ISO/IEC 27001:2013

Công nghệ thông tin – các kỹ thuật an ninh – Các yêu cầu Hệ thống quản lý an ninh thông tin

Công ty TNHH Chứng nhận DAS Việt Nam

Tiêu chuẩn ISO27001

Lời nói đầu ……..02

0. Giới thiệu…….....03
1. Khái quát……...03
2. Tương thích với các tiêu chuẩn quản lý khác……03

CÔNG NGHỆ THÔNG TIN – CÁC KỸ THUẬT AN NINH
HỆ THỐNG QUẢN LÝ AN NINH THÔNG TIN – CÁC YÊU CẦU

1. Phạm vi……...04
2. Tài liệu viện dẫn…….04
3. Thuật ngữ và định nghĩa……...04
4. Bối cảnh của Tổ chức……04
4.1 Hiểu về tổ chức và bối cảnh……04
4.2 Hiểu về yêu cầu và kỳ vọng của các bên quan tâm……04
4.3 Xác định phạm vi của hệ thống quản lý an toàn thông tin…….04
4.4 Hệ thống quản lý an ninh thông tin…….05
5. Sự Lãnh đạo ……..05
5.1 Lãnh đạo và sự cam kết……05
5.2 Chính sách……..05
5.3 Vai trò của tổ chức, trách nhiệm và quyền hạn……05
6. Hoạch định……..05
6.1 Các hành động để nhận biết rủi ro và các cơ hội…….05
6.2 Mục tiêu an ninh thông tin và hoạch định để đạt kết quả……..07
7. Hỗ trợ……..07
7.1 Nguồn lực……07
7.2 Năng lực……07
7.3 Nhận thức……07
7.4 Truyền thông……..08
7.5 Thông tin được văn bản hóa……..08
8. Hoạt động điều hành……..08
8.1 Lập kế hoạch điều hành và kiểm soát……08
8.2 Đánh giá rủi ro thông tin……09
8.3 Xử lý rủi ro thông tin…….09
9. Đánh giá việc thực hiện…….09
9.1 Giám sát, đo lường, phân tích và định lượng ……..09
9.2 Đánh giá nội bộ……..09
9.3 Xem xét lãnh đạo…….10
10. Cải tiến…….10
10.1 Hành động không phù hợp và khắc phục…….10
10.2 Hành động cải tiến……..11

Phụ lục A. Tham chiếu các mục tiêu kiểm soát và kiểm soát……12

Tham khảo………..27

Lời nói đầu

Tổ chức tiêu chuẩn hóa quốc tế ISO (viết tắt bởi the International Organization for Standarization) và Ủy ban điện kỹ thuật quốc tế IEC (được viết tắt bởi the International Electrotechnical Commission) đã xây dựng hệ thống đặc biệt này trở thành một tiêu chuẩn toàn cầu. Tổ chức của các quốc gia là thành viên của ISO hoặc IEC tham gia vào việc phát triển các tiêu chuẩn quốc tế thông qua ủy ban kỹ thuật được thiết lập bởi các tổ chức uy tín nhằm giải quyết các vấn đề kỹ thuật của lĩnh vực đặc biệt này. Ủy ban kỹ thuật của ISO và IEC hợp tác qua lại trong tất cả các mối quan tâm. Các tổ chức quốc tế khác, các chính phủ và phi chính phủ có mối liên kết với ISO và IEC cũng tham gia vào công việc này. Trong lĩnh vực công nghệ thông tin, Tổ chức ISO và IEC đã thành lập ủy ban hợp tác kỹ thuật, ISO/IEC JTC 1.

Các tiêu chuẩn được dự thảo phù hợp với các quy định ISO/IEC phần 2.

Nhiệm vụ chính của Ủy ban hợp tác kỹ thuật là chuẩn bị các tiêu chuẩn quốc tế. Các bản dự thảo tiêu chuẩn được chấp nhận bởi ủy ban hợp tác kỹ thuật được gửi tới Tổ chức tiêu chuẩn của các quốc gia cho ý kiến. Tiêu chuẩn được xuất bản khi đáp ứng ít nhất 75% ý kiến đồng thuận.

Lưu ý rằng, có khả năng các tài liệu đóng góp xây dựng tiêu chuẩn có thể là vấn đề bản quyền. Tổ chức ISO và IEC không có trách nhiệm xác định vấn đề nào là bản quyền.

Tiêu chuẩn ISO/IEC 27001 được soạn thảo bởi Ủy ban hợp tác kỹ thuật ISO/IEC JTC 1, công nghệ thông tin, Tiểu ủy ban SC27, Kỹ thuận an ninh công nghệ thông tin.

Việc tái bản lần 2 bộ tiêu chuẩn thay thế toàn bộ tiêu chuẩn xuất bản lần 1 (ISO/IEC 27001:2005), đã được xem xét cẩn thận.

0. Giới thiệu

0.1 Khái quát

Tiêu chuẩn quốc tế này được xây dựng nhằm cung cấp các yêu cầu cho việc thiết lập, thực hiện, duy trì và liên tục cải tiến hệ thống quản lý an ninh thông tin. Chấp nhận hệ thống quản lý an ninh thông tin (ISMS) là một quyết định chiến lược của tổ chức. Việc thiết lập và thực hiện hệ thống quản lý an ninh thông tin sẽ chịu sự chi phối bởi nhu cầu, mục tiêu, các yêu cầu an ninh, các quy trình công việc, quy mô và cơ cấu của tổ chức. Tất các các tác động này sẽ thay đổi theo thời gian.

Hệ thống quản lý an ninh thông tin bảo vệ thông tin được bảo mật, toàn vẹn và sẵn sàng được áp dụng bởi quá trình quản lý rủi ro và tạo sự tin cậy đối với các bên quan tâm rằng các rủi ro được quản lý thỏa đáng.

Một yêu cầu quan trọng rằng Hệ thống quản lý an ninh thông tin là một phần và được tích hợp với các quá trình của tổ chức, bao trùm lên toàn bộ cơ cấu quản lý và rằng an ninh thông tin phải được xem xét từ khi thiết kế quy trình. Áp dụng các kiểm soát hệ thống quản lý an ninh thông tin được kỳ vọng phù hợp với nhu cầu của tổ chức.

Tiêu chuẩn này được sử dụng nội bộ và cho các tổ chức bên ngoài đánh giá mức độ đáp ứng các yêu cầu an ninh thông tin của tổ chức.

Trật tự các yêu cầu trong bản tiêu chuẩn quốc tế này không phản ánh mức độ quan trọng hoặc ngụ ý về trật tự mà tổ chức phải áp dụng. Các hạng mục được liệt kê chỉ dành cho các mục yêu cầu được tham chiếu.

Tiêu chuẩn ISO/IEC 27000 miêu tả tổng quan và thuật ngữ - định nghĩa quản lý an ninh thông tin được tham chiếu trong bộ tiêu chuẩn quản lý an ninh thông tin (bao gồm ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005.

02. Tương thích với các tiêu chuẩn quản lý khác.

Tiêu chuẩn này áp dụng cho cấu trúc thượng tầng, tiểu tiêu đề đồng nhất, văn bản đồng nhất, điều khoản chung, định nghĩa lõi được xác định trong phụ lục SL của Hướng dẫn ISO/IEC, phần 1, Phần bổ trợ ISO, do vậy phải tương thích với các hệ thống quản lý khác được quy định tại phụ lục SL.

Cách tiếp cận chung này được xác định rõ trong Phụ lục SL giúp tổ chức lựa chọn áp dụng một hay nhiều hệ thống quản lý.

CÔNG NGHỆ THÔNG TIN – CÁC KỸ THUẬT AN NINH

HỆ THỐNG QUẢN LÝ AN NINH THÔNG TIN – CÁC YÊU CẦU.

1. Phạm vi

Tiêu chuẩn này chỉ rõ các yêu cầu cho việc thiết lập, thực hiện, duy trì và liên tục cải tiến hệ thống quản lý an ninh thông tin phù hợp bối cảnh của Tổ chức. Tiêu chuẩn này cũng bao gồm các yêu cầu cho đánh giá, xử lý các rủi ro an ninh thông tin được xây dựng đáp ứng yêu cầu của tổ chức. Các yêu cầu được thiết lập trong tiêu chuẩn này mang tính tổng quát và chủ đích để áp dụng cho tất cả các tổ chức, bất kỳ loại hình, quy mô nào .Việc loại trừ bất kỳ điều khoản riêng biệt nào trong Điều 4 đến 10 không được chấp nhận khi tổ chức công bố áp dụng tiêu chuẩn quốc tế này.

2. Tài liệu viện dẫn

Các tài liệu dưới đây, tất cả hoặc một phần, được quy chiếu trong tài liệu này là yêu cầu áp dụng. Ngày tháng chỉ có tính chất tham khảo, lần tái bản là trích dẫn áp dụng. Yêu cầu cập nhật các phiên bản mới nhất các tài liệu viện dẫn (bao gồm bất kỳ sự sửa đổi nào)

ISO/IEC 27000, *công nghệ thông tin – kỹ thuật an ninh – Hệ thống quản lý an ninh thông tin – Khái quát và từ vựng*.

3. Thuật ngữ và định nghĩa

Đối với các thuật ngữ và định nghĩa trong tiêu chuẩn này được xác định trong ISO/EC27000

4. Bối cảnh của Tổ chức

4.1. Hiểu tổ chức và bối cảnh tổ chức

Tổ chức phải xác định rõ các vấn đề nội bộ và bên ngoài liên quan đến mục đích và tác động của nó ảnh hưởng đến khả năng đạt được các kết quả mong đợi từ hệ thống quản lý an ninh thông tin

Ghi chú: Xác định các vấn đề trên tham chiếu đến điều khoản 5.3 tiêu chuẩn ISO31000:2009 – thiết lập bối cảnh nội bộ và bên ngoài của tổ chức.

4.2. Hiểu về yêu cầu và kỳ vọng của các bên liên quan.

Tổ chức sẽ phải xác định:

a. Các bên quan tâm đến hệ thống quản lý an ninh thông tin và
b. Các yêu cầu của các bên liên quan về an ninh thông tin.

Ghi chú: Các yêu cầu của các bên quan tâm bao gồm các yêu cầu của pháp luật và các điều khoản trong hợp đồng.

4.3. Xác định phạm vi hệ thống quản lý an ninh thông tin.

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

Khi xác định phạm vi, tổ chức phải xem xét:

a. Các vấn đề nội bộ và bên ngoài quy định tại khoản 4.1.
b. Các yêu cầu quy định tại khoản 4.2; và
c. Sự tương tác và phụ thuộc giữa các hoạt động trong tổ chức và vấn đề này với các tổ chức bên ngoài

Phạm vi áp dụng phải được văn bản hóa.

4.4. Hệ thống quản lý an ninh thông tin

Tổ chức phải thiết lập, thực hiện, duy trì và liên tục cải tiến Hệ thống quản lý an ninh 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 lãnh đạo và cam kết đối với hệ thống quản lý an ninh thông tin bằng cách:

a. Đảm bảo chính sách an ninh thông tin và mục tiêu an ninh thông tin được thiết lập và phù hợp với định hướng chiến lược của tổ chức.
b. Đảm bảo tích hợp các yêu cầu hệ thống quản lý an ninh thông tin các quá trình của tổ chức.
c. Đảm bảo sẵn sàng các nguồn lực cần thiết cho hệ thống quản lý an ninh thông tin.
d. Truyền thông tầm quan trọng về hiệu quả quản lý an ninh thông tin và sự phù hợp với các yêu cầu an ninh thông tin.
e. Đảm bảo rằng hệ thống quản lý an ninh thông tin đạt được các kết quả mong đợi
f. Chỉ đạo và hỗ trợ nhân sự tham gia vào hệ thống quản lý an ninh thông tin có hiệu quả.
g. Thúc đẩy cải tiến liên tục; và
h. Hỗ trợ các quản lý liên quan thể hiện được vai trò lãnh đạo trong vùng trách nhiệm họ được phân công.

5.2. Chính sách

Lãnh đạo cao nhất phải thiết lập chính sách an ninh thông tin đảm bảo:

a. Phù hợp với mục đích của tổ chức
b. Bao gồm các mục tiêu an ninh thông tin (xem 6.2) hoặc cung cấp khuôn khổ cho việc thiết lập các mục tiêu an ninh thông tin.
c. Bao gồm cam kết đáp ứng các yêu cầu áp dụng liên quan đến an ninh thông tin; và
d. Bao gồm cam kết nhằm cải tiến liên tục hệ thống quản lý an ninh thông tin.

Chính sách an ninh thông tin phải:

e. Được văn bản hóa
f. Được truyền thông trong tổ chức; và
g. Sẵn sàng với các bên quan tâm, khi thích hợp

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

Lãnh đạo cao nhất phải đảm bảo các trách nhiệm và phê duyệt quyền hạn liên quan đến an ninh thông tin và truyền thông

Lãnh đạo cao nhất phê duyệt trách nhiệm và quyền hạn nhằm :

a. Đảm bảo rằng hệ thống quản lý an ninh thông tin phù hợp với các yêu cầu của tiêu chuẩn quốc tế này; và
b. Báo cáo về sự thực hiện hệ thống quản lý an ninh thông tin tới lãnh đạo cao nhất.

GHI CHÚ: Lãnh đạo cao nhất có thể ký phê duyệt các trách nhiệm và quyền hạn báo cáo việc thực hiện hệ thống quản lý an ninh thông tin trong nội bộ của tổ chức.

6. Hoạch định

6.1. Các hành động đáp ứng rủi ro và các cơ hội

6.1.1 Tổng quát

Khi hoạch định hệ thống quản lý an ninh thông tin, tổ chức phải xem xét các vấn đề tham chiếu điều khoản 4.1. và các yêu cầu tham chiếu điều khoản 4.2 và xác định rủi ro cũng như các cơ hội đảm bảo các yêu cầu được đáp ứng:

a. Đảm bảo hệ thống an ninh thông tin có thể đạt được các kết quả mong đợi
b. Phòng ngừa hoặc giảm thiểu các tác động không mong muốn; và
c. Đạt được cải tiến liên tục

Tổ chức phải lập kế hoạch:

d. Hành động tập trung vào rủi ro và các cơ hội cải tiến; và
e. Làm thế nào để
    1. Tích hợp và triển khai các hành động trên vào các quá trình hệ thống quản lý an ninh thông tin; và
    2. Đánh giá hiệu quả của các hành động này

6.1.2. Đánh giá rủi ro bảo mật thông tin.

Tổ chức phải thiết lập và áp dụng các quá trình đánh giá rủi ro an ninh thông tin nhằm:

a. Thiết lập và duy trì các tiêu chí rủi ro an ninh thông tin bao gồm:
    1. Các tiêu chí chấp nhận rủi ro; và
    2. Tiêu chí cho việc thực hiện đánh giá rủi ro an ninh thông tin.
b. Đảm bảo rằng quá trình đánh giá rủi ro an ninh thông tin được triển khai liên tục, phù hợp, kết quả đánh giá có giá trị và có thể so sánh được.
c. Xác định các rủi ro an ninh thông tin.
    1. Áp dụng quá trình đánh giá rủi ro an ninh thông tin nhằm xác định các rủi ro liên quan đến việc mất tính bảo mật, tính toàn vẹn và tính sẵn sàng của thông tin trong phạm vi hệ thống quản lý an ninh thông tin; và
    2. Xác định những người nắm giữ rủi ro đó
d. Phân tích rủi ro an ninh thông tin
    1. Đánh giá những hậu quả tiềm ẩn gây ra bởi các rủi ro đã được xác định bằng văn bản trong điều khoản 6.1.2.c)
    2. Đánh giá khả năng trở thành hiện thực của các rủi ro đã được xác định bằng văn bản trong điều khoản 6.1.2.c); và
    3. Xác định các mức độ rủi ro.
e. Định lượng rủi ro an ninh thông tin.
    1. So sánh các kết quả phân tích rủi ro với các tiêu chí rủi ro đã được thiết lập trong điều khoản 6.1.2.a); và
    2. Đưa ra trật tự ưu tiên đối với các rủi ro đã được phân tích cho hoạt động xử lý rủi ro.

Tổ chức phải văn bản hóa quá trình đánh giá rủi ro an ninh thông tin.

6.1.3. Xử lý rủi ro an ninh thông tin

Tổ chức phải xác định và áp dụng quá trình đánh giá rủi ro an ninh thông tin nhằm:

a. Chọn lựa các giải pháp xử lý rủi ro an ninh thông tin phù hợp, dựa trên kết quả đánh giá rủi ro;
b. Xác định tất cả các kiểm soát cần thiết để thực hiện các giải pháp xử lý an ninh thông tin đã lựa chọn.

Ghi chú: Tổ chức có thể thiết kế các kiểm soát theo yêu cầu riêng hoặc xác định xác định chúng từ bất kỳ nguồn nào.

c. So sánh các kiểm soát đã được xác định trong khoản **6.1.3**.b. với Phụ lục A và làm rõ các lựa chọn nào không cần thiết để loại trừ;

Ghi chú 1: Phụ lục A bao gồm tổng thể danh mục các mục tiêu kiểm soát và yêu cầu kiểm soát. Các Tổ chức áp dụng tiêu chuẩn này đều kiểm soát các yêu cầu được quy định trong phụ lục A

Ghi chú 2: Các mục tiêu kiểm soát gồm các kiểm soát được lựa chọn. Các mục tiêu kiểm soát và các kiểm soát trong Phục lục A không phải toàn diện và bổ sung các mục tiêu kiểm soát và các kiểm soát khi cần thiết.

d. Ban hành công bố áp dụng bao gồm các kiểm soát được lựa chọn (xem 6.1.3.b và c) và làm rõ các các biện pháp kiểm soát được áp dụng hay loại trừ trong Phụ lục A.
e. Xây dựng kế hoạch xử lý rủi ro và
f. Phê duyệt người nắm giữ rủi ro trong kế hoạch xử lý rủi ro và chấp nhận những rủi ro còn sót lại.

Tổ chức phải lưu các thông tin được văn bản hóa về quá trình xử lý rủi ro an ninh thông tin.

Ghi chú: Đánh giá rủi ro an ninh thông tin và quá trình xử lý rủi ro trong tiêu chuẩn này phải tuân thủ các nguyên tắc và hướng dẫn chung quy định tại tiêu chuẩn ISO31000

6.2. Mục tiêu an ninh thông tin và lập kế hoạch thực đạt mục tiêu.

Tổ chức phải thiết lập các mục tiêu an ninh thông tin liên quan đến các chức năng nhiệm vụ và mức độ

Các mục tiêu an ninh thông tin phải:

a. Nhất quán với chính sách an ninh thông tin.
b. Đo lường được (một cách thích hợp)
c. Phù hợp với các yêu cầu an ninh thông tin, và kết quả từ việc đánh giá và xử lý rủi ro.
d. Được truyền đạt; và
e. Được cập nhật một cách thích hợp.

Tổ chức phải lưu giữ hồ sơ về các mục tiêu an ninh thông tin.

Khi lập kế hoạch làm thế nào để đạt được các mục tiêu an ninh thông tin, Tổ chức phải xác định:

a. Sẽ làm gì;
b. Nguồn lực yêu cầu là gì;
c. Ai chịu trách nhiệm ;
d. Khi nào thì hoàn thành;
e. Kết quả được đánh giá như thế nào;

7. Hỗ trợ

7.1. Nguồn lực

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

7.2. Năng lực

Tổ chức phải

a. Xác định năng lực cần thiết của nhân sự đang thực hiện các nhiệm vụ mà họ đang kiểm soát có tác động đến việc thực hiện an ninh thông tin.
b. Đảm bảo rằng những con người này có đủ năng lực dựa vào giáo dục, đào tạo hoặc kinh nghiệm thích hợp.

c. Khi thích hợp, tiến hành các hành động để họ đạt được năng lực cần thiết và đánh giá hiệu quả của các hành động đã triển khai.
d. Lưu giữ thông tin được văn bản hóa là bằng chứng chứng minh năng lực.

Ghi chú: Các hành động phù hợp có thể bao gồm, ví dụ: cung cấp đào tạo, tư vấn hoặc bổ nhiệm lại vị trí hiện tại hoặc thuê hoặc ký hợp đồng với những người có đủ năng lực.

7.3. Nhận thức.

Người làm việc cho tổ chức phải nhận thức được:

a. Chính sách an ninh thông tin.
b. Sự đóng góp của họ tới hiệu quả hệ thống quản lý an ninh, bao gồm lợi ích của các cải tiến việc thực hiện an ninh thông tin và
c. Liên can đến sự không phù hợp theo các yêu cầu của hệ thống quản lý an ninh thông tin.

7.4. Trao đổi thông tin.

Tổ chức phải xác định yêu cầu trao đổi thông tin nội bộ và bên ngoài về hệ thống quản lý an ninh thông tin bao gồm:

a. Trao đổi về vấn đề gì?
b. Khi nào trao đổi;
c. Trao đổi với ai;
d. Ai sẽ trao đổi và
e. Các quá trình trao đổi sẽ ảnh hưởng như thế nào

7.5. Thông tin được văn bản hóa

7.5.1. Khái quát

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

a. Các thông tin được văn bản hóa theo yêu cầu của Tiêu chuẩn quốc tế này; và
b. Các thông tin được văn bản hóa mà tổ chức xác định là cần thiết đảm bảo hiệu quả hệ thống quản lý an ninh thông tin.

Ghi chú: Thông tin được văn bản hóa từ bên ngoài đối với hệ thống quản lý an ninh thông tin giữa các tổ chức khác nhau bởi:

1) Quy mô của các tổ chức và loại hình hoạt động, quy trình, sản phẩm, dịch vụ
2) Mức độ phức tạp của các quy trình và tính tương tác; và
3) Năng lực của con người.

7.5.2. Thiết lập và cập nhật tài liệu

Khi thiết lập và cập nhật tài liệu, tổ chức phải đảm bảo sự phù hợp

a. Định nghĩa và diễn giải (ví dụ: tiêu đề, ngày, tác giả, số tham chiếu)
b. Định dạng (ví dụ: ngôn ngữ, phiên bản bản mềm, đồ họa) phương tiện (dạng giấy, điện tử)
c. Được xem xét và phê duyệt phù hợp và thỏa đáng.

7.5.3. Kiểm soát thông tin được văn bản hóa.

Thông tin được văn bản hóa được yêu cầu bởi hệ thống quản lý an ninh thông tin và yêu cầu bởi Tiêu chuẩn quốc tế này phải được kiểm soát đảm bảo:

a. Sẵn sàng và phù hợp cho sử dụng ở nơi và thời điểm khi cần; và

b. Được bảo vệ phù hợp (ví dụ từ việc mất tính bảo mật, sử dụng không được phép hoặc mất tính toàn vẹn)

Yêu cầu kiểm soát thông tin được văn bản hóa, tổ chức phải đáp các hoạt động sau một cách thích hợp:

c. Phân phối, truy cập, thu hồi và sử dụng
d. Lưu giữ và bảo vệ, bao gồm bảo vệ việc đọc được tài liệu;
e. Kiểm soát sự thay đổi (ví dụ: kiểm soát phiên bản) và
f. Sắp xếp và lưu giữ

Thông tin được văn bản hóa có nguồn gốc bên ngoài, được Tổ chức xác định là cần thiết cho việc lập kế hoạch và điều hành hệ thống quản lý an ninh thông tin phải được xác định rõ và được kiểm soát.

Ghi chú: Truy cập ở đây ngụ ý một quyết định cho phép chỉ được quyền xem thông tin được văn bản hóa, hoặc sự cho phép và phê duyệt quyền xem và sửa đổi thông tin được văn bản hóa.v.v.

8. Điều hành.

8.1. Lập kế hoạch và kiểm soát

Tổ chức phải lập kế hoạch, thực hiện và kiểm soát các quá trình cần thiết đáp ứng các yêu cầu an ninh thông tin, và thực hiện các hành động được quy định trong khoản 6.1. Tổ chức cũng phải thực hiện các kế hoạch nhằm đạt được các mục tiêu an ninh thông tin đã được xác định trong 6.2.

Tổ chức phải lưu giữ thông tin được văn bản hóa về mức độ tin cậy mà các quá trình được thực hiện theo kế hoạch đề ra

Tổ chức phải kiểm soát những thay đổi kế hoạch và xem xét hậu quả những thay đổi không có trong dự định, tiến hành những hành động nhằm giảm nhẹ những tác động bất lợi khi cần thiết.

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

8.2. Đánh giá rủi ro an ninh thông tin.

Tổ chức phải thực hiện đánh giá rủi ro an ninh thông tin định kỳ hoặc khi có những thay đổi lớn xuất hiện hoặc theo đề nghị hoặc các tiêu chí được thiết lập trong điều khoản 6.1.2.a.

Tổ chức phải lưu giữ các thông tin được văn bản hóa về kết quả đánh giá rủi ro an ninh thông tin.

8.3. Xử lý rủi ro an ninh thông tin.

Tổ chức phải thực hiện kế hoạch xử lý rủi ro an ninh thông tin.
Tổ chức phải lưu giữ thông tin được văn bản hóa về kết quản xử lý rủi ro an ninh thông tin

9. Đánh giá sự thực hiện .

9.1 . Giám sát, đo lường, phân tích và định lượng

Tổ chức phải đánh giá việc thực hiện an ninh thông tin và hiệu quả của hệ thống quản lý an ninh thông tin.
Tổ chức phải xác định:

a. Cần phải kiểm soát và đo lường cái gì, bao gồm các quá trình an ninh thông tin và các kiểm soát.
b. Phương pháp giám sát, đo lường, phân tích và định lượng, khi thích hợp, để đảm bảo các kết quả có giá trị

Ghi chú: Phương pháp được lựa chọn phải đưa ra các kết quả có thể so sánh được và có giá trị.

c. Khi nào các biện pháp đo lường và giám sát được thực hiện
d. Ai có trách nhiệm giám sát và đo lường
e. Khi nào các kết quả giám sát và đo lường được phân tích và định lượng; và
f. Ai có trách nhiệm phân tích và đánh giá các kết quả trên.

Tổ chức phải lưu trữ thông tin thông tin được văn bản hóa một cách thích hợp như là bằng chứng giám sát và đo lường các kết quả.

9.2. Đánh giá nội bộ

Tổ chức phải tiến hành đánh giá nội bộ định kỳ hteo kế hoạch nhằm nhằm cung cấp thông tin liệu hệ thống quản lý an ninh thông tin:

a. Phù hợp với
    1) Các yêu cầu của tổ chức đối với hệ thống quản lý an ninh thông tin; và
    2) Các yêu cầu của tiêu chuẩn quốc tế này.
b. Được thực hiện và duy trì có hiệu quả

Tổ chức phải

c. Lập kế hoạch, thiết lập, thực hiện và duy trì một (các) chương trình đánh giá, bao gồm tần suất, phương pháp, trách nhiệm, yêu cầu kế hoạch và báo cáo. (Các)chương trình đánh giá phải tập trung xem xét vào các quá trình quan trọng và kết quả của các lần đánh giá trước.
d. Xác định các tiêu chí đánh giá và phạm vi đánh giá cho mỗi cuộc đánh giá.
e. Lựa chọn đánh giá viên và thực hiện cuộc đánh giá đảm bảo các mục tiêu đánh giá và tính công bằng trong toàn bộ quá trình đánh giá.
f. Đảm bảo rằng kết của của các cuộc đánh giá được báo cáo tới các lãnh đạo liên quan; và
g. Lưu giữ thông tin được văn bản hóa như là bằng chứng của các chương trình đánh giá và kết quả cuộc đánh giá.

9.3 Xem xét lãnh đạo

Lãnh đạo cao nhất phải xem xét hệ thống quản lý an ninh thông tin định kỳ theo kế hoạch đảm bảo liên tục ổn định, phù hợp và hiệu quả.

Lãnh đạo phải xem xét

a. Tình trạng các hành động từ lần xem xét trước
b. Những thay đổi trong nội bộ và bên ngoài của hệ thống quản lý an ninh thông tin.

c. Các phản hồi về việc thực hiện an ninh thông tin, tập trung vào:
    1. Sự không phù hợp và các hành động khắc phục
    2. Các kết quả giám sát và đo lường
    3. Các cuộc đánh giá; và
    4. Hoàn thành các mục tiêu an ninh thông tin.
d. Phản hồi của các bên liên quan
e. Kết quả đánh giá rủi ro và thực trạng kế hoạch xử lý rủi ro; và
f. Các cơ hội cải tiến liên tục

Đầu ra của xem xét phải bao gồm các quyết định liên quan đến cơ hội cải tiến liên tục và bất kỳ yêu cầu nào cho những thay đổi hệ thống quản lý an ninh thông tin.

Tổ chức phải lưu trữ thông tin được văn bản hóa như là bằng chứng về các kết quả xem xét lãnh đạo.

10. Cải tiến

10.1. Sự không phù hợp và các hành động khắc phục

Khi xuất hiện một sự không phù hợp, tổ chức phải:
a. Ứng phó sự không phù hợp, và bằng cách:
    1. Tiến hành các hành động kiểm soát và khắc phục; và
    2. Giải quyết các hậu quả
b. Đánh giá các hành động cần thiết để loại trừ nguyên nhân sự không phù hợp, đảm bảo vấn đề này không xuất hiện ở bất kỳ nơi nào nữa: bằng cách:
    1. Xem xét sự không phù hợp
    2. Xác định nguyên nhân của sự không phù hợp và
    3. Xác định các sự không phù hợp tương tự còn tồn tại hoặc tiềm ẩn sẽ xuất hiện
c. Thực hiện bất kỳ các hành động cần thiết nào.
d. Xem xét tính hiệu quả của bất kỳ hành động khắc phục nào được thực hiện; và
e. Thay đổi hệ thống quản lý an ninh thông tin khi thấy cần thiết.

Các hành động khắc phục sẽ phải phù hợp với tác động của sự không phù hợp

Tổ chức phải lưu thông tin văn bản hóa là bằng chứng về
f. Bản chất của sự không phù hợp và bất kỳ hành động nào được thực hiện sau đó và
g. 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 ninh thông tin một cách thích hợp, đầy đủ và hiệu quả

PHỤ LỤC A
THAM CHIẾU CÁC MỤC TIÊU KIỂM SOÁT VÀ KIỂM SOÁT.

Các mục tiêu kiểm soát và các yêu cầu kiểm soát được liệt kê tại bảng A.1 dưới đây được lấy từ trật trự tương ứng tiêu chuẩn ISO/IEC 27002:2013, khoản 5 đến 18 và được sử dụng phù hợp với khoản 6.1.3 của tiêu chuẩn này.

BẢNG A.1 - Các mục tiêu kiểm soát và các kiểm soát.

A.5. Chính sách an ninh thông tin		
A.5.1. Định hướng lãnh đạo đối với an ninh thông tin		
Mục đích: Nhằm cung cấp định hướng lãnh đạo và hỗ trợ đối với an ninh thông tin phù hợp với các yêu cầu kinh doanh và văn bản pháp luật và các quy định liên quan		
A.5.1.1.	Các chính sách an ninh thông tin	*Kiểm soát* Một bộ chính sách an ninh thông tin phải được thiết lập, phê duyệt bởi lãnh đạo, công bố và truyền đạt tới các nhân viên và các bên ngoài liên quan
A.5.1.2.	Xem xét các chính sách an ninh thông tin	*Kiểm soát* Các chính sách an ninh thông tin phải được xem xét định kỳ theo kế hoạch hoặc khi có những thay đổi đáng kể xuất hiện đảm bảo sự phù hợp, đầy đủ và hiệu quả
A.6. Tổ chức an ninh thông tin		
A.6.1 Tổ chức nội bộ		
Mục tiêu: Nhằm thiết lập một khung quản lý khi xây dựng và kiểm soát việc thực hiện, điều hành an ninh thông tin trong tổ chức.		
A.6.1.	Vai trò và trách nhiệm an ninh thông tin	*Kiểm soát* Tất cả trách nhiệm an ninh thông tin phải được xác định và phân định
A.6.1.2.	Biệt lập nhiệm vụ	*Kiểm soát* Những xung đột trong nhiệm vụ và vùng trách nhiệm phải được biệt lập nhằm giảm cơ hội đối với những thay đổi không được phê duyệt hoặc không lường trước được hoặc sử dụng sai các tài sản của tổ chức.
A.6.1.3	Liên lạc với cơ quan/ tổ chức có thẩm quyền	*Kiểm soát* Phải duy trì liên lạc với các cơ quan/ tổ chức có thẩm quyền liên quan một cách phù hợp
A.6.1.4	Liên lạc với các nhóm quan tâm đặc thù	*Kiểm soát* Phải duy trì liên lạc với các nhóm quan tâm đặc biệt hoặc các diễn đàn an ninh đặc thù và các hiệp hội chuyên ngành

		một cách phù hợp.
A.6.1.5	An ninh thông tin trong quản lý dự án	*Kiểm soát* An ninh thông tin phải được giải quyết trong quản lý dự án, bất kể là loại dự án nào.
A.6.2. Các thiết bị di động và làm việc từ xa		
Mục đích :Đảm bảo an ninh trong sử dụng thiết bị di động và làm việc từ xa		
A.6.2.1	Chính sách thiết bị di động	*Kiểm soát* Thiết lập một chính sách và các biện pháp đo lường an ninh hỗ trợ phải được chấp nhận để quản lý rủi ro gây ra bởi việc sử dụng các thiết bị di động.
A.6.2.2.	Làm việc từ xa	*Kiểm soát* Thiết lập một chính sách và các biện pháp an ninh hỗ trợ phải được thực hiện để bảo vệ thông tin bị truy cập, xử lý và lưu trữ tại các địa điểm làm việc từ xa.
A.7. An ninh nguồn nhân lực		
A.7.1. Trước tuyển dụng		
Mục tiêu: Đảm bảo rằng các nhân viên và nhà thầu hiểu trách nhiệm và vai trò của họ phải được xem xét.		
A.7.1.1.	Sàng lọc	*Kiểm soát* Thẩm định gia cảnh của tất cả các ứng viên cho quá trình tuyển dụng được thực hiện phù hợp với yêu cầu của pháp luật, các quy định và đạo đức và phải phù hợp với các yêu cầu kinh doanh, sự phân loại thông tin bị truy cập nhận biết rủi ro
A.7.1.2.	Điều khoản và điều kiện tuyển dụng	*Kiểm soát* Thỏa thuận hợp đồng với người lao động và nhà thầu phải chỉ rõ trách nhiệm của người được tuyển dụng và tổ chức đối với an ninh thông tin
A.7.2. Trong quá trình tuyển dụng		
Mục đích: Nhằm đảm bảo rằng người lao động và nhà thầu nhận thức và thực hiện đầy đủ trách nhiệm bảo mật thông tin của họ.		
A.7.2.1.	Trách nhiệm Lãnh đạo	*Kiểm soát* Lãnh đạo phải yêu cầu tất cả người lao động, nhà thầu phải tuân thủ an ninh thông tin theo đúng chính sách đã thiết lập và quy trình của tổ chức

A.7.2.2	Nhận thức, giáo dục và đào tạo an ninh thông tin	*Kiểm soát* Tất cả nhân niên của tổ chức, những nơi liên quan, nhà thầu phải nhận được sự giáo dục đầy đủ, đào tạo và định kỳ cập nhật chính sách, quy trình có liên quan đến việc thực hiện công việc của họ.
A.7.2.3	Quá trình xử lý kỷ luật	*Kiểm soát* Phải thiết lập văn bản và truyền thông về quá trình xử lý kỷ luật tại chỗ đối với hành vi vi phạm an ninh của nhân viên
A.7.3. Chấm dứt hoặc thay đổi hợp đồng		
Mục đích: Để bảo vệ lợi ích của tổ chức khi có những thay đổi hay kết thúc hợp đồng		
A7.3.1.	Chấm dứt hoặc thay đổi trách nhiệm của nhân viên	*Kiểm soát* Trách nhiệm và nhiệm vụ bảo mật thông tin vẫn phải có hiệu lực sau khi có những thay đổi hoặc chấm dứt được xác định, được truyền thông tới nhân viên, nhà thầu và yêu cầu tuân thủ.
A.8. Quản lý tài sản		
A.8.1. Trách nhiệm đối với tài sản		
Mục đích: Nhằm xác định tài sản của tổ chức và chỉ rõ trách nhiệm bảo vệ phù hợp		
A.8.1.1.	Kiểm kê tài sản	*Kiểm soát* Tài sản chứa đựng thông tin và các thiết bị xử lý thông tin phải được nhận biết và việc kiểm kê các tài sản này phải được hoạch định và duy trì
A.8.1.2	Sở hữu tài sản	*Kiểm soát* Phải duy trì việc kiểm kể tài sản có sở hữu
A.8.1.2	Cho phép sử dụng tài sản	*Kiểm soát* Quy định cho phép sử dụng thông tin, tài sản chứa thông tin và các thiết bị xử lý thông tin phải được xác định rõ, văn bản hóa và được tuân thủ
A.8.1.4.	Hoàn trả tài sản	*Kiểm soát* Tất cả nhân viên, người sử dụng bên ngoài phải trả lại tổ chức các tài sản mà họ đang quản lý khi thuyên chuyển công tác, kết thúc hợp đồng hoặc các thỏa thuận
A.8.2. Phân loại thông tin		

Mục đích: Nhằm đảm bảo thông tin được bảo vệ mức độ thích hợp		
A.8.2.1	Phân loại thông tin	*Kiểm soát* Thông tin được phân loại theo các yêu cầu pháp luật, giá trị, tầm quan trọng, mức độ nhạy cảm khi bị tiết lộ hoặc sửa đổi.
A.8.2.2.	Dán nhãn thông tin	*Kiểm soát* Quy trình dán nhãn thông tin phải được thiết lập và thực hiệp phù hợp với các yêu cầu phân loại thông tin của tổ chức
A.8.2.3	Sử dụng tài sản	*Kiểm soát* Quy trình sử dụng tài sản thông tin phải được thiết lập và thực hiện phù hợp với các yêu cầu phân loại thông tin của tổ chức
A.8.3. Quản lý phương tiện truyền thông		
Mục đích: Nhằm ngăn ngừa những tiết lộ, chỉnh sửa, di chuyển hoặc xóa bỏ kho thông tin được lưu trữ trên phương tiện truyền thông		
A.8.3.1.	Quản lý phương tiện truyền thông có thể di dời	*Kiểm soát* Thủ tục quản lý phương tiện truyền thông có thể di dời phải được thiết lập phù hợp với sự phân loại các tài sản thông tin của tổ chức
A.8.3.2	Loại bỏ phương tiện truyền thông	*Kiểm soát* Phải thiết lập quy trình kiểm soát việc loại bỏ các phương tiện truyền thông không còn sử dụng
A.8.3.3.	Chuyển giao vật lý các phương tiện truyền thông	*Kiểm soát* Phương tiện truyền thông có chứa thông tin phải được bảo vệ chống lại sự truy cập trái phép, sử dụng trái phép hoặc di chuyển trái phép
A.9. Kiểm soát truy cập		
A.9.1. Yêu cầu kinh doanh đối với kiểm soát truy cập		
Mục đích: Nhằm hạn chế truy cập thông tin và các thiết bị xử lý thông tin		
A9.1.1.	Chính sách kiểm soát truy cập	*Kiểm soát* Chính sách kiểm soát truy cập phải được thiết lập, văn bản hóa và xem xét dựa trên các yêu cầu của hoạt động kinh doanh và an ninh thông tin
A.9.1.2.	Truy cập vào mạng và dịch vụ mạng	*Kiểm soát* Người dùng chỉ được cấp quyền truy cập vào mạng và

		các dịch vụ mạng khi được phép.
A.9.2. Quản lý truy cập người sử dụng		
Mục tiêu: Đảm bảo người dùng hợp pháp được truy cập và ngăn chặn truy cập bất hợp pháp vào các hệ thống và dịch vụ		
A.9.2.1.	Đăng ký thành viên và xóa đăng ký	*Kiểm soát* Quy trình đăng ký và xóa đăng ký thành viên phải được thiết lập để kích hoạt việc cấp quyền truy cập
A.9.2.2.	Cấp quyền truy cập	*Kiểm soát* Quy trình cấp quyền truy cập phải được thực hiện đảm bảo việc cấp hoặc xóa quyền truy cập của người dùng đối với tất cả các hệ thống và dịch vụ
A.9.2.3	Quản lý đặc quyền truy cập	*Kiểm soát* Việc cấp phát và sử dụng đặc quyền phải được giới hạn và kiểm soát.
A.9.2.4	Quản lý bảo mật thông tin xác thực người dùng	*Kiểm soát* Phải lập một quy trình quản lý, kiểm soát việc cấp thông tin xác thực của người dùng
A.9.2.5.	Xem xét quyền truy cập người dùng	*Kiểm soát* Chủ sở hữu tài sản phải định kỳ xem xét quyền truy cập của người dùng
A.9.2.6.	Cắt và điều chỉnh quyền truy cập	*Kiểm soát* Quyền truy cập của người dùng của tất cả nhân viên hay đối tác bên ngoài tới thông tin và các thiết bị xử lý thông tin phải được xóa theo căn cứ vào thời điểm kết thúc tuyển dụng, hợp đồng hoặc thỏa thuận hoặc điều chỉnh phụ thuộc vào những thay đổi
A.9.3. Trách nhiệm của người dùng		
Mục tiêu: Để người sử dụng có trách nhiệm đối với việc bảo vệ thông tin xác thực		
A.9.3.1.	Sử dụng bảo mật thông tin xác thực	*Kiểm soát* Người dùng được yêu cầu tuân thủ quy trình sử dụng bảo mật thông tin xác thực
A.9.4. Kiểm soát truy cập ứng dụng và hệ thống		
Mục tiêu: Nhằm ngăn ngừa truy cập trái phép vào các ứng dụng và các hệ thống		
A.9.4.1.	Giới hạn truy cập thông tin	*Kiểm soát* Việc truy cập thông tin và các chức năng hệ thống ứng

		dụng phải được giới hạn trong chính sách kiểm soát truy cập
A.9.4.2	Thủ tục an ninh kết nối	*Kiểm soát* ở những nơi áp dụng chính sách truy cập, việc truy cập vào hệ thống và ứng dụng phải được kiểm soát bởi thủ tục an ninh kết nối.
A.9.4.3.	Hệ thống quản lý mật khẩu	*Kiểm soát* Các hệ thống quản lý mật khẩu phải có tính tương hỗ và phải đảm bảo chất lượng của các mật khẩu
A.9.4.4.	Sử dụng các chương trình tiện ích đặc quyền	*Kiểm soát* Sử dụng các chương trình tiện ích phải được giới hạn và kiểm soát chặt chẽ bơi có thể gây ra quá tải việc kiểm soát hệ thống và ứng dụng.
A.9.4.5.	Kiểm soát truy cập tới source code	*Kiểm soát* Việc truy cập tới source code phải kiểm soát chặt
A.10. Mã hóa		
A.10.1. Kiểm soát mã hóa		
Mục tiêu: Đảm bảo việc sử dụng biện pháp mã hóa phù hợp và hiệu quả để bảo vệ tính bảo mật, xác thức và hoặc tính toàn vẹn của thông tin.		
A.10.1.1.	Chính sách kiểm soát sử dụng mã hóa	*Kiểm soát* Phải thiết lập chính sách và tuân thủ kiểm soát sử dụng mã hóa để bảo vệ thông tin
A.10.1.2.	Quản lý khóa	*Kiểm soát* Một chính sách sử dụng, bảo vệ vòng đời sử dụng khóa phải được thiết lập và yêu cầu tuân thủ
A.11. An ninh vật lý và môi trường		
A.11.1. Các khu vực an ninh		
Mục tiêu: Để phòng các truy cập vật lý bất hợp pháp, phá hoại và quấy rối tới tài sản thông tin và các thiết bị xử lý thông tin của tổ chức		
A.11.1.1.	Thiết bị kiểm soát an ninh vật lý	*Kiểm soát* Các thiết bị kiểm soát an ninh vật lý phải được xác định và sử dụng để bảo vệ các khu vực có chứa thông tin nhạy cảm hoặc bị giới hạn và các thiết bị xử lý thông tin.
A.11.1.2.	Kiểm soát truy cập vật	*Kiểm soát*

	lý	Các khu vực an ninh phải được bảo vệ bằng các kiểm soát truy cập phù hợp để đảm bảo chỉ có những người được phép mới được quyền truy cập
A.11.1.3	An ninh các khu vực văn phòng, không gian và thiết bị	*Kiểm soát* An ninh vật lý cho văn phòng, khu vực và thiết bị phải được hoạch định thiết kế và áp dụng
A.11.1.4.	Bảo vệ các mối nguy từ bên ngoài và môi trường	*Kiểm soát* Phải hoạch định và áp dụng các biện pháp bảo vệ vật lý đối với các thảm họa tự nhiên, sự tấn công có chủ đích hoặc các tai nạn
A.11.1.5	Làm việc trong khu vực an ninh	*Kiểm soát* Thiết lập quy trình và áp dụng việc kiểm soát làm việc tại các khu vực an ninh
A.11.1.6	Các khu vực truy cập tự do, phân phối và chuyển hàng	*Kiểm soát* Các điểm truy cập, ví dụ các khu vực giao hàng, phân phối và các điểm khác, nơi mà người truy cập không cần cấp phép phải được kiểm soát và nếu có thể biệt lập khỏi các phương tiện xử lý thông tin để tránh tình trạng truy cập trái phép.
A.11.2. Thiết bị		
Mục tiêu: Để phòng việc mất, phá hoại, mất cắp hoặc thỏa hiệp các tài sản và gián đoạn các hoạt động của tổ chức.		
A.11.2.1.	Bố trí và bảo vệ thiết bị	*Kiểm soát* Các thiết bị được bố trí bảo vệ nhằm giảm rủi ro đến từ các mối nguy, hiểm họa môi trường và các cơ hội cho sự truy cập trái phép
A.11.2.2.	Các tiện ích hỗ trợ	*Kiểm soát* Các thiết bị phải được bảo vệ khỏi sự cố từ nguồn điện hoặc những gián đoạn gây ra bởi lỗi các tiện ích hỗ trợ.
A.11.2.3	An ninh đường cáp	*Kiểm soát* Dây dẫn nguồn điện và dây cáp viễn thông có chứa thông tin hoặc các dịch vụ hỗ trợ thông tin phải được bảo vệ khỏi sự xâm phạm hoặc phá hoại.
A.11.24.	Bảo trì thiết bị	*Kiểm soát* Các thiết bị phải được bảo trì đúng quy định đảm bảo tín toàn vẹn và sẵn sàng
A.11.2.5	Di chuyển tài sản	*Kiểm soát*

		Thiết bị, thông tin hoặc phần mềm không được mang ra khỏi địa đểm nếu không có sự phê duyệt trước.
A.11.2.6	An ninh thiết bị và tài sản ở bên ngoài	*Kiểm soát* An ninh được áp dụng đối với các tài sản được được mang ra khỏi địa điểm, phải tính đến các rủi ro trong quá trình làm việc bên ngoài của tổ chức
A.11.2.7	An ninh đối với các thiết bị bị loại bỏ hoặc tái sử dụng	*Kiểm soát* Tất cả các hạng mục thiết bị có chứa thông tin lưu trữ phải được thẩm định đảm bảo bất kỳ thông tin nhạy cảm nào và phần mềm có bản quyền phải được gỡ bỏ hoặc ghi đè trước khi loại bỏ hoặc tái sử dụng
A.11.2.8	Các thiết bị vắng mặt người sử dụng	*Kiểm soát* Người sử dụng phải đảm bảo rằng tất cả các thiết bị vắng mặt người sử dụng phải được bảo vệ phù hợp
A.11.2..9	Chính sách bàn sạch và màn hình sạch	*Kiểm soát* Chính sách bàn làm việc sạch không có giấy và các phương tiện lưu trữ di động và chính sách màn hình sạch đối với các phương tiện xử lý thông tin phải được thực hiện
A.12. Điều hành an ninh		
A.12.1. Quy trình và trách nhiệm điều hành		
Mục tiêu: Đảm bảo việc điều hành các thiết bị xử lý thông tin được đúng và đảm bảo an ninh		
A.12.1.1	Văn bản hóa các quy trình điều hành	*Kiểm soát* Các quy trình điều hành phải được văn bản hóa và sẵn sàng cho tất cả người sử dụng khi cần
A.12.1.2	Quản lý thay đổi	*Kiểm soát* Những thay đổi về tổ chức, quá trình kinh doanh, các hệ thống và thiết bị xử lý thông tin ảnh hưởng đến an ninh thông tin phải được kiểm soát
A.12.1.3	Quản lý năng lực	*Kiểm soát* Việc sử dụng các nguồn lực phải được giám sát, điều chỉnh và dự đoán xu hướng yêu cầu năng lực đảm bảo hệ thống được thực thi đúng yêu cầu.
A.12.1.4	Biệt lập các môi trường phát triển, kiểm tra và điều hành	*Kiểm soát* Phát triển, kiểm thử và môi trường điều hành phải được biệt lập đảm bảo giảm rủi ro đối với truy cập trái

		phép hoặc những thay đổi tới môi trường điều hành
A.12.2. Bảo vệ khỏi mã độc		
Mục tiêu : Đảm bảo thông tin và các thiết bị xử lý thông tin được bảo vệ khỏi các mã độc		
A.12.2.1	Kiểm soát mã độc	*Kiểm soát* Các kiểm soát để phát hiện phòng ngừa, bảo vệ và phục hồi nhằm chống lại phải được thực hiện, kết hợp với nhận thức của người sử dụng
A.12.3 Sao lưu		
Mục tiêu: Bảo vệ việc mất dữ liệu		
A.12.3.1	Sao lưu dữ liệu	*Kiểm soát* Sao lưu thông tin, phần mềm và hình ảnh hệ thống phải được thực hiện kiểm tra định kỳ phù hợp với chính sách sao lưu được phê duyệt
A.12.4. Nhật ký và giám sát		
Mục tiêu : Để ghi lại các sự kiện và bằng chứng phát sinh		
A.12.4.1.	Nhật ký sự kiện	*Kiểm soát* Nhật ký ghi lại các hoạt động của người dùng, sự chấp nhận, lỗi và các sự kiện an ninh thông tin phải được thực hiện, lưu giữ và xem xét định kỳ
A.12.4.2	Bảo vệ các thông tin nhật ký	*Kiểm soát* Các thiết bị ghi nhật ký và thông tin nhật ký phải được bảo vệ khỏi những can thiệp và truy cập trái phép
A.12.4.3.	Nhật ký đăng nhập của Quản trị viên và người vận hành	*Kiểm soát* Quản trị viên hệ thống và các hoạt động vận hành hệ thống phải được ghi nhật ký và các bản ghi nhật ký phải được bảo vệ và xem xét thường xuyên
A.12.4.3.	Đồng bộ thời gian	*Kiểm soát* Đồng hồ trên tất cả các hệ thống xử lý thông tin trong tổ chức hoặc miền an ninh phải được đồng bộ với một nguồn thời gian tham chiếu.
A.12.5. Kiểm soát điều hành phần mềm		
Mục tiêu: Đảm bảo việc tích hợp các hệ thống điều hành		
A.12.5.1	Cài đặt phần mềm trên hệ thống điều hành	*Kiểm soát* Phải xây dựng quy trình để kiểm soát quá trình cài đặt

		các phần mềm trên các hệ thống điều hành
A.12.6. Quản lý điểm yếu kỹ thuật		
Mục tiêu: Nhằm bảo vệ việc khai thác các điểm yếu kỹ thuật		
A.12.6.1.	Quản lý các điểm yếu về kỹ thuật	*Kiểm soát* Thông tin về các điểm yếu kỹ thuật của hệ thống thông tin đang sử dụng phải được cập nhật, tổ chức phải đánh giá các điểm yếu trên và tiến hành các biện pháp kiểm soát phù hợp để giải quyết các rủi ro liên quan.
A.12.6.2	Giới hạn cài đặt các phần mềm	*Kiểm soát* Các quy tắc quản lý việc cài đặt phần mềm cho người dùng phải được thiết lập và kiểm soát
A.12.7. Đánh giá hệ thống thông tin		
Mục tiêu: Các hoạt động đánh giá nhằm giảm thiểu các tác động tới hệ thống điều hành		
A.12.7.1	Kiểm soát việc đánh giá hệ thống thông tin	*Kiểm soát* Các yêu cầu đánh giá và hoạt động thẩm định điều hành hệ thông thông tin phải được hoạch định cẩn trọng và phải có sự đồng thuận nhằm giảm thiểu những phá vỡ tới các quy trình kinh doanh
A.13. An ninh trong quá trình truyền đạt thông tin		
Mục đích: Đảm bảo việc bảo vệ thông tin trong hệ thống mạng và các thiết bị hỗ trợ xử lý thông tin		
A.13.1.1.	Kiểm soát mạng	*Kiểm soát* Các mạng phải được quản lý và kiểm soát để bảo vệ thông tin trong các hệ thống và ứng dụng
A.13.1.2	An ninh dịch vụ mạng	*Kiểm soát* Cơ chế an ninh, các mức dịch vụ và các yêu cầu quản lý tất cả dịch vụ mạng phải được xác định, bao gồm các thỏa thuận dịch vụ mạng, được cung cấp bởi nội bộ hoặc bên ngoài.
A.13.1.3	Tách biệt mạng	*Kiểm soát* Các nhóm dịch vụ thông tin, người sử dụng các hệ thống thông tin phải được biệt lập trên các mạng
A.13.2. Truyền tin		
Mục tiêu: Duy trì an ninh trong việc truyền tin giữa tổ chức và bất kỳ mối quan hệ bên ngoài nào		

A.13.2.1	Chính sách truyền tin và các quy trình	*Kiểm soát* Chính sách truyền tin, quy trình và các biện pháp kiểm soát để bảo vệ việc truyền tải thông tin khi sử dụng tất cả các thiết bị trao đổi thông tin.
A.13.2.2.	Thỏa thuận truyền tin	*Kiểm soát* Các thỏa thuận phải đảm bảo an ninh trong quá trình truyền tải tin giữa tổ chức và các bên ngoài.
A.13.2.3	Thông điệp điện tử	*Kiểm soát* Thông tin trong các thông điệp điện tử phải được bảo vệ thỏa đáng
A.13.2.4	Thỏa thuận bảo mật và không tiết lộ thông tin	*Kiểm soát* Các yêu cầu thỏa thuận bảo mật và không tiết lộ thông tin phản ánh yêu cầu của tổ chức trong việc bảo vệ thông tin phải được xác định, định kỳ xem xét và văn bản hóa
A.14. Yêu cầu hệ thống, phát triển và duy trì		
A.14.1. Các yêu cầu an ninh đối với hệ thống thông tin		
Mục tiêu: Đảm bảo an ninh thông tin là một phần được tích hợp vào toàn bộ vòng đời hệ thống thông tin của tổ chức. Điều này bao gồm các yêu cầu đối với các nhà hệ thống thông tin cung cấp dịch vụ mạng công cộng		
A.14.1.1.	Phân tích và đặc tả các yêu cầu về an toàn thông tin	*Kiểm soát* Các yêu cầu an ninh thông tin phải được đưa ra khi thiết lập mới hoặc nâng cấp hệ thống thông tin đang vận hành.
A.14.1.2	An ninh đối với các dịch vụ ứng dụng trên mạng công cộng	*Kiểm soát* Các thông tin trong các dịch vụ ứng dụng trên mạng công cộng phải được bảo vệ khỏi các hoạt động gian lận, tranh chấp hợp đồng , tiết lộ hoặc chỉnh sửa
A.14.1.3	Bảo vệ quá trình chuyển đổi dịch vụ ứng dụng	*Kiểm soát* Các thông tin trong quá trình chuyển đổi dịch vụ ứng dụng phải được bảo vệ tránh khỏi việc chuyển đổi không đầy đủ, sai sót, sửa tin bất hợp pháp, tiết lộ thông tin, tin bị lặp hoặc quay lại
A.14.2. An ninh trong các quá trình phát triển và hỗ trợ		
Mục tiêu: Đảm bảo an ninh thông tin được hoạch định, thực hiện trong vòng đời phát triển hệ thống thông tin		

A.14.2.1.	Chính sách phát triển an ninh	*Kiểm soát* Các nguyên tắc phát triển phần mềm và hệ thống phải được thiết lập và áp dụng nhằm phát triển trong tổ chức
A.14.2.2.	Quy trình kiểm soát sự thay đổi hệ thống	*Kiểm soát* Phải thiết lập quy trình kiểm soát sự thay đổi đối với những thay đổi hệ thống trong quá trình phát triển
A.14.2.3	Xem xét kỹ thuật các ứng dụng sau khi thay đổi nền tảng điều hành.	*Kiểm soát* Khi các nền tảng điều hành bị thay đổi, các ứng dụng giới hạn kinh doanh phải được xem xét và kiểm tra đảm bảo không có tác động có hại nào tới việc điều hành hoặc an ninh của tổ chức
A.14.2.4	Giới hạn sự thay đổi đối với các gói phần mềm	*Kiểm soát* Việc sửa đổi các gói phần mềm không được khuyến khích, phải giới hạn để những thay đổi cần thiết hoặc tất cả những thay đổi phải được kiểm soát nghiêm ngặt.
A.14.2.5	Các nguyên tắc kỹ thuật an ninh hệ thống	*Kiểm soát* Các nguyên tắc cho các kỹ thuật an ninh hệ thống phải được thiết lập, văn bản hóa, được duy trì và áp dụng bằng mọi nỗ lực
A.14.2.6	Môi trường phát triển an ninh	*Kiểm soát* Tổ chức phải thiết lập và bảo vệ phù hợp các môi trường phát triển an ninh cho các nỗ lực phát triển và tích hợp hệ thống, phải bao trùm được toàn bộ vòng đời phát triển hệ thống hiện tại.
A.14.2.7	Phát triển thuê ngoài	*Kiểm soát* Tổ chức phải quản lý và giám sát các hoạt động phát triển hệ thống thuê ngoài
A.14.2.8	Kiểm tra an ninh hệ thống	*Kiểm soát* Kiểm tra các chức năng an ninh phải được thực hiện trong suốt quá trình phát triển
A.14.2.9	Kiểm tra chấp nhận hệ thống	*Kiểm soát* Các chương trình kiểm tra chấp nhận và các tiêu chí liên quan phải được thiết lập khi thiết lập mới, cập nhật và nâng cấp hệ thống thông tin.
A.14.3. Kiểm tra dữ liệu		

Mục tiêu: Nhằm bảo vệ dữ liệu được sử dụng trong quá trình kiểm tra		
A.14.3.1	Bảo vệ dữ liệu kiểm tra	*Kiểm soát* Các dữ liệu kiểm tra phải được lựa chọn cẩn thẩn, bảo vệ và kiểm soát
A.15. Mối quan hệ với nhà cung cấp		
A.15.1. An ninh thông tin trong mối quan hệ với các nhà cung cấp		
Mục tiêu: Bảo đảm việc bảo vệ tài sản của tổ chức bị truy cập bởi nhà cung cấp		
A.15.1.1.	Chính sách an ninh thông tin đối với nhà cung cấp	*Kiểm soát* Các yêu cầu an ninh thông tin nhằm mục đích giảm các rủi ro khi nhà cung cấp truy cập vào tài sản thông tin phải được sự đồng ý của nhà cung cấp và được văn bản hóa
A.15.1.2.	Đáp ứng các thỏa thuận an ninh với nhà cung cấp	*Kiểm soát* Tất cả các yêu cầu an ninh thông tin phải được thiết lập và thỏa thuận với từng nhà cung cấp khi truy cập, xử lý, lưu trữ , trao đổi hoặc cung cấp hạ tầng thông tin của tổ chức
A.15.1.3	Chuỗi cung ứng công nghệ thông tin và truyền thông	*Kiểm soát.* Thỏa thuận với các nhà cung cấp phải bao gồm các yêu cầu đáp ứng rủi ro an ninh thông tin liên quan tới thông tin và các dịch vụ công nghệ truyền thông và chuỗi cung ứng.
A.15.2 Quản lý việc cung cấp dịch vụ của nhà cung cấp		
Mục tiêu: Nhằm đảm bảo một mức độ an ninh thông tin và tuân thủ cung cấp dịch vụ của các nhà cung cấp		
A.15.2.1.	Giám sát và xem xét dịch vụ của nhà cung cấp	*Kiểm soát* Tổ chức phải thường xuyên giám sát, xem xét và đánh giá dịch vụ của nhà cung cấp
A.15.2.2.	Kiểm soát những thay đổi về dịch vụ của nhà cung cấp	*Kiểm soát* Những thay đổi trong quá trình cung cấp dịch vụ, bao gồm bảo trì, cải tiến chính sách an ninh, quy trình, kiểm soát của nhà cung cấp phải được quản lý, xem xét tới các tiêu chí mức độ rủi ro kinh doanh, các hệ thống, các quá trình tham và tái đánh giá rủi ro
A.16. Quản lý sự cố an ninh thông tin		

A.16.1. Quản lý sự cố an ninh thông tin và các cải tiến		
Mục đích : Nhằm đảm bảo một phương pháp tiếp cận phù hợp và hiệu quả trong việc quản lý các sự cố an ninh thông tin, bao gồm cả việc truyền thông các sự kiện an ninh và các điểm yếu.		
A.16.1.1	Trách nhiệm và quy trình	*Kiểm soát* Trách nhiệm quản lý và quy trình phải được thiết lập đảm bảo việc phản ứng nhanh, hiệu quả và đúng trình tự đối với các sự cố an ninh thông tin.
A.16.1.2	Báo cáo các sự kiện an ninh thông tin	*Kiểm soát* Các sự kiện an ninh thông tin phải được báo cáo tới các cấp quản lý phù hợp càng nhanh càng tốt
A.16.1.3	Báo cáo điểm yếu an ninh thông tin	*Kiểm soát* Nhân viên và nhà thầu sử dụng hệ thống thông tin và dịch vụ của tổ chức phải được yêu cầu ghi chép lại và báo cáo bất kỳ các điểm yếu an ninh mà họ quan sát được hay nghi ngờ trong hệ thống và dịch vụ của tổ chức.
A.16.1.4	Đánh giá và và ra quyết định về sự kiện bảo mật thông tin	*Kiểm soát* Các sự kiện bảo mật thông tin phải được đánh giá và sẽ phải đưa ra quyết định nếu chúng được phân loại như là sự cố an ninh thông tin.
A.16.1.5	Ứng phó với các sự cố an ninh thông tin.	*Kiểm soát* Các sự cố an ninh thông tin phải được ứng phó phù hợp với quy trình được phê duyệt.
A.16.1.6	Học hỏi từ các sự cố an ninh thông tin	*Kiểm soát* Các kiến thức thu được từ việc phân tích và giải quyết các sự cố an ninh thông tin phải được sử dụng để giảm khả năng và tác động các sự cố trong tương lai.
A.16.1.7	Thu thập bằng chứng	*Kiểm soát* Phải thiết lập và áp dụng quy trình từ khâu: xác định, tập hợp, thu thập và bảo vệ thông tin, mà được coi là bằng chứng.
A.17. Các khía cạnh an ninh thông tin trong quản lý kinh doanh liên tục.		
A.17.1 Tính liên tục an ninh thông tin		
Mục tiêu : Tính liên tục của an ninh thông tin luôn gắn vào hệ thống quản lý kinh doanh liên tục		

của tổ chức		
A.17.1.1	Hoạch định tính liên tục an ninh thông tin	*Kiểm soát* Tổ chức phải xác định các yêu cầu đối với an ninh thông tin và tính liên tục của việc quản lý an ninh thông tin trong mọi tình huống bất lợi, ví dụ trong các cuộc khủng hoảng hoặc thảm họa
A.17.1.2	Áp dụng tính liên tục an ninh thông tin	*Kiểm soát* Tổ chức phải thiết lập, văn bản hóa, thực hiện và duy trì các quá trình, quy trình và các kiểm soát đảm bảo các mức yêu cầu của tính liên tục của an ninh thông tin trong mọi tình huống bất lợi
A.17.1.3	Thẩm định, xem xét và đánh giá tính liên tục an ninh thông tin	*Kiểm soát* Định kỳ tổ chức phải thẩm định việc thiết lập và định kỳ thực hiện các kiểm soát tính liên tục an ninh thông tin đảm bảo rằng hệ thống vẫn có hiệu lực và hiệu quả trong mọi tình huống bất lợi
A.17.2 : Sự dư thừa		
Mục tiêu : Để đảm bảo các thiết bị xử lý thông tin luôn sẵn có		
A.17.2.1	Sẵn có các thiết bị xử lý thông tin	*Kiểm soát* Các thiết bị xử lý thông tin phải được dư thừa để đáp ứng các yêu cầu sẵn có yêu cầu
A.18 . Sự phù hợp		
A.18.1. Phù hợp với các yêu cầu pháp lý và yêu cầu hợp đồng		
Mục tiêu : Để tránh các vi phạm về pháp lý, quy định hoặc các điều khoản bắt buộc trong hợp đồng liên quan đến an ninh thông tin và bất cứ các yêu cầu an ninh nào khác		
A.18.1.1	Xác định các yêu cầu luật định và yêu cầu hợp đồng	*Kiểm soát* Tất cả các yêu cầu chế định, luật định yêu cầu trong hợp đồng và phương thức đáp ứng yêu cầu của tổ chức phải được xác định, văn bản hóa, cập nhật cho từng hệ thống thông tin và tổ chức
A.18.1.2	Quyền sở hữu trí tuệ	*Kiểm soát* Một quy trình phù hợp phải được thực hiện để đảm bảo tuân thủ luật, quy định và các yêu cầu hợp đồng liên quan đến quyền sở hữu trí tuệ và việc sử dụng các sản phẩm phần mềm có bản quyền
A.18.1.3	Bảo vệ các hồ sơ	*Kiểm soát*

		Hồ sơ phải được bảo vệ khỏi sự mất mát, phá hoại, giả mạo, truy cập trái phép và bàn giao không cho phép , phù hợp với các quy định của pháp luật, điều khoản hợp đồng và các yêu cầu kinh doanh
A.18.1.4	Sự riêng tư và bảo vệ thông tin cá nhân	*Kiểm soát* Sự riêng tư và bảo vệ thông tin cá nhân phải được đảm bảo theo yêu cầu pháp luật và quy định tại nơi áp dụng
A.18.1.5	Quy định kiểm soát mã hóa	*Kiểm soát* Kiểm soát mã hóa phải được áp dụng phù hợp với các thỏa thuận liên quan, các quy định của pháp luật và của tổ chức
A.18.2 Độc lập xem xét an ninh thông tin		
Mục tiêu : Để đảm bảo an ninh thông tin được thực hiện và điều hành phù hợp với chính sách và quy trình của tổ chức		
A.18.2.1	Xem xét độc lập an ninh thông tin	*Kiểm soát* Cách tiếp cận của tổ chức để quản lý và thực hiện an ninh thông tin (ví dụ : các mục tiêu kiểm soát, các kiểm soát, chính sách quy trình và các quá trình an ninh) phải được định kỳ xem xét độc lập hoặc khi xuất hiện những thay đổi đáng kể nào
A.18.2.2	Sự phù hợp với các chính sách an ninh và tiêu chuẩn	*Kiểm soát* Các lãnh đạo phải định kỳ xem xét sự phù hợp của việc xử lý thông tin và các quy trình trong thẩm quyền trách nhiệm của họ có phù hợp với chính sách an ninh, tiêu chuẩn hay bất kỳ yêu cầu an ninh nào khác
A.18.2.3	Xem xét sự phù hợp yêu tố kỹ thuật	*Kiểm soát* Các hệ thống thông tin phải được thường xuyên xem xét phù hợp với chính sách an ninh và tiêu chuẩn

TÀI LIỆU THAM KHẢO