiếp cận phổ biến được xác định trong Phụ lục SL này sẽ hữu ích cho những tổ chức lựa chọn vận hành một hệ thống quản lý duy nhất đáp ứng yêu cầu của hai hoặc nhiều tiêu chuẩn hệ thống quản lý.

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

Information technology - Security techniques - Infornaton security management systems - Requirements

1 Phạm vi áp dụng

Tiêu chuẩn này quy định các yêu cầu đối với hoạt động thiết lập triển khai, duy trì và cải tiến liên tục hệ thống quản lý an toàn thông tin trong bối cảnh của một tổ chức. Tiêu chuẩn này cũng bao gồm các yêu cầu cho việc đánh giá và xử lý rủi ro an toàn thông tin phù hợp với yêu cầu của tổ chức. Các yêu cầu đặt ra trong tiêu chuẩn này mang tính chất tổng quan và nhằm áp dụng cho tất cả các tổ chức, không phân biệt loại hình, quy mô hay bản chất. Điều 4 đến Điều 10 của tiêu chuẩn là bắt buộc nếu một tổ chức công bố phù hợp với tiêu chuẩn này.

2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau đây là cần thiết để áp dụng tiêu chuẩn này. Đối với các tài liệu viện dẫn ghi năm công bố thì áp dụng phiên bản được nêu. Đối với các tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất (bao gồm cả các sửa đổi, bổ sung).

TCVN 11238:2015 (ISO/IEC 27000:2014), *Công nghệ thông tin - Các kỹ thuật an toàn - Hệ thống quản lý an toàn thông tin - Tổng quan và từ vựng (Information technology - Security techniques - Information security management systems - Overview and vocabulary).*

3 Thuật ngữ và định nghĩa

Tiêu chuẩn này sử dụng các thuật ngữ và định nghĩa nêu trong TCVN 11238:2015 (ISO/IEC 27000:2014).

4 Bối cảnh của tổ chức

4.1 Hiểu tổ chức và bối cảnh của tổ chức

Tổ chức cần xác định các vấn đề nội bộ và bên ngoài liên quan đến mục đích của tổ chức và có ảnh hưởng đến khả năng đạt được kết quả mong muốn của hệ thống quản lý an toàn thông tin của tổ chức.

CHÚ THÍCH: Việc xác định những vấn đề liên quan tới thiết lập phạm vi nội bộ và bên ngoài của tổ chức được nêu tại Điều 5.3 của TCVN ISO 31000:2011 (ISO 31000:2009) [5].

4.2 Hiểu được nhu cầu và mong đợi của các bên liên quan

Tổ chức phải xác định:

a) các bên có liên quan đến hệ thống quản lý an toàn thông tin;

b) các yêu cầu về an toàn thông tin của các bên có liên quan này.

CHÚ THÍCH: Các yêu cầu của các bên liên quan có thể bao gồm các yêu cầu pháp lý, quy định quản lý và các nghĩa vụ hợp đồng.

4.3 Xác định phạm vi của hệ thống quản lý an toàn thông tin

Tổ chức phải xác định các giới hạn và khả năng áp dụng hệ thống quản lý an toàn thông tin để thiết lập phạm vi hệ thống.

Khi xác định phạm vi hệ thống, tổ chức phải soát xét:

a) các vấn đề nội bộ và bên ngoài được nêu trong Điều 4.1;

b) các yêu cầu được nêu trong Điều 4.2;

c) sự tương tác và phụ thuộc giữa các hoạt động được thực hiện bởi tổ chức, và những hoạt động được thực hiện bởi tổ chức khác.

Phạm vi này phải sẵn có dưới dạng thông tin dạng văn bản.

4.4 Hệ thống quản lý an toàn thông tin

Tổ chức phải thiết lập, triển khai, duy trì và cải tiến liên tục hệ thống quản lý an toàn thông tin phù hợp với các yêu cầu của tiêu chuẩn này.

5 Sự lãnh đạo

5.1 Sự lãnh đạo và cam kết

Lãnh đạo cao nhất phải chứng tỏ sự lãnh đạo và cam kết đối với hệ thống quản lý an toàn thông tin bằng cách:

a) bảo đảm chính sách an toàn thông tin và các mục tiêu an toàn thông tin được thiết lập và thích hợp với định hướng chiến lược của tổ chức;

b) đảm bảo tích hợp các yêu cầu của hệ thống quản lý an toàn thông tin vào các quy trình xử lý của tổ chức;

c) đảm bảo rằng các nguồn lực cần thiết cho hệ thống quản lý an toàn thông tin luôn sẵn có;

d) truyền thông về tầm quan trọng của quản lý an toàn thông tin hiệu quả và tầm quan trọng của việc tuân thủ các yêu cầu hệ thống quản lý an toàn thông tin;

e) đảm bảo hệ thống quản lý an toàn thông tin đạt kết quả như dự kiến;

f) chỉ đạo và hỗ trợ nhân sự đóng góp cho hiệu quả của hệ thống quản lý an toàn thông tin;

g) thúc đẩy cải tiến liên tục;

h) hỗ trợ các cán bộ quản lý có liên quan nhằm chứng minh khả năng lãnh đạo của họ trong lĩnh vực mà họ chịu trách nhiệm quản lý.

5.2 Chính sách

Lãnh đạo cao nhất phải thiết lập một chính sách an toàn thông tin:

a) phù hợp với mục đích của tổ chức;

b) bao gồm các mục tiêu an toàn thông tin (xem 6.2) hoặc cung cấp khuôn khổ cho việc thiết lập các mục tiêu an toàn thông tin;

c) bao gồm một cam kết để đáp ứng các yêu cầu liên quan đến an toàn thông tin;

d) bao gồm một cam kết nhằm cải tiến liên tục hệ thống quản lý an toàn thông tin.

Chính sách an toàn thông tin phải:

e) sẵn có bằng thông tin dạng văn bản;

f) được truyền thông trong phạm vi tổ chức;

g) sẵn có cho các bên liên quan, khi phù hợp.

5.3 Vai trò, trách nhiệm và quyền hạn của tổ chức

Lãnh đạo cao nhất phải đảm bảo rằng các trách nhiệm và quyền hạn của các vai trò liên quan đến an toàn thông tin là được giao và truyền thông.

Lãnh đạo cao nhất phải phân công trách nhiệm và quyền hạn để:

a) đảm bảo rằng hệ thống quản lý an toàn thông tin phù hợp với các yêu cầu của tiêu chuẩn này;

b) báo cáo hiệu năng của hệ thống quản lý an toàn thông tin tới lãnh đạo cao nhất.

CHÚ THÍCH: Lãnh đạo cao nhất cũng có thể phân công trách nhiệm và quyền hạn cho việc báo cáo hiệu năng của hệ thống quản lý an toàn thông tin trong tổ chức.

6 Hoạch định

6.1 Hành động để xác định các rủi ro và các cơ hội tích cực

6.1.1 Tổng quan

Khi hoạch định cho hệ thống quản lý an toàn thông tin, tổ chức phải soát xét các vấn đề được đưa ra trong 4.1 và các yêu cầu được đưa ra trong 4.2 và xác định các rủi ro và cơ hội cải tiến cần được giải quyết để:

a) đảm bảo hệ thống quản lý an toàn thông tin có thể đạt được kết quả như dự kiến;

b) ngăn chặn, hoặc làm giảm các tác động không mong muốn;

c) được cải tiến liên tục.

Tổ chức phải hoạch định:

d) các hành động để giải quyết các rủi ro và cơ hội cải tiến;

e) cách thức để:

1) tích hợp và triển khai các hành động này vào các quy trình của hệ thống quản lý an toàn thông tin của tổ chức;

2) đánh giá hiệu quả của những hành động này.

6.1.2 Đánh giá rủi ro an toàn thông tin

Tổ chức phải xác định và áp dụng một quy trình đánh giá rủi ro an toàn thông tin nhằm:

a) thiết lập và duy trì các tiêu chí về rủi ro an toàn thông tin bao gồm:

1) các tiêu chí chấp nhận rủi ro;

2) các tiêu chí để thực hiện đánh giá rủi ro an toàn thông tin;

b) đảm bảo rằng đánh giá rủi ro an toàn thông tin được lặp lại tạo ra kết quả nhất quán, hợp lệ và có khả năng so sánh;

c) xác định các rủi ro an toàn thông tin:

1) áp dụng quy trình đánh giá rủi ro an toàn thông tin để xác định các rủi ro liên quan đến việc mất tính bí mật, tính toàn vẹn và tính sẵn sàng của thông tin trong phạm vi của hệ thống quản lý an toàn thông tin;

2) xác định chủ thể rủi ro;

d) phân tích các rủi ro an toàn thông tin:

1) đánh giá các hậu quả tiềm ẩn nếu các rủi ro được xác định tại 6.1.2 c) 1) xảy ra;

2) đánh giá khả năng xảy ra của các rủi ro được xác định tại 6.1.2 c) 1);

3) xác định các mức độ rủi ro;

e) đánh giá các rủi ro an toàn thông tin:

1) so sánh kết quả phân tích rủi ro với tiêu chí rủi ro được đưa ra trong 6.1.2 a);

2) ưu tiên các rủi ro được phân tích để xử lý rủi ro.

Tổ chức phải lưu giữ thông tin dạng văn bản về quy trình đánh giá rủi ro an toàn thông tin.

6.1.3 Xử lý rủi ro an toàn thông tin

Tổ chức phải xác định và áp dụng một quy trình xử lý rủi ro an toàn thông tin để:

a) lựa chọn các tùy chọn xử lý rủi ro an toàn thông tin phù hợp, có tính đến các kết quả đánh giá rủi ro;

b) xác định tất cả các biện pháp kiểm soát cần thiết để thực hiện các phương án xử lý rủi ro an toàn thông tin đã được lựa chọn;

CHÚ THÍCH: Tổ chức có thể thiết kế các biện pháp kiểm soát theo yêu cầu, hoặc nhận diện chúng từ bất kỳ nguồn nào.

c) so sánh các biện pháp kiểm soát được xác định trong 6.1.3 b) ở trên với các điều đưa ra trong Phụ lục A và xác minh rằng không có biện pháp kiểm soát cần thiết nào bị bỏ qua.

CHÚ THÍCH 1: Phụ lục A chứa một danh sách tổng hợp các mục tiêu kiểm soát và các biện pháp kiểm soát. Người dùng tiêu chuẩn được trỏ tới Phụ lục A để đảm bảo không bỏ qua các kiểm soát cần thiết.

CHÚ THÍCH 2: Các mục tiêu kiểm soát mặc định bao gồm trong các biện pháp kiểm soát đã lựa chọn. Các mục tiêu kiểm soát và các biện pháp kiểm soát được liệt kê trong Phụ lục A là không đầy đủ hết mọi khía cạnh và có thể được bổ sung khi cần thiết.

d) đưa ra một Bản tuyên bố về khả năng áp dụng, bao gồm:

- các biện pháp kiểm soát cần thiết (xem 6.1.3 b) và c));
- các lý giải cho việc đưa các biện pháp đó vào;
- bất kể các biện pháp kiểm soát cần thiết có được triển khai hay không; và
- các lý giải cho việc bỏ qua các biện pháp kiểm soát trong Phụ lục A.

e) xây dựng một kế hoạch xử lý rủi ro an toàn thông tin;

f) đạt được sự chấp thuận của chủ sở hữu rủi ro về kế hoạch xử lý rủi ro an toàn thông tin và chấp nhận các rủi ro an toàn thông tin còn tồn tại.

Tổ chức phải lưu giữ lại thông tin dạng văn bản về quy trình xử lý rủi ro an toàn thông tin.

CHÚ THÍCH: Quy trình xử lý và đánh giá rủi ro an toàn thông tin trong tiêu chuẩn gắn với các nguyên tắc và hướng dẫn chung được cung cấp trong TCVN 31000:2011.

6.2 Các mục tiêu an toàn thông tin và hoạch định để thực hiện mục tiêu.

Tổ chức phải thiết lập các mục tiêu an toàn thông tin ở các chức năng và mức độ thích hợp.

Các mục tiêu an toàn thông tin phải:

a) phù hợp với chính sách an toàn thông tin;

b) có thể đo lường được (nếu có thể);

c) soát xét các yêu cầu về an toàn thông tin sẵn có và các kết quả từ việc đánh giá và xử lý rủi ro;

d) được truyền thông;

e) phải được cập nhật phù hợp.

Tổ chức phải lưu trữ thông tin dạng văn bản về các mục tiêu an toàn thông tin.

Khi lập kế hoạch để đạt được mục tiêu an toàn thông tin, tổ chức phải xác định:

f) những gì sẽ được thực hiện;

g) những nguồn lực sẽ được yêu cầu;

h) người sẽ chịu trách nhiệm;

i) thời điểm sẽ được hoàn thành;

j) kết quả sẽ được đánh giá như thế nào.

7 Hỗ trợ

7.1 Nguồn lực

Tổ chức phải xác định và cung cấp nguồn nhân lực cần thiết cho việc thiết lập, triển khai, duy trì và cải tiến liên tục hệ thống quản lý an toàn thông tin.

7.2 Năng lực

Tổ chức phải:

a) xác định năng lực cần thiết của người làm việc dưới sự kiểm soát của tổ chức có ảnh hưởng tới hiệu năng an toàn thông tin;

b) đảm bảo rằng những người có năng lực căn cứ trên cơ sở quá trình giáo dục, đào tạo hoặc kinh nghiệm;

c) khi thích hợp, tiến hành các hành động để có được các năng lực cần thiết, và đánh giá hiệu quả của các hành động đã thực hiện;

d) lưu trữ thông tin dạng văn bản thích hợp như là một bằng chứng cho năng lực.

CHÚ THÍCH: các hành động có thể áp dụng được bao gồm, ví dụ: cung cấp đào tạo, cố vấn, hoặc phân công lại lao động hiện có; hoặc tuyển dụng hoặc ký kết hợp đồng của người đủ năng lực.

7.3 Nhận thức

Người lao động làm việc dưới sự kiểm soát của tổ chức phải nhận thức:

a) chính sách an toàn thông tin;

b) đóng góp vào hiệu quả của hệ thống quản lý an toàn thông tin, bao gồm lợi ích của việc cải tiến an toàn thông tin;

c) những tác động của sự không phù hợp với các yêu cầu hệ thống quản lý an toàn thông tin.

7.4 Trao đổi thông tin

Tổ chức phải xác định nhu cầu trao đổi thông tin nội bộ và bên ngoài có liên quan tới hệ thống quản lý an toàn thông tin bao gồm:

a) trao đổi thông tin gì;

b) trao đổi thông tin khi nào;

c) trao đổi thông tin với ai;

d) ai là người trao đổi thông tin;

e) các quá trình mà trao đổi thông tin có tác dụng.

7.5 Thông tin dạng văn bản

7.5.1 Khái quát

Hệ thống quản lý an toàn thông tin của tổ chức phải gồm:

a) thông tin dạng văn bản được yêu cầu bởi tiêu chuẩn này; và

b) thông tin dạng văn bản được tổ chức xác định là cần thiết cho hiệu quả của hệ thống quản lý an toàn thông tin.

CHÚ THÍCH: Mức độ thông tin dạng văn bản cho một hệ thống quản lý an toàn thông tin có thể khác nhau giữa các tổ chức do:

1) quy mô của tổ chức và loại hình hoạt động, các quy trình, sản phẩm và dịch vụ của tổ chức đó;

2) sự phức tạp và sự tương tác của của các quá trình;

3) năng lực của con người.

7.5.2 Tạo lập và cập nhật

Khi tạo lập và cập nhật thông tin dạng văn bản, tổ chức phải đảm bảo phù hợp:

a) định danh và mô tả (ví dụ: tiêu đề, ngày, tác giả hoặc mã số tài liệu);

b) định dạng (ví dụ: ngôn ngữ, phiên bản phần mềm, đồ họa) và phương tiện truyền thông (ví dụ: giấy, điện tử);

c) soát xét và chấp thuận cho phù hợp và đầy đủ.

7.5.3 Kiểm soát thông tin dạng văn bản

Thông tin dạng văn bản theo yêu cầu của hệ thống quản lý an toàn thông tin và tiêu chuẩn này phải được kiểm soát để đảm bảo:

a) sẵn có và phù hợp để sử dụng tại mọi thời điểm và vị trí khi cần thiết;

b) được bảo vệ một cách đầy đủ (ví dụ: khỏi việc mất tính bí mật, sử dụng không đúng cách, hoặc mất tính toàn vẹn).

Để kiểm soát thông tin dạng văn bản, tổ chức phải lưu ý các hoạt động sau đây, khi thực hiện:

c) phân phối, truy cập, thu hồi và sử dụng;

d) bảo quản và lưu trữ, bao gồm cả việc duy trì tính rõ ràng;

e) kiểm soát các thay đổi (ví dụ kiểm soát phiên bản);

f) duy trì và hủy bỏ.

Thông tin dạng văn bản có nguồn gốc bên ngoài mà được tổ chức xác định là cần thiết cho việc hoạch định và vận hành hệ thống quản lý an toàn thông tin phải được xác định phù hợp, và được kiểm soát.

CHÚ THÍCH: Truy cập bao gồm việc chỉ cho phép xem các thông tin dạng văn bản hoặc cho phép vừa xem và vừa chỉnh sửa thông tin dạng văn bản...

8 Vận hành

8.1 Hoạch định và kiểm soát vận hành.

Tổ chức phải hoạch định, thực hiện và kiểm soát các quá trình cần thiết để đáp ứng các yêu cầu an toàn thông tin và triển khai các hành động được xác định trong 6.1. Tổ chức cũng phải thực hiện các kế hoạch để đạt được các mục tiêu an toàn thông tin được xác định trong 6.2.

Tổ chức phải lưu giữ thông tin dạng văn bản ở mức độ cần thiết để có thể tin tưởng được rằng các quy trình đã được thực hiện như kế hoạch.

Tổ chức phải kiểm soát những thay đổi đã được hoạch định và soát xét các kết quả của những thay đổi ngoài ý muốn, thực hiện hành động để giảm thiểu bất kỳ tác động bất lợi, nếu cần.

Tổ chức phải đảm bảo rằng các quy trình được thuê ngoài được xác định và kiểm soát.

8.2 Đánh giá rủi ro an toàn thông tin

Tổ chức phải thực hiện đánh giá rủi ro an toàn thông tin định kỳ theo kế hoạch hoặc khi có sự thay đổi đáng kể xảy ra hoặc được đề xuất, có tính đến các tiêu chí được thiết lập trong 6.1.2 a).

Tổ chức phải lưu giữ thông tin dạng văn bản về kết quả đánh giá rủi ro an toàn thông tin.

8.3 Xử lý rủi ro an toàn thông tin

Tổ chức phải thực hiện các kế hoạch xử lý rủi ro an toàn thông tin.

Tổ chức phải lưu giữ thông tin dạng văn bản về kết quả xử lý rủi ro an toàn thông tin.

9 Đánh giá hiệu năng

9.1 Giám sát, đo lường, phân tích và đánh giá

Tổ chức phải đánh giá hiệu năng an toàn thông tin và hiệu quả của hệ thống quản lý an toàn thông tin.

Tổ chức phải xác định:

a) những gì cần phải được giám sát và đo lường, bao gồm cả các quy trình và biện pháp kiểm soát an toàn thông tin;

b) các phương pháp giám sát, đo lường, phân tích và đánh giá có thể áp dụng để đảm bảo kết quả hợp lệ;

CHÚ THÍCH: các phương pháp được lựa chọn được coi là hợp lệ phải cho kết quả có thể lặp lại và so sánh được.

c) thời điểm giám sát và đo lường được thực hiện;

d) người sẽ giám sát và đo lường;

e) thời điểm kết quả từ việc giám sát và đo lường phải được phân tích và đánh giá;

f) người sẽ phân tích và đánh giá các kết quả này.

Tổ chức phải giữ lại thông tin dạng văn bản thích hợp làm bằng chứng về các kết quả đo lường và giám sát.

9.2 Đánh giá nội bộ

Tổ chức phải thực hiện đánh giá nội bộ theo kế hoạch để cung cấp thông tin về hệ thống quản lý an toàn thông tin:

a) phù hợp với

1) các yêu cầu của riêng tổ chức cho hệ thống quản lý an toàn thông tin của họ;

2) các yêu cầu của tiêu chuẩn này;

b) được thực hiện và duy trì hiệu quả.

Tổ chức phải có trách nhiệm:

c) hoạch định, thiết lập, thực hiện và duy trì một (nhiều) chương trình kiểm toán, bao gồm tần suất, phương pháp, trách nhiệm, các yêu cầu kế hoạch và báo cáo. Các chương trình đánh giá sẽ phải soát xét tầm quan trọng của quá trình có liên quan và kết quả các cuộc đánh giá trước đó;

d) xác định phạm vi và tiêu chí đánh giá cho mỗi đợt đánh giá;

e) lựa chọn các đánh giá viên và thực hiện các cuộc đánh giá nhằm đảm bảo tính khách quan và tính công bằng của quá trình đánh giá;

f) đảm bảo rằng các kết quả đánh giá đã được báo cáo tới cấp quản lý có liên quan;

g) lưu trữ thông tin dạng văn bản làm bằng chứng về các chương trình đánh giá và kết quả đánh giá.

9.3 Soát xét của lãnh đạo

Lãnh đạo cao nhất phải soát xét hệ thống quản lý an toàn thông tin của tổ chức theo kế hoạch đã định để luôn đảm bảo tính phù hợp, đầy đủ và có hiệu quả.

Việc soát xét của lãnh đạo cao nhất phải bao gồm các vấn đề:

a) tình trạng của các hành động từ những soát xét của lãnh đạo trước đó;

b) những thay đổi trong các vấn đề nội bộ và bên ngoài có liên quan đến hệ thống quản lý an toàn thông tin;

c) phản hồi về hiệu năng an toàn thông tin, bao gồm cả xu hướng về:

1) sự không phù hợp và các hành động khắc phục;

2) các kết quả đo lường và giám sát;

3) các kết quả đánh giá;

4) việc hoàn thành các mục tiêu an toàn thông tin;

d) phản hồi từ các bên liên quan;

e) các kết quả đánh giá rủi ro và tình trạng của kế hoạch xử lý rủi ro;

f) các cơ hội cải tiến liên tục.

Đầu ra sự soát xét của lãnh đạo phải bao gồm các quyết định liên quan đến các cơ hội cải tiến liên tục và bất cứ nhu cầu nào cho việc thay đổi hệ thống quản lý an toàn thông tin.

Tổ chức phải lưu giữ thông tin dạng văn bản làm bằng chứng về các kết quả soát xét của lãnh đạo.

10 Cải tiến

10.1 Sự không phù hợp và hành động khắc phục

Khi xảy ra sự không phù hợp, tổ chức phải:

a) ứng phó với sự không phù hợp, và có thể:

   1) đưa ra hành động để kiểm soát và sửa đổi;

   2) xử lý các hệ quả;

b) đánh giá sự cần thiết cho hành động để loại bỏ các nguyên nhân của sự không phù hợp, nhằm không để tái diễn hay xảy ra ở những nơi khác, bằng cách:

   1) soát xét sự không phù hợp;

   2) xác định các nguyên nhân của sự không phù hợp;

   3) xác định nếu có sự không phù hợp tương tự tồn tại, hoặc có khả năng có thể xảy ra;

c) thực hiện mọi hành động cần thiết;

d) soát xét tính hiệu quả của mọi hành động khắc phục đang được thực hiện;

e) thực hiện các thay đổi với hệ thống quản lý an toàn thông tin, nếu cần thiết.

Các hành động khắc phục phải phù hợp với các tác động của sự không phù hợp đang gặp phải.

Tổ chức phải lưu giữ thông tin dạng văn bản để làm bằng chứng cho:

f) bản chất của sự không phù hợp và mọi hành động tiếp theo được thực hiện;

g) các kết quả của bất kỳ hành động khắc phục nào.

10.2 Cải tiến liên tục

Tổ chức phải liên tục cải tiến hệ thống quản lý an toàn thông tin cho phù hợp, đầy đủ và hiệu quả.

Phụ lục A

(Quy định)

Các mục tiêu kiểm soát và biện pháp kiểm soát tham chiếu

Các mục tiêu kiểm soát và biện pháp kiểm soát được liệt kê trong Bảng A.1 dưới đây được dẫn xuất trực tiếp và liên kết với các điều từ Điều 5 đến Điều 18 trong tiêu chuẩn ISO/IEC 27002:2013 và sẽ được sử dụng trong bối cảnh của 6.1.3.

Bảng A.1 – Các mục tiêu kiểm soát và biện pháp kiểm soát

A.5 Các chính sách an toàn thông tin		
A.5.1 Định hướng quản lý an toàn thông tin		
Mục tiêu: Nhằm cung cấp định hướng quản lý và hỗ trợ đảm bảo an toàn thông tin phù hợp với các yêu cầu trong hoạt động nghiệp vụ, môi trường pháp lý và các quy định phải tuân thủ.		
A.5.1.1	Các chính sách an toàn thông tin	Biện pháp kiểm soát Một tập hợp các chính sách an toàn thông tin cần được xác định, do ban quản lý phê duyệt, được công bố và thông báo cho nhân viên và các đối tác bên ngoài có liên quan.
A.5.1.2	Soát xét các chính sách an toàn thông tin	Biện pháp kiểm soát Cần soát xét các chính sách an toàn thông tin định kỳ theo kế hoạch hoặc khi có sự thay đổi đáng kể xảy ra để luôn đảm bảo sự phù hợp, đầy đủ và hiệu quả.
A.6 Tổ chức đảm bảo an toàn thông tin		
A.6.1 Tổ chức nội bộ		
Mục tiêu: Thiết lập một khuôn khổ quản lý nhằm khởi tạo và kiểm soát việc thực hiện và hoạt động của an toàn thông tin trong tổ chức.		
A.6.1.1	Các vai trò và trách nhiệm đảm bảo an toàn thông tin	Biện pháp kiểm soát Tất cả các trách nhiệm an toàn thông tin phải được định nghĩa và phân phối.
A.6.1.2	Sự phân tách	Biện pháp kiểm soát

		Các nhiệm vụ và phạm vi trách nhiệm đối lập nhau phải được phân tách nhằm giảm thiểu khả năng sửa đổi trái phép hoặc vô tình, hoặc lạm dụng tài sản của tổ chức.
A.6.1.3	Liên lạc với những cơ quan/tổ chức có thẩm quyền	Biện pháp kiểm soát Cần duy trì kênh liên lạc thích hợp với các cơ quan có thẩm quyền liên quan.
A.6.1.4	Liên lạc với các nhóm chuyên gia	Biện pháp kiểm soát Cần duy trì liên lạc đầy đủ với các nhóm chuyên gia chuyên sâu hoặc các diễn đàn và các hiệp hội về an toàn thông tin.
A.6.1.5	An toàn thông tin trong quản lý dự án	Biện pháp kiểm soát An toàn thông tin cần được gắn với quản lý dự án, và bất kì loại dự án nào.
A.6.2 Các thiết bị di động và làm việc từ xa		
Mục tiêu: Nhằm đảm bảo an toàn khi làm việc từ xa và sử dụng các thiết bị di động.		
A.6.2.1	Chính sách đối với thiết bị di động	Biện pháp kiểm soát Một chính sách và các biện pháp hỗ trợ an toàn cần được áp dụng để quản lý các rủi ro được đã được nêu ra khi sử dụng các thiết bị di động.
A.6.2.2	Làm việc từ xa	Biện pháp kiểm soát Một chính sách và các biện pháp hỗ trợ an toàn cần được thực hiện để bảo vệ thông tin được truy nhập, xử lý hoặc được lưu trữ tại các nơi làm việc từ xa.
A.7 An toàn nguồn nhân lực		
A.7.1 Trước khi tuyển dụng		
Mục tiêu: Để đảm bảo rằng các nhân viên và các nhà tuyển dụng nhận thức được và thực hiện trách nhiệm bảo mật thông tin của họ.		
A.7.1.1	Thẩm tra	Biện pháp kiểm soát Việc xác minh lý lịch của tất cả các ứng viên tuyển dụng

		phải được thực hiện phù hợp theo quy định của pháp luật, các quy định và đạo đức có liên quan và phải tỷ lệ thuận với các yêu cầu của công việc, phân loại thông tin được truy nhập và các rủi ro có thể nhận thấy được.
A.7.1.2	Các điều khoản và điều kiện tuyển dụng	Biện pháp kiểm soát Các thỏa thuận hợp đồng giữa nhân viên và người ký kết hợp đồng phải được ghi rõ trách nhiệm của người được tuyển dụng và tổ chức tuyển dụng trong việc đảm bảo an toàn thông tin.
A.7.2 Trong thời gian làm việc		
Mục tiêu: Đảm bảo rằng mọi nhân viên và nhà tuyển dụng nhận thức được và thực hiện trách nhiệm bảo mật an toàn thông tin của họ.		
A.7.2.1	Trách nghiệm của ban quản lý	Biện pháp kiểm soát Ban quản lý phải yêu cầu tất cả nhân viên và nhà thầu áp dụng an toàn thông tin phù hợp với các chính sách và thủ tục an toàn thông tin đã được thiết lập của tổ chức.
A.7.2.2	Nhận thức, giáo dục và đào tạo về an toàn thông tin	Biện pháp kiểm soát Tất cả nhân viên trong tổ chức và, nếu có thể, các nhà thầu có liên quan cần phải được giáo dục và đào tạo nâng cao nhận thức thích hợp và cập nhật thường xuyên các chính sách và thủ tục của tổ chức, nếu phù hợp với chức năng công việc của họ.
A.7.2.3	Xử lý kỷ luật	Biện pháp kiểm soát Phải có hình thức xử lý kỷ luật chính thức và công khai nhằm ngăn chặn kịp thời các nhân viên vi phạm an toàn thông tin.
A.7.3 Chấm dứt hoặc thay đổi công việc		
Mục tiêu: Bảo vệ lợi ích của tổ chức trong quá trình thay đổi hoặc chấm dứt công việc.		
A.7.3.1	Trách nhiệm chấm dứt hoặc thay đổi	Biện pháp kiểm soát Trách nhiệm và nghĩa vụ bảo vệ an toàn thông tin vẫn có

	việc làm	hiệu lực sau khi chấm dứt hoặc thay đổi việc làm phải được xác định, được thông báo tới nhân viên hoặc nhà thầu và phải được thi hành.
A.8 Quản lý tài sản		
A.8.1 Trách nhiệm đối với tài sản		
Mục tiêu: Nhằm xác định tài sản của tổ chức và xác định các trách nhiệm bảo vệ thích hợp.		
A.8.1.1	Kiểm kê tài sản	Biện pháp kiểm soát Thông tin, tất cả tài sản khác liên quan đến thông tin và phương tiện xử lý thông tin phải được xác định và việc kiểm kê các tài sản này phải được thiết lập và duy trì.
A.8.1.2	Quyền sở hữu tài sản	Biện pháp kiểm soát Các tài sản được duy trì trong bảng kiểm kê phải có chủ sở hữu.
A.8.1.3	Sử dụng hợp lý tài sản	Biện pháp kiểm soát Các quy định về việc sử dụng hợp lý thông tin và sử dụng các tài sản gắn liền với thiết bị xử lý thông tin và thông tin phải được xác định, được ghi thành văn bản và được triển khai.
A.8.1.4	Bàn giao tài sản	Biện pháp kiểm soát Tất cả nhân viên và người sử dụng bên ngoài phải hoàn trả tất cả tài sản của tổ chức sở hữu tài sản đó khi chấm dứt việc làm, hợp đồng hay thỏa thuận của họ.
A.8.2 Phân loại thông tin		
Mục tiêu: Nhằm đảm bảo rằng thông tin sẽ có mức độ bảo vệ phù hợp theo tầm quan trọng của thông tin với tổ chức.		
A.8.2.1	Phân loại thông tin	Biện pháp kiểm soát Thông tin cần được phân loại dựa trên các yêu cầu pháp lý, giá trị, mức độ quan trọng và độ nhạy cảm với việc tiết lộ hoặc sửa đổi trái phép.

A.8.2.2	Dán nhãn thông tin	Biện pháp kiểm soát Một tập hợp các thủ tục về việc dán nhãn thông tin một cách hợp lý cần được phát triển và triển khai phù hợp với kế hoạch phân loại thông tin đã được tổ chức thông qua.
A.8.2.3	Xử lý tài sản	Biện pháp kiểm soát Cần phải xây dựng và triển khai các thủ tục xử lý tài sản phù hợp với kế hoạch phân loại thông tin đã được tổ chức thông qua.
A.8.3 Thông tin và các phương tiện xử lý thông tin		
Mục tiêu: Nhằm ngăn ngừa việc tiết lộ, sửa đổi, xóa bỏ hoặc phá hoại trái phép thông tin được lưu trữ trên phương tiện truyền thông.		
A.8.3.1	Quản lý phương tiện truyền thông có thể di dời	Biện pháp kiểm soát Cần triển khai các thủ tục quản lý các phương tiện có thể di dời phù hợp với cơ cấu phân loại đã được tổ chức thông qua.
A.8.3.2	Loại bỏ các phương tiện truyền thông	Biện pháp kiểm soát Các phương tiện cần được loại bỏ một cách an toàn khi không còn cần thiết theo các thủ tục xử lý chính thức.
A.8.3.3	Vận chuyển phương tiện vật lý	Biện pháp kiểm soát Phương tiện truyền thông có chứa thông tin phải được bảo vệ chống lại sự truy cập trái phép, sử dụng sai mục đích hoặc làm hư hỏng trong quá trình vận chuyển.
A.9 Quản lý truy cập		
A.9.1 Các yêu cầu nghiệp vụ cho việc kiểm soát truy cập		
Mục tiêu: Nhằm giới hạn quyền truy cập vào các phương tiện xử lý thông tin và thông tin.		
A.9.1.1	Chính sách quản lý truy cập	Biện pháp kiểm soát Một chính sách quản lý truy cập phải được thiết lập, được ghi thành văn bản và soát xét dựa trên các yêu cầu nghiệp vụ và an toàn thông tin.

A.9.1.2	Truy cập vào hệ thống mạng và các dịch vụ mạng	Biện pháp kiểm soát Người dùng chỉ được cấp quyền truy cập vào mạng và các dịch vụ mạng mà họ đã được cấp quyền sử dụng cụ thể.
A.9.2 Quản lý truy cập người dùng		
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 tới các hệ thống và dịch vụ thông tin.		
A.9.2.1	Đăng ký và xóa đăng ký thành viên	Biện pháp kiểm soát Quy trình đăng ký và xóa đăng ký thành viên chính thức phải được thực hiện để cho phép gán các quyền truy cập hợp lệ.
A.9.2.2	Cấp phát quyền truy cập người dùng	Biện pháp kiểm soát Quy trình cấp phát quyền truy cập người dùng chính thức phải được triển khai để gán hoặc thu hồi quyền truy cập cho tất cả loại người sử dụng tới tất cả các hệ thống và dịch vụ.
A.9.2.3	Quản lý đặc quyền truy cập	Biện pháp kiểm soát Việc cấp phát và sử dụng các đặc quyền truy cập phải được giới hạn và kiểm soát.
A.9.2.4	Quản lý thông tin xác thực bí mật người dùng	Biện pháp kiểm soát Việc cấp phát thông tin xác thực bí mật phải được kiểm soát thông qua quá trình quản lý chính thức.
A.9.2.5	Soát xét quyền truy cập người dùng	Biện pháp kiểm soát Chủ sở hữu tài sản cần định kỳ soát xét các quyền truy cập của người dùng.
A.9.2.6	Hủy bỏ hoặc điều chỉnh quyền truy cập	Biện pháp kiểm soát Quyền truy cập của tất cả người lao động và người sử dụng bên ngoài vào các phương tiện xử lý thông tin và thông tin phải được dỡ bỏ sau khi chấm dứt công việc, hợp đồng hoặc thoả thuận của họ, hoặc phải điều chỉnh khi thay đổi.

A.9.3 Trách nhiệm của người sử dụng		
Mục tiêu: Nhằm làm cho người dùng có trách nhiệm đảm bảo an toàn thông tin xác thực của họ.		
A.9.3.1	Sử dụng thông tin xác thực bí mật	Biện pháp kiểm soát Người dùng phải được yêu cầu tuân thủ quy tắc thực hành của tổ chức trong quá trình sử dụng thông tin xác thực bí mật.
A.9.4 Quản lý truy cập vào hệ thống và ứng dụng		
Mục tiêu: Nhằm ngăn chặn truy cập trái phép vào các hệ thống và ứng dụng.		
A.9.4.1	Hạn chế truy cập thông tin	Biện pháp kiểm soát Truy cập 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 xác định.
A.9.4.2	Các thủ tục đăng nhập an toàn	Biện pháp kiểm soát Khi có yêu cầu của chính sách quản lý truy cập, việc truy cập đến các hệ thống và ứng dụng cần được kiểm soát bởi thủ tục đăng nhập an toàn.
A.9.4.3	Hệ thống quản lý mật khẩu	Biện pháp kiểm soát Các hệ thống quản lý mật khẩu phải có khả năng tương tác và đảm bảo độ khó của mật khẩu.
A.9.4.4	Sử dụng các chương trình tiện ích ưu tiên	Biện pháp kiểm soát Việc sử dụng các chương trình tiện ích có khả năng ảnh hưởng đến các biện pháp kiểm soát ứng dụng và hệ thống phải được giới hạn và kiểm soát chặt chẽ.
A.9.4.5	Kiểm soát truy cập vào mã nguồn của chương trình	Biện pháp kiểm soát Việc truy cập đến mã nguồn của chương trình cần được giới hạn chặt chẽ.
A.10 Mật mã		
A.10.1 Biện pháp kiểm soát mật mã		

Mục tiêu: Đảm bảo sử dụng phù hợp và hiệu quả mật mã để bảo vệ tính bí mật, tính xác thực và/hoặc tính toàn vẹn của thông tin.		
A.10.1.1	Chính sách sử dụng các biện pháp kiểm soát mật mã	Biện pháp kiểm soát Một chính sách về việc sử dụng các biện pháp kiểm soát mật mã để bảo vệ thông tin cần được xây dựng và triển khai.
A.10.1.2	Quản lý khóa	Biện pháp kiểm soát Cần xây dựng và triển khai chính sách sử dụng, bảo vệ và thời gian tồn tại của khóa mật mã trong suốt toàn bộ vòng đời của chúng.
A.11 Đảm bảo an toàn vật lý và môi trường		
A.11.1 Khu vực an toàn		
Mục tiêu: Nhằm ngăn chặn truy cập vật lý trái phép, gây thiệt hại và can thiệp tới các phương tiện xử lý thông tin và thông tin của tổ chức.		
A.11.1.1	Vành đai an toàn vật lý	Biện pháp kiểm soát Vành đai an toàn phải được xác định và sử dụng để bảo vệ khu vực chứa các phương tiện xử lý thông tin và thông tin quan trọng hoặc nhạy cảm.
A.11.1.2	Kiểm soát lối vào vật lý	Biện pháp kiểm soát Các khu vực cần được bảo vệ bằng các biện pháp kiểm soát lối vào thích hợp nhằm đảm bảo chỉ những người có quyền mới được phép truy cập.
A.11.1.3	An toàn văn phòng, phòng làm việc và các thiết bị	Biện pháp kiểm soát 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.11.1.4	Bảo vệ chống lại các mối đe dọa từ môi trường và bên ngoài	Biện pháp kiểm soát Bảo vệ vật lý chống lại các thảm họa thiên nhiên, các tai nạn hoặc tấn công độc hại phải được thiết kế và áp dụng.

A.11.1.5	Làm việc trong các khu vực an toàn	Biện pháp kiểm soát Cần thiết kế và áp dụng các thủ tục để làm việc trong các khu vực an toàn.
A.11.1.6	Các khu vực phân phối và tập kết hàng	Biện pháp kiểm soát Các điểm truy cập mà người truy cập không cần cấp phép như khu vực phân phối và tập kết 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 cập trái phép.
A.11.2 Thiết bị		
Mục tiêu: Nhằm ngăn ngừa sự mất mát, hư hại, đánh cắp hoặc lợi dụng tài sản và làm gián đoạn hoạt động của tổ chức.		
A.11.2.1	Bố trí và bảo vệ thiết bị	Biện pháp kiểm soát Thiết bị phải được bố trí và được bảo vệ nhằm giảm thiểu các rủi ro từ các mối đe dọa, các hiểm họa từ môi trường hay các truy cập trái phép.
A.11.2.2	Các tiện ích hỗ trợ	Biện pháp kiểm soát Thiết bị phải được bảo vệ khỏi sự cố về nguồn điện cũng như các sự gián đoạn khác có nguyên nhân từ các tiện ích hỗ trợ.
A.11.2.3	An toàn cho dây cáp	Biện pháp kiểm soát Dây cáp điện và cáp truyền thông mang dữ liệu hoặc các dịch vụ thông tin hỗ trợ phải được bảo vệ khỏi việc bị chặn, bị xâm phạm hoặc làm hư hại.
A.11.2.4	Bảo dưỡng thiết bị	Biện pháp kiểm soát Thiết bị cần được bảo dưỡng đúng quy cách nhằm đảm bảo luôn sẵn sàng và toàn vẹn.
A.11.2.5	Di dời tài sản	Biện pháp kiểm soát Không được mang thiết bị, thông tin hoặc phần mềm ra khỏi trụ sở nếu chưa được phép.

A.11.2.6	An toàn cho thiết bị và tài sản hoạt động bên ngoài trụ sở của tổ chức	Biện pháp kiểm soát Phải đảm bảo an toàn cho các tài sản sử dụng bên ngoài, chú ý đến các rủi ro khác nhau khi làm việc bên ngoài phạm vi của tổ chức.
A.11.2.7	An toàn khi loại bỏ và tái sử dụng thiết bị	Biện pháp kiểm soát 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.11.2.8	Thiết bị người dùng khi không sử dụng	Biện pháp kiểm soát Người dùng cần đảm bảo rằng thiết bị phải được bảo vệ thích hợp khi không sử dụng.
A.11.2.9	Chính sách bàn sạch và màn hình sạch	Biện pháp kiểm soát Một chính sách bàn sạch cho các loại giấy tờ và phương tiện truyền thông lưu trữ di động và một chính sách màn hình sạch cho các phương tiện xử lý thông tin phải được thông qua.
A.12 An toàn vận hành		
A.12.1 Các thủ tục và trách nhiệm vận hành		
Mục tiêu: Nhằm đảm bảo vận hành các phương tiện xử lý thông tin được an toàn và chính xác.		
A.12.1.1	Các thủ tục vận hành được lập thành văn bản	Biện pháp kiểm soát Các thủ tục vận hành cần được lập thành văn bản và luôn sẵn sàng đối với mọi người dùng cần dùng đến.
A.12.1.2	Quản lý thay đổi	Biện pháp kiểm soát Cần phải kiểm soát các thay đổi trong tổ chức, các quy trình nghiệp vụ, các phương tiện xử lý thông tin và hệ thống xử lý thông tin có ảnh hưởng tới an toàn thông tin.
A.12.1.3	Quản lý năng lực	Biện pháp kiểm soát

	hệ thống	Việc sử dụng tài nguyên phải được theo dõi, điều chỉnh và dự báo các yêu cầu năng lực hệ thống trong tương lai để đảm bảo yêu cầu hiệu năng.
A.12.1.4	Phân tách các chức năng phát triển, kiểm thử và vận hành	Biện pháp kiểm soát Các chức năng phát triển, kiểm thử và môi trường hoạt động cần được phân tách nhằm giảm thiểu các rủi ro của việc truy cập hoặc thay đổi môi trường vận hành trái phép.
A.12.2 Bảo vệ chống lại phần mềm độc hại		
Mục tiêu: Nhằm đảm bảo rằng các phương tiện xử lý thông tin và thông tin được bảo vệ chống lại phần mềm độc hại.		
A.12.2.1	Quản lý chống lại phần mềm độc hại	Biện pháp kiểm soát Các biện pháp kiểm soát trong việc phát hiện, ngăn chặn và phục hồi nhằm bảo vệ chống lại các phần mềm độc hại phải được thực hiện, kết hợp với nâng cao nhận thức của người sử dụng.
A.12.3 Sao lưu		
Mục tiêu: Nhằm bảo vệ chống lại việc mất mát dữ liệu.		
A.12.3.1	Sao lưu thông tin	Biện pháp kiểm soát Bản sao lưu các thông tin, phần mềm và các hình ảnh hệ thống phải được thực hiện và kiểm tra thường xuyên theo một chính sách sao lưu đã được thông qua.
A.12.4 Ghi nhật ký và giám sát		
Mục tiêu: Nhằm ghi lại các sự kiện và tạo chứng cứ.		
A.12.4.1	Ghi nhật ký sự kiện	Biện pháp kiểm soát Việc ghi nhật ký tất cả các hoạt động của người dùng, các ngoại lệ, các lỗi và các sự kiện an toàn thông tin cần phải được thực hiện và duy trì và soát xét thường xuyên.
A.12.4.2	Bảo vệ thông tin nhật ký.	Biện pháp kiểm soát 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.12.4.3	Nhật ký điều hành và quản trị	Biện pháp kiểm soát Tất cả hoạt động của người quản trị cũng như người điều hành hệ thống cần phải được ghi nhật ký và các bản ghi đó cần được bảo vệ và soát xét thường xuyên.
A.12.4.4	Đồng bộ thời gian	Biện pháp kiểm soát Đồng hồ của các hệ thống xử lý thông tin có liên quan trong phạm vi tổ chức hoặc trong một phạm vi an toàn cần được đồng bộ với một nguồn thời gian tham chiếu duy nhất.
A.12.5 Quản lý các phần mềm vận hành		
Mục tiêu: Nhằm đảm bảo tính toàn vẹn của các hệ thống vận hành.		
A.12.5.1	Cài đặt phần mềm trên các hệ thống vận hành	Biện pháp kiểm soát Cần triển khai các thủ tục để kiểm soát quá trình cài đặt các phần mềm trên hệ thống vận hành.
A.12.6 Quản lý lỗ hổng kỹ thuật		
Mục tiêu: Nhằm ngăn chặn việc khai thác các lỗ hổng kỹ thuật.		
A.12.6.1	Quản lý các lỗ hổng kỹ thuật	Biện pháp kiểm soát Thông tin về các lỗ hổng kỹ thuật của các hệ thống thông tin đang được sử dụng cần phải được thu thập kịp thời. Tổ chức cần công bố đánh giá về các lỗ hổng này và thực hiện các biện pháp thích hợp để giải quyết các rủi ro liên quan.
A.12.6.2	Hạn chế việc cài đặt phần mềm	Biện pháp kiểm soát Cần thiết lập và triển khai các quy tắc cài đặt phần mềm đối với người dùng.
A.12.7 Soát xét việc đánh giá các hệ thống thông tin		
Mục tiêu: Nhằm giảm thiểu tác động của các hoạt động đánh giá đến các hệ thống vận hành.		

A.12.7.1	Các biện pháp kiểm soát đánh giá hệ thống thông tin	Biện pháp kiểm soát Các yêu cầu và hoạt động đánh giá các hệ thống vận hành cần được hoạch định kỹ lưỡng và thống nhất để giảm thiểu sự gián đoạn của các quy trình nghiệp vụ.
A.13 An toàn truyền thông		
A.13.1 Quản lý an toàn mạng		
Mục tiêu: Đảm bảo an toàn thông tin trong các mạng và hỗ trợ các phương tiện xử lý thông tin.		
A.13.1.1	Các biện pháp kiểm soát mạng	Biện pháp kiểm soát Các mạng phải được kiểm soát và quản lý nhằm bảo vệ thông tin trong các hệ thống và các ứng dụng.
A.13.1.2	An toàn các dịch vụ mạng	Biện pháp kiểm soát Các cơ chế bảo mật, các mức dịch vụ và các yêu cầu quản lý của tất cả dịch vụ mạng phải được xác định và bao gồm trong thỏa thuận dịch vụ mạng, bất kể dịch vụ là do nội bộ cung cấp hay thuê khoán bên ngoài.
A.13.1.3	Sự phân tách trên mạng	Biện pháp kiểm soát Các nhóm dịch vụ thông tin, người dùng và hệ thống thông tin cần được phân tách trên các mạng.
A.13.2 Truyền thông tin		
Mục tiêu: Nhằm duy trì an toàn cho các thông tin truyền trong nội bộ tổ chức hoặc với các thực thể bên ngoài.		
A.13.2.1	Các thủ tục và chính sách truyền thông tin	Biện pháp kiểm soát Các chính sách, thủ tục và biện pháp kiểm soát chính thức phải được thực hiện nhằm bảo vệ việc truyền thông tin thông qua việc sử dụng tất cả các loại phương tiện truyền thông.
A.13.2.2	Các thỏa thuận truyền thông tin	Biện pháp kiểm soát Các thỏa thuận phải đặt ra việc truyền thông an toàn các thông tin nghiệp vụ giữa tổ chức và các đối tác bên ngoài.

A.13.2.3	Thông điệp điện tử	Biện pháp kiểm soát Thông tin bao hàm trong các thông điệp điện tử cần được bảo vệ một cách thích hợp.
A.13.2.4	Thỏa thuận bảo mật hoặc không tiết lộ	Biện pháp kiểm soát Các yêu cầu cho thỏa thuận bảo mật hoặc không tiết lộ phản ánh nhu cầu của tổ chức đối với việc bảo vệ thông tin phải được xác định rõ, thường xuyên được soát xét và được ghi thành văn bản.
A.14 Tiếp nhận, phát triển và duy trì các hệ thống thông tin		
A.14.1 Các yêu cầu an toàn của hệ thống thông tin		
Mục tiêu: Nhằm đảm bảo rằng an toàn thông tin là một phần không thể tách rời của các hệ thống thông tin trong toàn bộ vòng đời. Điều này cũng bao gồm các yêu cầu đối với hệ thống thông tin cung cấp các dịch vụ trên mạng công cộng.		
A.14.1.1	14.1.1 Phân tích và đặc tả các yêu cầu an toàn thông tin	Biện pháp kiểm soát Các yêu cầu liên quan tới an toàn thông tin phải được bao gồm trong các yêu cầu đối với các hệ thống thông tin mới hoặc các cải tiến từ các hệ thống thông tin hiện có.
A.14.1.2	An toàn các dịch vụ ứng dụng trên mạng công cộng	Biện pháp kiểm soát Thông tin liên quan trong các dịch vụ ứng dụng đi qua mạng công cộng phải được bảo vệ khỏi các hành vi gian lận, tranh chấp kết nối, tiết lộ và sửa đổi trái phép.
A.14.1.3	Bảo vệ các giao dịch dịch vụ ứng dụng	Biện pháp kiểm soát Thông tin liên quan đến các giao dịch dịch vụ ứng dụng phải được bảo vệ để ngăn ngừa sự truyền dẫn không đầy đủ, lỗi định tuyến, thay đổi thông điệp trái phép, tiết lộ trái phép, sao chép hoặc chuyển tiếp thông tin trái phép.
A.14.2 An toàn trong quá trình phát triển và hỗ trợ		
Mục tiêu: Nhằm đảm bảo rằng an toàn thông tin được thiết kế và triển khai trong vòng đời phát triển của các hệ thống thông tin.		

A.14.2.1	Chính sách phát triển an toàn	Biện pháp kiểm soát Quy tắc cho phát triển phần mềm và hệ thống cần được thiết lập và áp dụng để phát triển trong tổ chức.
A.14.2.2	Các thủ tục kiểm soát thay đổi hệ thống	Biện pháp kiểm soát Các thay đổi hệ thống trong vòng đời phát triển phải được kiểm soát bằng cách sử dụng các thủ tục kiểm soát thay đổi chính thức.
A.14.2.3	Soát xét kỹ thuật của các ứng dụng sau khi thay đổi nền tảng hệ điều hành	Biện pháp kiểm soát Khi nền tảng hệ điều hành thay đổi, các ứng dụng nghiệp vụ quan trọng phải được soát xét và kiểm tra nhằm đảm bảo không có tác động xấu đến hoạt động hoặc sự an toàn của tổ chức.
A.14.2.4	Hạn chế thay đổi các gói phần mềm	Biện pháp kiểm soát Việc sửa đổi các gói phần mềm không được khuyến khích, chỉ giới hạn trong những thay đổi cần thiết và tất cả những thay đổi phải được kiểm soát chặt chẽ.
A.14.2.5	Các nguyên tắc kỹ thuật an toàn hệ thống	Biện pháp kiểm soát Các nguyên tắc kỹ thuật an toàn hệ thống phải được thiết lập, ghi thành văn bản, duy trì và áp dụng cho bất kỳ hệ thống thông tin nào được triển khai.
A.14.2.6	An toàn môi trường phát triển	Biện pháp kiểm soát Các tổ chức cần thiết lập và bảo vệ thích hợp môi trường phát triển an toàn cho hệ thống và các nỗ lực tích hợp bao gồm toàn bộ vòng đời phát triển hệ thống.
A.14.2.7	Phát triển phần mềm thuê ngoài	Biện pháp kiểm soát Tổ chức phải thực hiện giám sát và theo dõi các hoạt động phát triển hệ thống phần mềm thuê ngoài.
A.14.2.8	Kiểm thử an toàn hệ thống	Biện pháp kiểm soát Kiểm thử các chức năng an toàn phải được thực hiện trong quá trình phát triển.

A.14.2.9	Kiểm thử chấp nhận hệ thống	Biện pháp kiểm soát Các chương trình kiểm thử chấp nhận và các tiêu chí liên quan phải được thiết lập cho các hệ thống thông tin mới, các nâng cấp và phiên bản mới.
A.14.3 Dữ liệu kiểm thử		
Mục tiêu: Nhằm đảm bảo bảo vệ dữ liệu được sử dụng cho việc kiểm thử.		
A.14.3.1	Bảo vệ dữ liệu kiểm thử	Biện pháp kiểm soát Dữ liệu kiểm thử cần được lựa chọn, kiểm soát và bảo vệ một cách thận trọng.
A.15 Quan hệ với nhà cung cấp		
A.15.1 An toàn thông tin trong các mối quan hệ với nhà cung cấp		
Mục tiêu: Nhằm đảm bảo bảo vệ các tài sản có thể truy cập bởi các nhà cung cấp của tổ chức.		
A.15.1.1	Chính sách an toàn thông tin trong mối quan hệ với nhà cung cấp	Biện pháp kiểm soát Các yêu cầu an toàn thông tin nhằm giảm thiểu rủi ro liên quan đến việc truy cập của các nhà cung cấp tới hệ thống thông tin hoặc các phương tiện xử lý thông tin của tổ chức phải lập thành văn bản.
A.15.1.2	Đảm bảo an toàn trong các thỏa thuận với nhà cung cấp	Biện pháp kiểm soát Tất cả các yêu cầu an toàn thông tin liên quan phải được thiết lập và thống nhất với từng nhà cung cấp để có thể truy cập, xử lý, lưu trữ, truyền thông hoặc cung cấp các thành phần cơ sở hạ tầng công nghệ thông tin cho tổ chức.
A.15.1.3	Chuỗi cung ứng công nghệ thông tin và truyền thông	Biện pháp kiểm soát Các thỏa thuận với các nhà cung cấp phải bao gồm các yêu cầu để giải quyết các rủi ro an toàn thông tin liên quan đến chuỗi cung cấp sản phẩm và các dịch vụ truyền thông và công nghệ thông tin.
A.15.2 Quản lý chuyển giao dịch vụ cho nhà cung cấp		
Mục tiêu: Để duy trì một mức độ thống nhất về an toàn thông tin và chuyển giao dịch vụ phù hợp		

trong các thỏa thuận với nhà cung cấp.		
A.15.2.1	Giám sát và soát xét các dịch vụ của nhà cung cấp	Biện pháp kiểm soát Các tổ chức phải thường xuyên giám sát, soát xét và đánh giá dịch vụ cung cấp.
A.15.2.2	Quản lý các thay đổi của các dịch vụ cung cấp	Biện pháp kiểm soát Các thay đổi về cung cấp các dịch vụ của các nhà cung cấp, bao gồm việc duy trì và cải tiến các chính sách, thủ tục và biện pháp kiểm soát an toàn thông tin hiện hành, cần được quản lý, chú ý đến mức độ rủi ro của thông tin, hệ thống và quy trình nghiệp vụ cũng như việc đánh giá lại các rủi ro.
A.16 Quản lý các sự cố an toàn thông tin		
A.16.1 Quản lý sự cố an toàn thông tin và các cải tiến		
Mục tiêu: Nhằm đảm bảo một cách tiếp cận nhất quán và hiệu quả được áp dụng trong việc quản lý các sự cố an toàn thông tin, bao gồm cả truyền thông về các điểm yếu và các sự kiện an toàn thông tin.		
A.16.1.1	Các trách nhiệm và thủ tục	Biện pháp kiểm soát 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.16.1.2	Báo cáo các sự kiện an toàn thông tin	Biện pháp kiểm soát 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.16.1.3	Báo cáo các điểm yếu về an toàn thông tin	Biện pháp kiểm soát Mọi nhân viên, người kí kết hợp đồng sử dụng dịch vụ và hệ thống thông tin của tổ chức cần được yêu cầu ghi chú và báo cáo lại bất kỳ điểm yếu nào về an toàn thông tin thấy được hoặc cảm thấy nghi ngờ trong các hoạt động hoặc dịch vụ của hệ thống.
A.16.1.4	Đánh giá và quyết	Biện pháp kiểm soát

	định về các sự kiện an toàn thông tin	Các sự kiện an toàn thông tin phải được đánh giá và quyết định liệu chúng có được phân loại là các sự cố an toàn thông tin.
A.16.1.5	Ứng phó với các sự cố an toàn thông tin	Biện pháp kiểm soát Các sự cố an toàn thông tin phải được ứng phó phù hợp với các thủ tục đã được lập thành văn bản.
A.16.1.6	Rút bài học kinh nghiệm từ các sự cố an toàn thông tin	Biện pháp kiểm soát Kiến thức thu được từ việc phân tích và giải quyết các sự cố an toàn thông tin phải được sử dụng để giảm thiểu khả năng hoặc tác động của các sự cố trong tương lai.
A.16.1.7	Tập hợp bằng chứng	Biện pháp kiểm soát Các tổ chức phải xác định và áp dụng các quy trình xác định, tập hợp, thu nhận và bảo quản thông tin có thể được dùng làm bằng chứng.
A.17 Các khía cạnh an toàn thông tin trong quản lý hoạt động nghiệp vụ liên tục		
A.17.1 Đảm bảo an toàn thông tin liên tục		
Mục tiêu: Tính liên tục của an toàn thông tin cần phải nằm trong các hệ thống quản lý tính liên tục nghiệp vụ của tổ chức.		
A.17.1.1	Kế hoạch đảm bảo an toàn thông tin liên tục	Biện pháp kiểm soát Tổ chức phải xác định các yêu cầu của mình cho an toàn thông tin và tính liên tục của việc quản lý an toàn thông tin trong các tình huống bất lợi, ví dụ: trong một cuộc khủng hoảng hay thiên tai.
A.17.1.2	Triển khai đảm bảo an toàn thông tin liên tục	Biện pháp kiểm soát Tổ chức phải thiết lập, lập văn bản, triển khai và duy trì các quy trình, thủ tục và các biện pháp kiểm soát nhằm đảm bảo mức độ liên tục cho an toàn thông tin được yêu cầu trong các tình huống bất lợi.
A.17.1.3	Xác minh, soát xét và đánh giá đảm	Biện pháp kiểm soát Tổ chức cần xác minh việc thiết lập và triển khai các biện

	bảo an toàn thông tin liên tục	pháp kiểm soát an toàn thông tin liên tục thường xuyên trong nội bộ để đảm bảo rằng chúng có hiệu lực cũng như hiệu quả trong các tình huống bất lợi.
A.17.2 Dự phòng		
Mục tiêu: Nhằm đảm bảo tính sẵn sàng của các phương tiện xử lý thông tin.		
A.17.2.1	Tính sẵn sàng của các phương tiện xử lý thông tin	Biện pháp kiểm soát Các phương tiện xử lý thông tin phải được triển khai với dự phòng đủ để đáp ứng các yêu cầu về tính sẵn sàng.
A.18 Sự tuân thủ		
A.18.1 Sự tuân thủ với các yêu cầu pháp lý và hợp đồng		
Mục tiêu: Nhằm tránh sự vi phạm pháp luật, quy định, nghĩa vụ theo các hợp đồng đã ký kết có liên quan đến an toàn thông tin và tránh vi phạm các yêu cầu về đảm bảo an toàn thông tin.		
A.18.1.1	Xác định các yêu cầu của hợp đồng và điều luật được áp dụng	Biện pháp kiểm soát Tất cả các yêu cầu về luật pháp, quy định, hợp đồng đã ký có liên quan và phương pháp tiếp cận của tổ chức để đáp ứng các yêu cầu này phải được xác định một cách rõ ràng, lập thành văn bản và cập nhật thường xuyên cho mỗi hệ thống và tổ chức.
A.18.1.2	Quyền sở hữu trí tuệ (IPR)	Biện pháp kiểm soát Các thủ tục phù hợp cần được triển khai nhằm đảm bảo sự tuân thủ với các yêu cầu pháp lý, các quy định và cam kết theo hợp đồng liên quan đến quyền sở hữu trí tuệ và sử dụng các sản phẩm phần mềm bản quyền.
A.18.1.3	Bảo vệ các hồ sơ	Biện pháp kiểm soát Các hồ sơ cần được bảo vệ khỏi sự mất mát, phá hủy, giả mạo, truy cập trái phép và phát hành trái phép, phù hợp với pháp luật, quy định, các nghĩa vụ trong hợp đồng đã ký và các yêu cầu nghiệp vụ.
A.18.1.4	Sự riêng tư và bảo vệ thông tin có thể	Biện pháp kiểm soát Sự riêng tư và thông tin có thể định danh cá nhân phải

	định danh cá nhân	được đảm bảo theo yêu cầu của pháp luật và các quy định liên quan nếu có.
A.18.1.5	Quy định về quản lý mật mã	Biện pháp kiểm soát Các kiểm soát mật mã phải được áp dụng phù hợp với tất cả các thỏa thuận, luật pháp và các quy định liên quan.
A.18.2 Soát xét an toàn thông tin		
Mục tiêu: Nhằm đảm bảo rằng an toàn thông tin được triển khai và vận hành phù hợp với các chính sách và thủ tục của tổ chức.		
A.18.2.1	Soát xét một cách độc lập về an toàn thông tin	Biện pháp kiểm soát Cách tiếp cận của tổ chức để quản lý an toàn thông tin và việc triển khai (tức là các mục tiêu, biện pháp kiểm soát, các chính sách, các quá trình và thủ tục đảm bảo an toàn thông tin) phải được soát xét độc lập theo định kỳ hoặc khi xuất hiện những thay đổi đáng kể về triển khai an toàn xảy ra.
A.18.2.2	Sự tuân thủ các chính sách và tiêu chuẩn an toàn	Biện pháp kiểm soát Người quản lý phải thường xuyên soát xét sự tuân thủ của việc xử lý thông tin và quy trình trong phạm vi trách nhiệm của mình với các chính sách, các tiêu chuẩn an toàn và các yêu cầu an toàn khác.
A.18.2.3	Soát xét tuân thủ kỹ thuật	Biện pháp kiểm soát Các hệ thống thông tin phải được soát xét thường xuyên sự tuân thủ các chính sách và các tiêu chuẩn an toàn thông tin của tổ chức.

Thư mục tài liệu tham khảo

[1] ISO/IEC 27002:2013, *Information technology - Security techniques - Code of practice for information security controls.*

[2] TCVN 10541 (ISO/IEC 27003), *Công nghệ thông tin - Các kỹ thuật an toàn - Hướng dẫn triển khai hệ thống quản lý an toàn thông tin.*

[3] TCVN 10542 (ISO/IEC 27004), *Công nghệ thông tin - Các kỹ thuật an toàn - Quản lý an toàn thông tin - Đo lường.*

[4] TCVN 10295 (ISO/IEC 27005), *Công nghệ thông tin - Các kỹ thuật an toàn - Quản lý rủi ro an toàn thông tin.*

[5] TCVN ISO 31000:2011 (ISO 31000:2009), *Quản lý rủi ro - Nguyên tắc và hướng dẫn.*

[6] ISO/IEC Directives, Part 1, *Consolidated ISO Supplement - Procedures specific to ISO, 2012.*