TCVN TIÊU CHUẨN QUỐC GIA

TCVN 11238:2015
ISO/IEC 27000:2014

Sx1(2015)

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

HÀ NỘI - 2015

Mục lục

Lời nói đầu

TCVN 11238:2015 hoàn toàn tương đương với ISO/IEC 27000:2014.

TCVN 11238:2015 do Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) 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.

Lời giới thiệu

Tổng quan

Các tiêu chuẩn cho hệ thống quản lý cung cấp một mô hình cho việc thiết lập và vận hành một hệ thống quản lý. Mô hình này kết hợp các đặc tính mà các chuyên gia trong lĩnh vực an toàn thông tin đã đạt được sự đồng thuận ở phạm vi quốc tế. Các tiêu chuẩn quốc gia về quản lý an toàn thông tin gọi là họ tiêu chuẩn về hệ thống quản lý an toàn thông tin (ISMS - Information Security Management System).

Thông qua sử dụng họ tiêu chuẩn ISMS, các tổ chức có thể xây dựng và triển khai một bộ khung cho việc quản lý an toàn các tài sản thông tin của họ, bao gồm các thông tin tài chính, sở hữu trí tuệ, chi tiết về nhân sự, hoặc các thông tin đã được các khách hàng hay bên thứ ba cung cấp. Các tiêu chuẩn này cũng có thể được dùng để chuẩn bị cho các đánh giá độc lập các hệ thống ISMS đã được áp dụng để bảo vệ thông tin.

Họ tiêu chuẩn ISMS

Họ tiêu chuẩn ISMS (xem Điều 4) nhằm mục đích hỗ trợ các tổ chức thuộc mọi loại hình, mọi quy mô để triển khai và vận hành một hệ thống quản lý an toàn thông tin, bao gồm các tiêu chuẩn sau đây dưới tiêu đề chung *Công nghệ thông tin - Các kỹ thuật an toàn* (sắp xếp theo thứ tự con số):

- TCVN 11238 (*ISO/IEC 27000*), Hệ thống quản lý an toàn thông tin - Tổng quan và từ vựng *(Information security management systems - Overview and vocabulary).*

- TCVN ISO/IEC 27001 (ISO/IEC 27001), Hệ thống quản lý an toàn thông tin - Các yêu cầu *(ISO/IEC 2700Information security management systems - Requirements)*

- TCVN ISO/IEC 27002 (ISO/IEC 27002), Quy tắc thực hành cho hệ thống quản lý an toàn thông tin *(Code of practice for information security management).*

- TCVN 10541 (ISO/IEC 27003), Hướng dẫn triển khai hệ thống quản lý an toàn thông tin *(Information security management system implementation guidance).*

- TCVN 10542 (ISO/IEC 27004), Quản lý an toàn thông tin - Đo lường *(Information security management - Measurement).*

- TCVN 10295 (ISO/IEC 27005), Quản lý rủi ro an toàn thông tin *(Information security risk management).*

- ISO/IEC 27006, Các yêu cầu đối với cơ quan đánh giá và chứng nhận hệ thống quản lý an toàn thông tin (Requirements for bodies providing audit and certification of information security management systems).

- ISO/IEC 27007, Hướng dẫn đánh giá hệ thống quản lý an toàn thông tin *(Guidelines for information security management systems auditing).*

- ISO/IEC TR 27008, Hướng dẫn cho đánh giá viên về biện pháp kiểm soát hệ thống quản lý an toàn thông tin *(Guidelines for auditors on information security management systems controls).*

- TCVN 10543 (ISO/IEC 27010), Quản lý an toàn trao đổi thông tin liên tổ chức, liên ngành *(Information security management guidelines for inter-sector and inter-organisational communications).*

- ISO/IEC 27011, Hướng dẫn quản lý an toàn thông tin cho các tổ chức viễn thông dựa theo ISO/IEC 27002 *(Information security management guidelines for telecommunications organisations based on ISO/IEC 27002).*

- TCVN 9965 (ISO/IEC 27013), Hướng dẫn triển khai tích hợp TCVN ISO/IEC 27001 và ISO/IEC 20000-1 *(Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1).*

- ISO/IEC 27014, Quản trị an toàn thông tin *(Governance of information security).*

- ISO/IEC TR 27015, Hướng dẫn quản lý an toàn thông tin cho các dịch vụ tài chính *(Information security management guidelines for financial services).*

- ISO/IEC TR 27016, Quản lý an toàn thông tin - Kinh tế của tổ chức *(Information security management - Organisational economics).*

CHÚ THÍCH: Tiêu đề chung "Công nghệ thông tin - Các kỹ thuật an toàn" biểu thị các tiêu chuẩn này được biên soạn bởi Ủy ban kỹ thuật liên ngành ISO/IEC JTC 1, *Công nghệ thông tin*, tiểu ban SC 27, *Các kỹ thuật an toàn Công nghệ thông tin*.

Các tiêu chuẩn không thuộc tiêu đề chung nêu trên song vẫn thuộc họ tiêu chuẩn ISMS bao gồm:

- ISO 27799:2008, Tin học y tế - Quản lý an toàn thông tin trong y tế sử dụng ISO/IEC 27002 *(Health informatics - Information security management in health using ISO/IEC 27002).*

Mục đích của tiêu chuẩn này

Tiêu chuẩn này trình bày tổng quan về hệ thống quản lý an toàn thông tin, định nghĩa các thuật ngữ liên quan.

CHÚ THÍCH: Phụ lục A trình bày rõ hơn về việc các dạng quy ước được sử dụng để biểu thị các yêu cầu và/hoặc hướng dẫn trong họ tiêu chuẩn ISMS.

Họ tiêu chuẩn ISMS bao gồm các tiêu chuẩn với nội dung:

a) Xác định các yêu cầu đối với một hệ thống quản lý an toàn thông tin (ISMS) và việc chứng nhận các hệ thống đó;

b) Cung cấp hỗ trợ trực tiếp, hướng dẫn chi tiết và/hoặc giải nghĩa cho các yêu cầu và các quy trình khái quát để thiết lập, triển khai, duy trì và cải thiện một hệ thống quản lý an toàn thông tin.

c) Trình bày các hướng dẫn theo lĩnh vực cụ thể cho hệ thống quản lý an toàn thông tin (ISMS);

d) Trình bày việc đánh giá tuân thủ cho hệ thống quản lý an toàn thông tin (ISMS) .

Các thuật ngữ và định nghĩa đưa ra trong tiêu chuẩn này:

- gồm các thuật ngữ và định nghĩa được sử dụng chung trong họ tiêu chuẩn ISMS;

- Không gồm tất cả các thuật ngữ và định nghĩa áp dụng trong họ tiêu chuẩn ISMS;
- Không hạn chế họ tiêu chuẩn ISMS trong việc đưa thêm các thuật ngữ mới khi áp dụng.

Công nghệ thông tin - Các kỹ thuật an toàn - Hệ thống quản lý an toàn thông tin - Tổng quan và từ vựng

Infomation technology - Security techniques - Infomation security manegement system - Overview and Vocabulary

1 Phạm vi áp dụng

Tiêu chuẩn này cung cấp tổng quan về hệ thống quản lý an toàn thông tin và các thuật ngữ, định nghĩa thường được sử dụng trong họ tiêu chuẩn ISMS. Tiêu chuẩn này được áp dụng cho tất cả các loại hình và quy mô tổ chức (ví dụ các doanh nghiệp thương mại, các cơ quan chính phủ, các tổ chức phi lợi nhuận).

2 Thuật ngữ và định nghĩa

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

2.1

Biện pháp kiểm soát truy cập (access control)

Sự đảm bảo về việc truy cập vào các tài sản là được phép và bị hạn chế dựa trên cơ sở những yêu cầu an toàn và nghiệp vụ.

2.2

Mô hình phân tích (analytical model)

Mô hình có sử dụng thuật toán hoặc phép tính toán kết hợp một hoặc nhiều *số đo cơ bản* (2.10) và/hoặc các *số đo dẫn xuất* (2.22) với tiêu chí quyết định liên quan.

2.3

Tấn công (attack)

Việc tìm cách phá hủy, làm lộ, thay đổi, vô hiệu hóa, đánh cắp hoặc giành quyền truy cập trái phép hoặc thực thi việc sử dụng trái phép một tài sản.

2.4

Thuộc tính (attribute)

Đặc tính hoặc đặc điểm của một *đối tượng* (2.55) có thể dùng để phân biệt định tính hoặc định lượng bởi con người hoặc các phương thức tự động.

[ISO/IEC 15939:2007]

2.5

Đánh giá (audit)

Quy trình (2.61) có hệ thống, độc lập và được lập tài liệu để thu được bằng chứng đánh giá và đánh giá bằng chứng này một cách khách quan để xác định mức độ đáp ứng của các tiêu chí đánh giá.

CHÚ THÍCH 1: Đánh giá có thể là đánh giá nội bộ (bên thứ nhất) hoặc đánh giá bên ngoài (bên thứ hai hoặc bên thứ ba) và có thể là một cuộc đánh giá kết hợp (kết hợp hai hoặc nhiều hơn các nguyên tắc).

CHÚ THÍCH 2: "Bằng chứng đánh giá" và "tiêu chí đánh giá" được định nghĩa trong TCVN ISO 19011

2.6

Phạm vi đánh giá (audit scope)

Mức độ và giới hạn của việc *đánh giá* (2.5).

[TCVN ISO 19011:2013]

2.7

Xác thực (authentication)

Cung cấp sự đảm bảo về việc một đặc điểm được tuyên bố của một thực thể là chính xác.

2.8

Tính xác thực (authenticity)

Đặc tính mà một thực thể là thứ đã được tuyên bố.

2.9

Tính sẵn sàng (availability)

Đặc tính có thể truy cập và sử dụng được theo yêu cầu của một thực thể được phép.

2.10

Số đo cơ bản (base measure)

Số đo (2.47) xác định bởi một *thuộc tính* (2.4) và phương pháp định lượng nó.

[ISO/IEC 15939:2007]

CHÚ THÍCH 1: Số đo cơ bản là độc lập về chức năng với các số đo khác.

2.11

Năng lực (competence)

Khả năng ứng dụng kiến thức và kỹ năng để đạt được kết quả dự kiến.

2.12

Tính bí mật (confidentiality)

Đặc tính thông tin không sẵn sàng cung cấp hoặc không được tiết lộ cho các cá nhân, thực thể hoặc các quá trình 2.61 không được phép.

2.13

Sự phù hợp (conformity)

Sự đáp ứng một *yêu cầu* (2.63).

CHÚ THÍCH: Thuật ngữ "conformance" là đồng nghĩa nhưng hiện đã không dùng.

2.14

Hậu quả (consequence)

Kết quả của một *sự kiện* (2.25) có ảnh hưởng tác động đến *mục tiêu* (2.56).

[Có sửa đổi TCVN 9788:2013 (ISO GUIDE 73:2009)]

CHÚ THÍCH 1: Một sự kiện có thể dẫn đến một loạt các hậu quả.

CHÚ THÍCH 2: Một hậu quả có thể chắc chắn hoặc không chắc chắn và thường có tính tiêu cực trong bối cảnh an toàn thông tin.

CHÚ THÍCH 3: Hậu quả có thể được biểu thị định tính hoặc định lượng.

CHÚ THÍCH 4: Hậu quả ban đầu có thể bị leo thang qua hiệu ứng dây chuyền.

2.15

Cải tiến liên tục (continual improvement)

Hoạt động có định kỳ để nâng cao hiệu năng (2.59).

2.16

Biện pháp kiểm soát (control)

Biện pháp điều chỉnh *rủi ro* (2.68).

[TCVN 9788:2013 (ISO GUIDE 73:2009)]

CHÚ THÍCH 1: Biện pháp kiểm soát bao gồm bất kỳ quy trình, chính sách, thiết bị, thực hành hoặc các hành động khác nhằm điều chỉnh rủi ro.

CHÚ THÍCH 2: Biện pháp kiểm soát không phải lúc nào cũng có tác động như mong muốn hoặc như đã giả định.

2.17

Mục tiêu của biện pháp kiểm soát (control objective)

Tuyên bố mô tả những gì cần đạt được như là kết quả của việc thực thi các *biện pháp kiểm soát* (2.16).

2.18

Khắc phục (correction)

Hành động để loại bỏ *điểm không phù hợp* (2.53) đã phát hiện.

2.19

Hành động khắc phục (corrective action)

Hành động để loại bỏ nguyên nhân gây ra *điểm không phù hợp* (2.53) và để ngăn chặn sự tái diễn.

2.20

Dữ liệu (data)

Tập hợp các giá trị được gán cho các *số đo cơ bản* (2.10), các *số đo dẫn xuất* (2.22) và/hoặc các *chỉ báo* (2.27).

[ISO/IEC 15939:2007]

CHÚ THÍCH 1: Định nghĩa này chỉ áp dụng trong bối cảnh của TCVN 10542:2014.

2.21

Tiêu chí quyết định (decision criteria)

Ngưỡng, mục tiêu hoặc các mẫu được dùng để xác định sự cần thiết cho hành động hoặc điều tra thêm, hoặc để mô tả mức độ tin cậy trong kết quả đưa ra.

[ISO/IEC 15939:2007]

2.22

Số đo dẫn xuất (derived measure)

Số đo (2.47) được định nghĩa là một hàm của hai hay nhiều giá trị của các *số đo cơ bản* (2.10).

[ISO/IEC 15939:2007]

2.23

Thông tin được lập tài liệu (documented information)

Thông tin có yêu cầu được kiểm soát và duy trì bởi một *tổ chức* (2.57) và môi trường mà nó được chứa đựng.

CHÚ THÍCH 1: Thông tin được lập tài liệu có thể ở bất cứ định dạng, phương tiện và từ bất kỳ nguồn nào.

CHÚ THÍCH 2: Thông tin được lập tài liệu có thể đề cập tới:

- *Hệ thống quản lý* (2.46), bao gồm các *quy trình* (2.61) liên quan;

- Thông tin được tạo để tổ chức vận hành (tài liệu);

- Bằng chứng về các kết quả đã đạt được (bản ghi).

2.24

Hiệu quả (effectiveness)

Mức độ mà các hoạt động theo kế hoạch được thực hiện và các kết quả theo kế hoạch đã đạt được.

2.25

Sự kiện (event)

Sự xuất hiện hoặc thay đổi của một tập sự việc cụ thể.

[TCVN 9788:2013]

CHÚ THÍCH 1: Một sự kiện có thể là một hoặc nhiều biến cố và có thể do nhiều nguyên nhân gây ra.

CHÚ THÍCH 2: Một sự kiện có thể bao gồm những việc không xảy ra.

CHÚ THÍCH 3: Một sự kiện đôi khi có thể được coi là một "sự cố" hoặc "tai nạn".

2.26

Bộ phận quản lý thực thi (executive management)

Cá nhân hoặc nhóm người có trách nhiệm được giao bởi *cơ quan điều hành* (2.29) để triển khai các chiến lược và chính sách để hoàn thành mục tiêu/mục đích của tổ chức (2.57)

CHÚ THÍCH: Bộ phận quản lý thực thi đôi khi còn được gọi là Ban quản lý cấp cao và có thể bao gồm các giám đốc điều hành, giám đốc tài chính, giám đốc công nghệ thông tin và những người có vai trò tương tự.

2.27

Ngữ cảnh bên ngoài (external context)

Môi trường bên ngoài, trong đó một tổ chức tìm cách đạt được mục tiêu của mình.

[TCVN 9788:2013]

CHÚ THÍCH: Bối cảnh bên ngoài có thể bao gồm:

- Môi trường văn hóa, xã hội, chính trị, pháp lý, quy định, tài chính, công nghệ, kinh tế, tự nhiên và cạnh tranh, cho dù là quốc tế, quốc gia, khu vực và địa phương nào;

- Động lực và xu hướng căn bản có ảnh hưởng đến các *mục tiêu* (2.56) của *tổ chức* (2.57);

- Mối quan hệ với các đối tác bên ngoài và nhận thức cũng như giá trị của chúng.

2.28

Quản trị về an toàn thông tin (governance of information security)

Hệ thống mà các hoạt động về an toàn thông tin một *tổ chức* (2.57) được định hướng và kiểm soát.

2.29

Cơ quan điều hành (governing body)

Cá nhân hoặc một nhóm người có trách nhiệm đảm bảo về *hiệu năng* (2.59) và sự tuân thủ của *tổ chức* (2.57)

CHÚ THÍCH: Cơ quan điều hành về pháp lý có thể là một ban giám đốc.

2.30

Chỉ báo (indicator)

Số đo (2.47) cung cấp một ước tính hoặc ước lượng của các *thuộc tính* (2.4) cụ thể được suy ra từ một *mô hình phân tích* (2.2) dành cho các *nhu cầu thông tin* (2.31) xác định.

2.31

Nhu cầu thông tin (information need)

Hiểu biết cần thiết để quản lý các mục tiêu, mục đích, rủi ro và các vấn đề

[ISO/IEC 15939:2007]

2.32

Các phương tiện xử lý thông tin (information processing facilities)

Bất kỳ hệ thống xử lý thông tin, dịch vụ hoặc cơ sở hạ tầng, hoặc vị trí vật lý chứa đựng chúng.

2.33

An toàn thông tin (information security)

Bảo toàn *tính bí mật* (2.11), *tính toàn vẹn* (2.40) và *tính sẵn sàng* (2.9) của thông tin

CHÚ THÍCH: Ngoài ra, an toàn thông tin có thể bao gồm các thuộc tính khác như *tính xác thực* (2.8), trách nhiệm giải trình, *tính chống chối bỏ* (2.54) và *tính tin cậy* (2.62).

2.34

Tính liên tục an toàn thông tin (information security continuity)

Các *quy trình* (2.61) và thủ tục để đảm bảo vận hành liên lục *an toàn thông tin* (2.33).

2.35

Sự kiện an toàn thông tin (information security event)

Sự kiện xác định của một hệ thống, dịch vụ hoặc trạng thái mạng cho thấy có khả năng vi phạm chính sách an toàn thông tin hay sự thất bại của các biện pháp kiểm soát hoặc một tình huống chưa biết có thể liên quan đến an toàn thông tin.

2.36

Sự cố an toàn thông tin (information security incident)

Một hoặc một loạt các *sự kiện an toàn thông tin* (2.35) không mong muốn hoặc không dự tính có khả năng ảnh hưởng đáng kể các đến hoạt động nghiệp vụ và đe dọa *an toàn thông tin* (2.33).

2.37

Quản lý sự cố an toàn thông tin (information security incident management)

Các quy trình (2.61) phát hiện, báo cáo, đánh giá, đáp ứng, đối phó và đúc rút kinh nghiệm từ *sự cố an toàn thông tin* (2.36).

2.38

Cộng đồng chia sẻ thông tin (information sharing community)

Nhóm các tổ chức đồng ý chia sẻ thông tin.

CHÚ THÍCH: tổ chức có thể là một cá nhân

2.39

Hệ thống thông tin (information system)

Là tập hợp các ứng dụng, dịch vụ, tài sản công nghệ thông tin hoặc các thành phần xử lý thông tin khác.

2.40

Tính toàn vẹn (integrity)

Đặc tính về độ chính xác và đầy đủ.

2.41

Bên quan tâm (interested party)

Cá nhân hoặc *tổ chức* (2.57) có thể ảnh hưởng hoặc bị ảnh hưởng bởi, hoặc tự nhận thấy bị ảnh hưởng bởi một quyết định hoặc hành động.

2.42

Ngữ cảnh bên trong (internal context)

Môi trường nội bộ, trong đó tổ chức tìm cách đạt được mục tiêu của mình.

[TCVN 9788:2013]

CHÚ THÍCH: Ngữ cảnh bên trong có thể bao gồm:

- Quản lý, cơ cấu tổ chức, các vai trò và trách nhiệm giải trình;
- Chính sách, mục tiêu và các chiến lược được đưa ra để đạt được chúng;
- Năng lực, được hiểu là tài nguyên và kiến thức (ví dụ như vốn, thời gian, con người, quy trình, hệ thống và công nghệ);
- Hệ thống thông tin, các luồng thông tin và các quy trình ra quyết định (cả chính thức và không chính thức);
- Mối quan hệ, nhận thức và giá trị của các bên liên quan trong nội bộ;
- Văn hóa của tổ chức;
- Các tiêu chuẩn, hướng dẫn và các mô hình được chấp nhận bởi tổ chức;
- Hình thức và mức độ của các mối quan hệ hợp đồng.

2.43

Dự án ISMS (ISMS project)

Các hoạt động có trình tự được thực hiện bởi một *tổ chức* (2.57) để thực thi một hệ thống ISMS.

2.44

Mức rủi ro (level of risk)

Mức độ nghiêm trọng của một *rủi ro* (2.68) thể hiện bằng sự kết hợp của *hậu quả* (2.15) và *khả năng xảy ra* (2.40) của rủi ro.

[TCVN 9788:2013, đoạn "hoặc kết hợp các rủi ro" đã bị xoá bỏ.]

2.45

Khả năng xảy ra (likelihood)

Cơ hội xảy ra một điều gì đó.

[TCVN 9788:2013]

2.46

Hệ thống quản lý (management system)

Tập hợp các phần tử có tương quan hoặc tác động lẫn nhau trong một *tổ chức* (2.57) để thiết lập *chính sách* (2.60), *mục tiêu (*2.56) và *quy trình* (2.61) để đạt được mục tiêu của tổ chức.

CHÚ THÍCH 1: Một hệ thống quản lý có thể có một hoặc một vài quy tắc.

CHÚ THÍCH 2: Các thành phần hệ thống gồm cơ cấu tổ chức, vai trò và trách nhiệm, kế hoạch, vận hành...

CHÚ THÍCH 3: Phạm vi của một hệ thống quản lý có thể bao gồm toàn bộ tổ chức, một số chức năng cụ thể và đã được xác định của tổ chức, một số phần cụ thể và đã được xác định của tổ chức hoặc một hay vài chức năng qua một nhóm của tổ chức.

2.47

Số đo (measure)

Biến số dùng để gán một giá trị có được từ kết quả của một *phép đo* (2,48).

[ISO/IEC 15939:2007]

CHÚ THÍCH: Thuật ngữ "số đo" được dùng để chỉ chung các số đo cơ bản, số đo dẫn xuất và chỉ báo.

2.48

Phép đo (measurement)

Quy trình (2.61) để nhận biết một giá trị.

CHÚ THÍCH: Trong bối cảnh *an toàn thông tin* (2.33) quy trình để nhận biết một giá trị yêu cầu các thông tin về tính *hiệu quả* (2.24) của một *hệ thống quản lý an toàn thông tin* (2.46) và các biện pháp kiểm soát (2.16) có liên quan, sử dụng một *phương pháp đo lường* (2.50), một *hàm đo lường* (2.49), một *mô hình phân tích* (2.2) và các *tiêu chí quyết định* (2.21).

2.49

Chức năng đo lường (measurement function)

Thuật toán hoặc tính toán thực hiện để kết hợp hai hoặc nhiều *số đo cơ bản* (2.10)

[ISO/IEC 15939:2007]

2.50

Phương pháp đo lường (measurement method)

Trình tự logic của các hoạt động, được mô tả một cách tổng quát, được sử dụng để định lượng một *thuộc tính* (2.4) xét theo một *thang đo* (2.80) cụ thể.

[ISO/IEC 15939:2007]

CHÚ THÍCH: Loại của phương pháp đo lường phụ thuộc vào bản chất của các hoạt động được sử dụng để định lượng một thuộc tính. Có thể phân biệt hai loại:

- Chủ quan: định lượng liên quan đến sự phán xét của con người;

- Khách quan: định lượng dựa trên nguyên tắc các con số.

2.51

Kết quả đo lường (measurement results)

Một hoặc nhiều *chỉ báo* (2.30) và các giải thích liên quan của chúng nhằm giải quyết một *nhu cầu thông tin* (2.31).

2.52

Giám sát (monitoring)

Hoạt động xác định và phát hiện trạng thái của một hệ thống, một *quy trình* (2.61) hoặc một hành động.

CHÚ THÍCH: Để phát hiện tình trạng có thể cần để kiểm tra, giám sát hoặc quan sát chặt chẽ.

2.53

Điểm không phù hợp (nonconformity)

Sự không đáp ứng một *yêu cầu* (2.63)

2.54

Chống chối bỏ (non-repudiation)

Khả năng chứng minh sự xuất hiện của một sự kiện hoặc hành động đã yêu cầu và các thực thể sinh ra chúng.

2.55

Đối tượng (object)

Thành phần đặc trưng qua *phép đo* (2.48) của *thuộc tính* (2.4) của nó.

2.56

Mục tiêu (objective)

Kết quả cần đạt được

CHÚ THÍCH 1: Mục tiêu có thể là chiến lược, chiến thuật hoặc sự vận hành.

CHÚ THÍCH 2: Mục tiêu có thể liên quan đến nhiều quy tắc khác nhau (như mục đích tài chính, sức khoẻ, an toàn và môi trường) và có thể áp dụng các mức khác nhau (như chiến lược, toàn bộ tổ chức, dự án và quy trình (2.61).

CHÚ THÍCH 3: Mục tiêu có thể được thể hiện theo các các khác như kết quả của một dự định, một mục đích, một tiêu chí vận hành, một mục tiêu an toàn thông tin hoặc bằng việc sử dụng các từ với nghĩa tương tự (như mục đích, mục tiêu, đích).

CHÚ THÍCH 4: Trong bối cảnh của hệ thống quản lý an toàn thông tin, mục tiêu an toàn thông tin được thiết lập bởi tổ chức, phù hợp với chính sách an toàn thông tin để đạt được các kết quả cụ thể.

2.57

Tổ chức (organization)

Cá nhân hoặc một nhóm người có chức năng riêng với trách nhiệm, quyền hạn và mối quan hệ để đạt được các mục tiêu đề ra (2.56).

CHÚ THÍCH: Khái niệm tổ chức bao gồm nhưng không giới hạn đến: doanh nghiệp tư nhân, công ty, tập đoàn, hãng, doanh nghiệp, cơ quan, quan hệ đối tác, tổ chức từ thiện, hoặc phần hoặc sự kết hợp của các thành phần, bất kể là có hay không có sự hợp nhất, công hoặc tư.

2.58

Thuê ngoài (outsource)

Tạo một sự sắp xếp mà một *tổ chức* (2.57) bên ngoài thực hiện một phần chức năng hoặc *quy trình* (2.61) của tổ chức.

CHÚ THÍCH: Một tổ chức bên ngoài là nằm ngoài phạm vi của *hệ thống quản lý* (2.46), mặc dù chức năng hoặc quá trình thuê ngoài nằm trong phạm vi.

2.59

Hiệu năng (performance)

Kết quả của phép đo

CHÚ THÍCH 1: Hiệu năng có thể liên quan đến kết quả định lượng hay định tính.

CHÚ THÍCH 2: Hiệu năng có thể liên quan đến việc quản lý các hoạt động, *quy trình* (2.61), sản phẩm (bao gồm các dịch vụ), các hệ thống hoặc các *tổ chức* (2.57).

2.60

Chính sách (policy)

Mục đích và định hướng của một *tổ chức* (2.57) được thể hiện chính thức bởi *ban quản lý cấp cao* (2.84).

2.61

Quy trình (process)

Tập các hoạt động tương tác hoặc có liên quan nhằm biến đổi đầu vào thành đầu ra.

2.62

Tính tin cậy (reliability)

Đặc tính của hành vi và kết quả mong đợi có tính nhất quán.

2.63

Yêu cầu (requirement)

Nhu cầu hay mong muốn đã được quy định, thường là ngụ ý hoặc bắt buộc.

CHÚ THÍCH 1: "thường là ngụ ý" có nghĩa là theo thông lệ hay tục lệ của tổ chức hay các bên quan tâm thì nhu cầu hoặc mong muốn đang xem xét là bắt buộc.

CHÚ THÍCH 2: Một yêu cầu cụ thể là yêu cầu được tuyên bố, ví dụ trong thông tin được lập tài liệu.

2.64

Rủi ro tồn đọng (residual risk)

Rủi ro (2.68) còn lại sau khi *xử lý rủi ro* (2.79).

CHÚ THÍCH 1: Rủi ro tồn đọng có thể gồm cả rủi ro không xác định.

CHÚ THÍCH 2: Rủi ro tồn đọng cũng có thể coi là "rủi ro được giữ lại".

2.65

Soát xét (review)

Hoạt động được thực hiện để xác định tính phù hợp, sự thích đáng và *hiệu quả* (2.24) của chủ thể đối tượng nhằm đạt được mục tiêu đã thiết lập.

2.66

Đối tượng soát xét (review object)

Thành phần cụ thể đang được soát xét.

2.67

Mục tiêu soát xét (review objective)

Tuyên bố mô tả những gì phải đạt được trong kết quả của việc soát xét.

2.68

Rủi ro (risk)

Tác động của sự không chắc chắn lên các mục tiêu.

[TCVN 9788:2013]

CHÚ THÍCH 1: Tác động là sự chênh lệch so với dự kiến - có thể là dương hoặc âm.

CHÚ THÍCH 2: Sự không chắc chắn là tình trạng, thậm chí là một phần, thiếu hụt thông tin liên quan tới việc hiểu hoặc nhận thức về một *sự kiện* (2.25), *hậu quả* (2.14) của sự kiện đó hoặc *khả năng xảy ra* (2.45).

CHÚ THÍCH 3: Rủi ro thường được đặc trưng bởi các tham chiếu đến các *sự kiện* (2.25) và *hậu quả* (2.14) có thể có, hoặc là sự kết hợp của chúng.

CHÚ THÍCH 4: Rủi ro an toàn thông tin thường được thể hiện bằng sự kết hợp của các *hậu quả* (2.14) của một sự kiện (bao gồm cả những thay đổi về hoàn cảnh) và *khả năng xảy ra* (2.45) kèm theo.

CHÚ THÍCH 5: Trong bối cảnh của các hệ thống quản lý an toàn thông tin, các rủi ro an toàn thông tin có thể được thể hiện như ảnh hưởng không chắc chắn lên các mục tiêu an toàn thông tin.

CHÚ THÍCH 6: Rủi ro an toàn thông tin có liên quan đến khả năng phát sinh *mối đe dọa* (2.83) khai thác *điểm yếu* (2.89) của một tài sản thông tin hoặc một nhóm các tài sản thông tin và do đó gây ra thiệt hại cho tổ chức.

2.69

Chấp nhận rủi ro (risk acceptance)

Quyết định có hiểu biết về việc đối mặt với một *rủi ro* (2.68) cụ thể.

[TCVN 9788:2013]

CHÚ THÍCH 1: Chấp nhận rủi ro có thể xảy ra mà không cần *xử lý rủi ro* (2.79) hoặc xảy ra trong quá trình xử lý rủi ro.

CHÚ THÍCH 2: Rủi ro được chấp nhận là đối tượng của việc *giám sát* (2.52) và *soát xét* (2.65).

2.70

Phân tích rủi ro (risk analysis)

Quy trình nhằm tìm hiểu bản chất của *rủi ro* (2.68) và để xác định *mức rủi ro* (2.44)

[TCVN 9788:2013]

CHÚ THÍCH 1: Phân tích rủi ro cung cấp cơ sở cho việc *đánh giá rủi ro* (2.74) và quyết định về cách *xử lý rủi ro* (2.79).

CHÚ THÍCH 2: Phân tích rủi ro bao gồm việc dự đoán rủi ro.

2.71

Đánh giá rủi ro (risk assessment)

Quy trình (2.61) tổng thể về việc *nhận biết rủi ro* (2.75), *phân tích rủi ro* (2.70) và *đánh giá rủi ro* (2.74).

[TCVN 9788:2013]

2.72

Tư vấn và truyền thông rủi ro (risk communication and consultation)

Các quy trình liên tục và lặp lại mà tổ chức cần thực hiện để cung cấp, chia sẻ hoặc có được thông tin và tham gia vào đối thoại với các *bên liên quan* (2.82) trong việc *quản lý rủi ro* (2.68)

CHÚ THÍCH 1: Thông tin có thể liên quan đến sự tồn tại, bản chất, hình thức, khả năng xảy ra, tầm quan trọng, ước lượng, chấp nhận và xử lý rủi ro.

CHÚ THÍCH 2: Tư vấn là một quy trình hai chiều trao đổi thông tin giữa tổ chức và các bên liên quan về một vấn đề trước khi đưa ra quyết định hoặc xác định một hướng đi về vấn đề đó. Tư vấn là:

- Một quy trình có tác động đến việc ra quyết định thông qua ảnh hưởng chứ không phải là qua ép buộc;

- Một đầu vào để đưa ra quyết định, không tham gia vào việc ra quyết định.

2.73

Tiêu chí rủi ro (risk criteria)

Điều tham chiếu, qua đó để ước lượng tầm quan trọng của *rủi ro* (2.68).

[TCVN 9788:2013]

CHÚ THÍCH 1: Tiêu chí rủi ro được dựa trên các mục tiêu của tổ chức, ngữ cảnh bên ngoài và bên trong.

CHÚ THÍCH 2: Tiêu chí rủi ro có thể được bắt nguồn từ tiêu chuẩn, luật pháp, chính sách và các yêu cầu khác.

2.74

Đánh giá rủi ro (risk evaluation)

Quy trình (2.61) so sánh các kết quả *phân tích rủi ro* (2.70) với các *tiêu chí rủi ro* (2.73) để xác định xem *rủi ro* (2.68) và / hoặc tầm cỡ của nó là có thể chấp nhận được hay bỏ qua được hay không.

[TCVN 9788:2013]

CHÚ THÍCH: Ước lượng rủi ro hỗ trợ trong việc ra quyết định về việc *xử lý rủi ro* (2.79).

2.75

Nhận biết rủi ro (risk identification)

Quy trình tìm kiếm, nhận biết và mô tả *rủi ro* (2.68).

[TCVN 9788:2013]

CHÚ THÍCH 1: Nhận biết rủi ro liên quan đến việc xác định các nguồn rủi ro, các sự kiện, nguyên nhân gây ra chúng, hậu quả tiềm ẩn của chúng.

CHÚ THÍCH 2: Nhận biết rủi ro có thể liên quan đến dữ liệu lịch sử, phân tích lý thuyết, sự hiểu biết và các ý kiến chuyên gia, nhu cầu của các bên liên quan.

2.76

Quản lý rủi ro (risk management)

Các hoạt động phối hợp để định hướng và biện pháp kiểm soát một *tổ chức* (2.57) về mặt *rủi ro* (2.68).

[TCVN 9788:2013]

2.77

Quy trình quản lý rủi ro (risk management process)

Việc ứng dụng một cách hệ thống các chính sách quản lý, các thủ tục và thực hành trong các hoạt động truyền thông, tư vấn, thiết lập ngữ cảnh, xác định, phân tích, ước lượng, xử lý, giám sát và soát xét *rủi ro* (2.68).

[TCVN 9788:2013]

CHÚ THÍCH 1: TCVN 10295 sử dụng thuật ngữ "quy trình" để mô tả việc quản lý rủi ro nói chung. Các phần tử trong quy trình quản lý rủi ro được gọi là "các hoạt động".

2.78

Chủ thể rủi ro (risk owner)

Cá nhân hoặc thực thể có trách nhiệm và quyền hạn quản lý một *rủi ro* (2.68).

[TCVN 9788:2013]

2.79

Xử lý rủi ro (risk treatment)

Quy trình (2.61) để sửa đổi *rủi ro* (2.68).

[TCVN 9788:2013]

CHÚ THÍCH 1: Xử lý rủi ro có thể bao gồm:

- Tránh rủi ro bằng cách quyết định không bắt đầu hoặc tiếp tục các hoạt động làm phát sinh rủi ro;

- Bám theo hoặc làm tăng rủi ro để nắm bắt cơ hội;

- Loại bỏ các nguồn rủi ro;

- Thay đổi khả năng xảy ra;

- Thay đổi hậu quả;

- Chia sẻ rủi ro với một bên hoặc các bên khác (bao gồm các hợp đồng và tài chính rủi ro); và

- Duy trì các rủi ro bằng cách lựa chọn với sự hiểu biết.

CHÚ THÍCH 2: Cách xử lý rủi ro để đối phó với hậu quả tiêu cực đôi khi được gọi là "giảm bớt rủi ro", "loại bỏ rủi ro", "phòng ngừa rủi ro" và "giảm thiểu rủi ro".

CHÚ THÍCH 3: Xử lý rủi ro có thể tạo ra những rủi ro mới hoặc sửa đổi những rủi ro hiện tại.

2.80

Thang đo (scale)

Tập hợp có thứ tự các giá trị, có thể là liên tục hoặc rời rạc, hoặc một tập hợp các phân loại giá trị có ánh xạ đến các *thuộc tính* (2.4).

[ISO/IEC 15939:2007]

CHÚ THÍCH 1: Các loại thang đo phụ thuộc vào bản chất của mối quan hệ giữa các giá trị trên thang đo. Bốn loại thang đo thường được định nghĩa:

- Danh mục: Các giá trị đo lường được phân loại;

- Thứ tự: Các giá trị đo được xếp hạng;

- Khoảng thời gian: Các giá trị đo lường có khoảng cách bằng nhau tương ứng với số lượng bằng nhau của thuộc tính;

- Tỷ lệ: Các giá trị đo lường có khoảng cách bằng nhau tương ứng với số lượng bằng nhau của thuộc tính, trong đó giá trị bằng không tương ứng với không có thuộc tính.

Đây chỉ là một số ví dụ về các loại thang đo.

2.81

Tiêu chuẩn thực thi an toàn (security implementation standard)

Tài liệu xác định những cách thức được phép để thực thi an toàn.

2.82

Bên liên quan (stakeholder)

Cá nhân hoặc tổ chức có thể gây ảnh hưởng, chịu ảnh hưởng hoặc tự cảm thấy bị ảnh hưởng bởi một quyết định hoặc hoạt động.

[TCVN 9788:2013]

2.83

Mối đe dọa (threat)

Nguyên nhân tiềm ẩn của một sự cố không mong muốn, có thể gây tổn hại đến hệ thống hay tổ chức.

2.84

Ban quản lý cấp cao (top management)

Cá nhân hoặc nhóm người mà định hướng và biện pháp kiểm soát một *tổ chức* (2.57) ở mức cao nhất.

CHÚ THÍCH 1: Ban quản lý cấp cao có quyền để uỷ quyền đại diện và cung cấp nguồn lực trong tổ chức

CHÚ THÍCH 2: Nếu phạm vi của *hệ thống quản lý* (2.46) chỉ bao gồm một phần của *tổ chức* (2.57) thì Ban quản lý cấp cao được đề cập tới là những người định hướng và kiểm soát một phần của các *tổ chức* (2.57).

2.85

Thực thể thông tin truyền thông tin cậy (trusted information communication entity)

Tổ chức độc lập hỗ trợ trao đổi thông tin trong một cộng đồng chia sẻ thông tin.

2.86

Đơn vị đo lường (unit of measurement)

Số lượng cụ thể, được xác định và áp dụng theo quy ước, được so sánh với số lượng khác cùng loại để thể hiện tầm quan trọng liên quan của chúng đến số lượng đó.

[ISO/IEC 15939:2007]

2.87

Kiểm tra tính hợp lệ (validation)

Xác nhận, thông qua cung cấp các bằng chứng khách quan, về việc các yêu cầu cho việc sử dụng hoặc áp dụng dự kiến cụ thể đã được đáp ứng.

[ISO 9000:2008]

2.88

Sự xác minh (verification)

Xác nhận, thông qua cung cấp các bằng chứng khách quan, về việc các yêu cầu cụ thể đã được đáp ứng.

[ISO 9000:2008]

CHÚ THÍCH 1: Thuật ngữ này cũng có thể được gọi là kiểm thử tuân thủ.

2.89

Điểm yếu (vulnerability)

Yếu điểm của một tài sản hoặc *biện pháp kiểm soát* (2.16) dẫn đến việc có thể bị khai thác bởi một hoặc nhiều *mối đe dọa* (2.83).

3 Hệ thống quản lý an toàn thông tin

3.1 Giới thiệu

Các tổ chức thuộc các loại hình và quy mô đều có các nhiệm vụ:

a) thu thập, xử lý, lưu trữ và truyền tải thông tin;

b) nhận thức được rằng những thông tin đó, các quy trình liên quan, các hệ thống, mạng lưới và con người đều là những tài sản quan trọng để đạt được mục tiêu của tổ chức;

c) phải đối mặt với một loạt các rủi ro có thể ảnh hưởng đến hoạt động của tài sản; và

d) giải quyết các rủi ro nhận biết được thông qua việc triển khai biện pháp kiểm soát an toàn thông tin.

Tất cả các thông tin được sắp xếp và xử lý bởi một tổ chức đều là mục tiêu cho các mối đe dọa tấn công, lỗi phát sinh, phá hoại của tự nhiên (ví dụ như lụt, hoả hoạn)... và các điểm yếu vốn có trong việc sử dụng nó. Khái niệm an toàn thông tin thường được dựa trên việc coi thông tin là một tài sản có giá trị cần được bảo vệ thích đáng, ví dụ, chống lại sự mất mát về tính sẵn sàng, tính bảo mật và tính toàn vẹn. Việc sẵn sàng cung cấp thông tin chính xác và đầy đủ một cách kịp thời đáp ứng nhu cầu hợp pháp là một chất xúc tác cho hiệu quả của hoạt động nghiệp vụ kinh doanh.

Bảo vệ tài sản thông tin thông qua việc xác định, thực hiện, duy trì và cải thiện hiệu quả an toàn thông tin là cần thiết cho phép một tổ chức đạt được mục tiêu của mình cũng như duy trì và nâng cao hình ảnh và tính tuân thủ luật pháp của tổ chức. Các hoạt động phối hợp định hướng cho việc triển khai các biện pháp kiểm soát thích hợp, xử lý các rủi ro an toàn thông tin không thể chấp nhận được thường được xem là các thành phần cơ bản của quản lý an toàn thông tin.

Do những rủi ro an toàn thông tin và hiệu quả của các biện pháp kiểm soát thay đổi phụ thuộc vào hoàn cảnh thay đổi, các tổ chức cần phải:

a) giám sát và đánh giá hiệu quả của các biện pháp kiểm soát và các thủ tục đã được triển khai;

b) xác định những rủi ro mới xuất hiện cần được xử lý;

c) lựa chọn, thực thi và cải thiện các biện pháp kiểm soát thích hợp khi cần thiết.

Để tương tác với nhau và phối hợp các hoạt động an toàn thông tin như vậy, mỗi tổ chức cần phải xây dựng chính sách và mục tiêu an toàn thông tin của mình và đạt được những mục tiêu đó một cách hiệu quả bằng cách sử dụng một hệ thống quản lý.

3.2 ISMS là gì ?

3.2.1 Tổng quan và nguyên tắc

Hệ thống quản lý an toàn thông tin (ISMS) bao gồm các chính sách, thủ tục, hướng dẫn và các nguồn lực và các hoạt động liên quan, được quản lý chung bởi một tổ chức, trong việc theo đuổi bảo vệ tài sản thông tin của mình. Một ISMS là một cách tiếp cận có hệ thống để thiết lập, thực hiện, vận hành, giám sát, soát xét, duy trì và cải thiện an toàn thông tin của tổ chức để đạt được mục tiêu nghiệp vụ. Cách tiếp cận này dựa trên đánh giá rủi ro và mức chấp nhận rủi ro được thiết kế để xử lý và quản lý rủi ro có hiệu quả. Việc phân tích các yêu cầu về bảo vệ tài sản thông tin và áp dụng các biện pháp kiểm soát thích hợp để đảm bảo việc bảo vệ các tài sản thông tin theo yêu cầu sẽ góp phần vào việc thực hiện thành công một hệ thống ISMS. Các nguyên tắc cơ bản sau đây cũng góp phần vào việc thực hiện thành công một hệ thống ISMS:

a) nhận thức về sự cần thiết của an toàn thông tin;

b) phân công trách nhiệm đảm bảo an toàn thông tin;

c) kết hợp cam kết quản lý và lợi ích của các bên liên quan;

d) nâng cao giá trị xã hội;

e) việc đánh giá rủi ro quyết định các biện pháp kiểm soát thích hợp để đạt được mức độ chấp nhận rủi ro;

f) hợp tác về an ninh như một yếu tố thiết yếu của mạng lưới thông tin và hệ thống;

g) Ngăn chặn và phát hiện một cách tích cực các sự cố an toàn thông tin;

h) đảm bảo một cách tiếp cận toàn diện để quản lý an toàn thông tin; và

i) đánh giá lại liên tục an toàn thông tin và thực hiện các sửa đổi cho phù hợp.

3.2.2 Thông tin

Thông tin là một tài sản, giống như các tài sản nghiệp vụ quan trọng khác, là điều cần thiết cho nghiệp vụ của tổ chức và do đó cần được bảo vệ thích hợp. Thông tin có thể được lưu trữ dưới nhiều hình thức, bao gồm: hình thức kỹ thuật số (ví dụ như tập tin dữ liệu được lưu trữ trên phương tiện lưu trữ điện tử hoặc quang học), hình thức vật chất (ví dụ như trên giấy). Thông tin có thể được truyền bằng các phương tiện khác nhau bao gồm: chuyển phát nhanh, giao tiếp điện tử hoặc bằng lời nói. Bất cứ hình thức mang thông tin nào hoặc các phương tiện mà thông tin được truyền đi, thông tin luôn luôn cần được bảo vệ thích hợp.

Trong nhiều tổ chức thông tin phụ thuộc vào công nghệ thông tin và truyền thông. Công nghệ này thường là một yếu tố thiết yếu trong tổ chức và hỗ trợ thúc đẩy việc tạo ra, xử lý, lưu trữ, truyền tải, bảo vệ và phá hủy thông tin.

3.2.3 An toàn thông tin

An toàn thông tin bao gồm 3 khía cạnh chính: Tính bí mật, tính sẵn sàng và tính toàn vẹn. An toàn thông tin liên quan đến việc áp dụng và quản lý các biện pháp an ninh thích hợp có liên quan đến việc xem xét các mối đe dọa, với mục tiêu đảm bảo kinh doanh bền vững thành công, duy trì liên tục và giảm thiểu tác động của các sự cố an toàn thông tin.

An toàn thông tin đạt được thông qua việc thực hiện một tập các biện pháp kiểm soát, được lựa chọn thông qua các quy trình quản lý rủi ro đã chọn và được quản lý qua một hệ thống ISMS, bao gồm các chính sách, quy trình, thủ tục, cơ cấu tổ chức, phần mềm và phần cứng để bảo vệ tài sản thông tin đã xác định. Các biện pháp kiểm soát này cần phải được xác định, thực hiện, giám sát, soát xét và cải thiện khi cần thiết, để đảm bảo rằng an toàn thông tin và các mục tiêu kinh doanh cụ thể của tổ chức được đáp ứng. Các biện pháp kiểm soát an toàn thông tin liên quan dự kiến sẽ được tích hợp nhuần nhuyễn với các quy trình kinh doanh của tổ chức.

3.2.4 Quản lý

Quản lý liên quan đến các hoạt động chỉ đạo, biện pháp kiểm soát và cải tiến liên tục tổ chức trong các cơ cấu tương ứng. Hoạt động quản lý bao gồm hành động, cách thức, hay thực hành tổ chức, xử lý, chỉ đạo, giám sát và kiểm soát các nguồn tài nguyên. Cơ cấu quản lý mở rộng từ một người trong một tổ chức nhỏ đến phân cấp quản lý bao gồm nhiều cá nhân trong một tổ chức lớn.

Trong khái niệm một hệ thống ISMS, quản lý liên quan đến việc giám sát và ra các quyết định cần thiết để đạt được mục tiêu kinh doanh thông qua việc bảo vệ tài sản thông tin của tổ chức. Quản lý an toàn thông tin được thể hiện qua việc xây dựng và áp dụng các chính sách, thủ tục, hướng dẫn an toàn thông tin và áp dụng trong toàn bộ tổ chức bởi tất cả các cá nhân liên quan trong tổ chức.

3.2.5 Hệ thống quản lý

Một hệ thống quản lý sử dụng một bộ khung các nguồn lực để đạt được mục tiêu của tổ chức. Hệ thống quản lý bao gồm cơ cấu tổ chức, chính sách, lập kế hoạch, trách nhiệm, thực hành, các thủ tục, quy trình và nguồn lực.

Trong phạm vi an toàn thông tin, hệ thống quản lý cho phép một tổ chức thực thi:

a) đáp ứng các yêu cầu an toàn thông tin của khách hàng và các bên liên quan khác;

b) cải thiện các kế hoạch và hoạt động của một tổ chức;

c) đáp ứng các mục tiêu an toàn thông tin của tổ chức;

d) tuân thủ các quy định, pháp luật và các yêu cầu bắt buộc của lĩnh vực;

e) quản lý tài sản thông tin một cách có tổ chức tạo điều kiện cải thiện liên tục và điều chỉnh các mục tiêu tổ chức hiện hành.

3.3 Cách tiếp cận quy trình

Các tổ chức cần phải xác định và quản lý nhiều hoạt động để thực hiện chức năng hiệu quả và hữu hiệu. Mọi hoạt động có sử dụng tài nguyên cần phải được quản lý để cho phép việc chuyển đổi đầu vào thành đầu ra sử dụng một tập hợp các hoạt động có liên quan hay có tương tác - Đây được xem như một quy trình. Kết quả của một quy trình có thể trực tiếp tạo thành đầu vào cho quy trình khác và thường việc chuyển đổi này được thực hiện trong điều kiện có kế hoạch và có kiểm soát. Việc áp dụng một hệ thống các quy trình trong tổ chức, cùng với sự nhận biết và tương tác giữa các quy trình và việc quản lý chúng có thể được gọi là một "cách thức tiếp cận quy trình".

3.4 Tại sao ISMS lại quan trọng

Rủi ro liên quan đến tài sản thông tin của một tổ chức cần phải được giải quyết. Đạt được an toàn thông tin đòi hỏi phải quản lý rủi ro, bao gồm rủi ro từ các mối đe dọa liên quan về vật lý, con người và công nghệ đối với tất cả các hình thức thông tin trong tổ chức hoặc được sử dụng bởi tổ chức.

Việc áp dụng một hệ thống ISMS được trông đợi là một quyết định chiến lược cho một tổ chức và điều cần thiết là quyết định này được tích hợp nhuần nhuyễn, có mở rộng và cập nhật phù hợp với nhu cầu của tổ chức.

Việc thiết kế và thực hiện hệ thống ISMS của một tổ chức bị ảnh hưởng bởi nhu cầu và mục tiêu của tổ chức, các yêu cầu an ninh, các quy trình kinh doanh được áp dụng, quy mô và cấu trúc của tổ chức. Thiết kế và hoạt động của một hệ thống ISMS cần phản ánh lợi ích và yêu cầu an toàn thông tin của tất cả các bên liên quan đến tổ chức bao gồm khách hàng, nhà cung cấp, các đối tác kinh doanh, các cổ đông và các bên thứ ba khác có liên quan.

Trong một thế giới kết nối với nhau, thông tin và các quy trình liên quan, các hệ thống và mạng lưới là các tài sản kinh doanh quan trọng. Tổ chức và các hệ thống thông tin cũng như mạng lưới của họ phải đối mặt với các mối đe dọa an ninh từ một loạt các nguồn khác nhau, bao gồm gian lận máy tính, hoạt động gián điệp, phá hoại, hỏa hoạn và lũ lụt. Thiệt hại cho hệ thống thông tin và mạng lưới gây ra bởi mã độc hại, tin tặc máy tính và tấn công từ chối dịch vụ đã trở nên phổ biến hơn, với nhiều tham vọng hơn và ngày càng tinh vi hơn.

Hệ thống ISMS quan trọng cho các hoạt động nghiệp vụ cả khu vực công và tư. Trong bất cứ ngành nào, hệ thống ISMS tạo động lực hỗ trợ thương mại điện tử và rất cần thiết cho các hoạt động quản lý rủi ro. Việc kết nối các mạng công cộng và tư nhân, chia sẻ tài sản thông tin càng làm tăng khó khăn trong việc kiểm soát truy cập thông tin và xử lý thông tin. Ngoài ra, việc phân tán các thiết bị lưu trữ di động có chứa tài sản thông tin có thể làm giảm hiệu quả của các biện pháp kiểm soát truyền thống. Khi tổ chức áp dụng hệ thống tiêu chuẩn ISMS, họ có khả năng thể hiện việc áp dụng một cách nhất quán các nguyên tắc an toàn thông tin phù hợp tương ứng cho các đối tác kinh doanh và các bên liên quan khác.

An toàn thông tin thường không phải lúc nào cũng được tính đến khi thiết kế và phát triển hệ thống thông tin. Mặt khác, an toàn thông tin thường chỉ được coi như là một giải pháp kỹ thuật. Tuy nhiên, an toàn thông tin đạt được thông qua các phương tiện kỹ thuật có những hạn chế và có thể không có hiệu quả nếu không được hỗ trợ bởi quản lý và các thủ tục phù hợp trong khuôn khổ một hệ thống ISMS. Tích hợp an ninh vào một hệ thống thông tin sau khi đã triển khai thực tế có thể rất cồng kềnh và tốn kém. Một hệ thống ISMS liên quan đến việc xác định các biện pháp kiểm soát nào được đưa ra và yêu cầu cần lập kế hoạch cặn kẽ, chi tiết. Ví dụ, kiểm soát truy cập có thể về mặt kỹ thuật (logic), vật lý, hành chính (quản lý) hoặc kết hợp giữa chúng, sẽ cung cấp một phương tiện để đảm bảo quyền truy cập vào tài sản thông tin được hợp pháp và có giới hạn dựa trên các yêu cầu nghiệp vụ và an toàn thông tin.

Việc áp dụng thành công một hệ thống ISMS là điều quan trọng để bảo vệ tài sản thông tin cho phép một tổ chức:

a) đảm bảo rằng thông tin của mình được bảo vệ đầy đủ chống lại các mối đe dọa liên tục;

b) duy trì một bộ khung tổng thể, có cấu trúc để xác định và đánh giá rủi ro an toàn thông tin, lựa chọn và áp dụng các biện pháp kiểm soát khả dụng, đo lường và cải thiện hiệu quả của chúng;

c) liên tục cải thiện môi trường kiểm soát;

d) tuân thủ pháp luật và các quy định một cách hiệu quả.

3.5 Thiết lập, giám sát, duy trì và cải thiện một hệ thống ISMS

3.5.1 Tổng quan

Một tổ chức cần thực hiện các bước sau đây trong việc xây dựng, giám sát, duy trì và cải thiện hệ thống ISMS:

a) xác định tài sản thông tin và yêu cầu an toàn thông tin liên quan (xem 3.5.2);

b) đánh giá rủi ro an toàn thông tin (xem 3.5.3) và xử lý rủi ro an toàn thông tin (xem 3.5.4);

c) lựa chọn và thực hiện các biện pháp kiểm soát liên quan đến quản lý rủi ro không thể chấp nhận (xem 3.5.5);

d) giám sát, duy trì và nâng cao hiệu quả các biện pháp kiểm soát tài sản thông tin của tổ chức (xem 3.5.6).

Để đảm bảo hệ thống ISMS hoạt động hiệu quả trong việc bảo vệ tài sản thông tin của tổ chức trên cơ sở liên tục, cần thực hiện các bước (a) - (d) lặp đi lặp lại để xác định những thay đổi trong rủi ro hoặc trong chiến lược của tổ chức, mục tiêu kinh doanh.

3.5.2 Xác định các yêu cầu an toàn thông tin

Trong chiến lược kinh doanh và mục tiêu chung của tổ chức, quy mô hoạt động, không gian địa lý và các yêu cầu an toàn thông tin có thể được xác định thông qua:

a) tài sản thông tin xác định và giá trị của chúng;

b) nhu cầu kinh doanh để xử lý thông tin, lưu trữ và truyền thông;

c) yêu cầu pháp lý, quy định và hợp đồng.

Việc thực hiện phương pháp đánh giá rủi ro gắn với tài sản thông tin của một tổ chức liên quan đến thực hiện phân tích: các mối đe dọa đến tài sản thông tin, các điểm yếu và khả năng xảy ra mối đe dọa cụ thể tới các tài sản thông tin, tác động tiềm năng của bất kỳ sự cố an toàn thông tin nào về tài sản thông tin. Chi phí cho các biện pháp kiểm soát tương ứng dự kiến sẽ tỷ lệ thuận với tác động có thể thấy được vào hoạt động kinh doanh của rủi ro.

3.5.3 Đánh giá các rủi ro an toàn thông tin

Quản lý rủi ro an toàn thông tin đòi hỏi phải đánh giá nguy cơ và có phương pháp xử lý rủi ro thích hợp, có thể bao gồm một dự toán chi phí và lợi ích, các yêu cầu pháp lý, mối quan tâm của các bên liên quan, các đầu vào và các biến thích hợp khác.

Đánh giá rủi ro cần xác định, định lượng và đặt mức ưu tiên cho các rủi ro theo các tiêu chí chấp nhận rủi ro và các mục tiêu có liên quan đến tổ chức. Kết quả sẽ hướng dẫn và xác định hành động quản lý phù hợp và mức ưu tiên cho việc quản lý rủi ro an toàn thông tin và thực thi biện pháp kiểm soát được lựa chọn để bảo vệ chống lại những rủi ro.

Đánh giá rủi ro phải bao gồm các phương pháp tiếp cận có hệ thống ước tính mức độ rủi ro (phân tích rủi ro) và quy trình so sánh rủi ro ước tính theo các tiêu chí rủi ro để xác định tầm quan trọng của rủi ro (đánh giá rủi ro).

Đánh giá rủi ro phải được thực hiện định kỳ để giải quyết vấn đề thay đổi trong các yêu cầu an toàn thông tin và trong tình huống rủi ro, ví dụ như trong các tài sản, các mối đe dọa, các điểm yếu, tác động, ước lượng rủi ro và khi xảy ra những thay đổi đáng kể. Việc đánh giá rủi ro cần được thực hiện một cách có phương pháp, có khả năng cho ra kết quả so sánh và tái tạo được kết quả.

Đánh giá rủi ro an toàn thông tin nên có một phạm vi xác định rõ ràng để có hiệu quả và nên bao gồm các mối quan hệ với đánh giá rủi ro trong các lĩnh vực khác, nếu thích hợp.

TCVN 10295 cung cấp hướng dẫn quản lý rủi ro an toàn thông tin, bao gồm cả tư vấn về đánh giá rủi ro, xử lý rủi ro, chấp nhận rủi ro, báo cáo rủi ro, giám sát rủi ro và soát xét rủi ro. Ngoài ra còn có các ví dụ về các phương pháp đánh giá rủi ro.

3.5.4 Xử lý các rủi ro an toàn thông tin

Trước khi xem xét xử lý rủi ro, tổ chức nên quyết định tiêu chí để xác định có hay không những rủi ro có thể được chấp nhận. Rủi ro có thể được chấp nhận nếu nó được đánh giá là nguy cơ thấp hoặc chi phí xử lý không hiệu quả. Quyết định này nên được ghi lại.

Đối với mỗi rủi ro được xác định sau khi đánh giá rủi ro, cần phải đưa ra một quyết định xử lý rủi ro. Tùy chọn có thể cho xử lý rủi ro bao gồm:

a) áp dụng các biện pháp kiểm soát thích hợp để giảm thiểu rủi ro;

b) chấp nhận rủi ro có chủ ý và khách quan, nếu chúng đáp ứng rõ ràng chính sách và tiêu chí của tổ chức đặt ra về chấp nhận rủi ro;

c) tránh rủi ro bằng cách không cho phép những hành động có thể gây ra những rủi ro xảy ra;

d) chia sẻ các rủi ro liên quan đến các bên khác, ví dụ như công ty bảo hiểm hoặc các nhà cung cấp.

Đối với những rủi ro mà các quyết định xử lý rủi ro đã chỉ định việc áp dụng các biện pháp kiểm soát thích hợp, nên lựa chọn và thực hiện các biện pháp kiểm soát này.

3.5.5 Chọn lựa và triển khai các biện pháp kiểm soát

Khi các yêu cầu an toàn thông tin đã được xác định (xem 3.5.2), rủi ro an toàn thông tin cho các tài sản thông tin cụ thể đã được xác định và đánh giá (xem 3.5.3), quyết định xử lý rủi ro an toàn thông tin đã được đưa ra (xem 3.5.4), khi đó việc lựa chọn và thực hiện các biện pháp kiểm soát cho áp dụng để giảm thiểu rủi ro.

Các biện pháp kiểm soát phải đảm bảo rằng rủi ro được giảm đến một mức chấp nhận được có xem xét đến:

a) các yêu cầu và hạn chế của pháp luật và quy định của quốc gia và quốc tế;

b) các mục tiêu tổ chức;

c) các yêu cầu và hạn chế trong hoạt động;

d) chi phí thực hiện và hoạt động liên quan đến rủi ro được giảm và còn lại tỷ lệ thuận với các yêu cầu và hạn chế của tổ chức;

e) nên thực hiện giám sát, đánh giá và nâng cao hiệu quả và hiệu lực của các biện pháp kiểm soát an toàn thông tin nhằm hỗ trợ mục tiêu của tổ chức. Việc lựa chọn và thực hiện biện pháp kiểm soát nên được ghi chép trong một tuyên bố áp dụng nhằm hỗ trợ các yêu cầu tuân thủ.

f) sự cần thiết để cân bằng đầu tư trong việc thực hiện và vận hành các biện pháp kiểm soát với sự mất mát có thể là kết quả của sự cố an toàn thông tin.

Các biện pháp kiểm soát được trình bày trong tiêu chuẩn TCVN ISO/IEC 27002 được coi là thực hành tốt nhất cho hầu hết các tổ chức và dễ dàng thiết kế riêng để phù hợp với các quy mô và độ phức tạp khác nhau của các tổ chức. Các tiêu chuẩn khác trong hệ thống tiêu chuẩn ISMS đưa ra hướng dẫn về việc lựa chọn và áp dụng các biện pháp kiểm soát trong tiêu chuẩn TCVN ISO/IEC 27002 cho hệ thống quản lý an toàn thông tin.

Các biện pháp kiểm soát an toàn thông tin cần được xem xét ngay trong giai đoạn thiết kế và đặc tả các yêu cầu hệ thống và yêu cầu dự án. Nếu không làm như vậy có thể dẫn đến thêm chi phí và các giải pháp kém hiệu quả và có thể, trong trường hợp xấu nhất, không có khả năng để đạt được an ninh đầy đủ. Các biện pháp kiểm soát có thể được lựa chọn từ TCVN ISO/IEC 27002 hoặc từ các tập kiểm

soát khác hoặc các biện pháp kiểm soát mới có thể được thiết kế để đáp ứng các nhu cầu cụ thể của tổ chức. Cần nhận ra rằng một số biện pháp kiểm soát có thể không áp dụng đối với mọi hệ thống thông tin, môi trường và có thể không khả thi cho tất cả các tổ chức.

Đôi khi phải mất thời gian để thực hiện thiết lập một chọn lựa về các biện pháp kiểm soát và trong khoảng thời gian đó mức rủi ro có thể cao hơn mức chịu đựng được trên cơ sở dài hạn. Tiêu chí rủi ro nên gồm khả năng chịu lỗi của rủi ro trên cơ sở ngắn hạn trong khi các biện pháp kiểm soát đang được triển khai. Các bên quan tâm nên được thông báo về mức rủi ro được ước lượng hoặc dự kiến tại các thời điểm khác nhau khi các biện pháp triển khai được tăng lên.

Cần lưu ý rằng không có một tập các biện pháp kiểm soát nào có thể đạt được an toàn thông tin đầy đủ. Hoạt động quản lý bổ sung nên được thực hiện để giám sát, đánh giá và nâng cao hiệu quả và hiệu lực của các biện pháp kiểm soát an toàn thông tin nhằm hỗ trợ mục tiêu của tổ chức.

Việc lựa chọn và thực hiện biện pháp kiểm soát nên được ghi chép trong một tuyên bố áp dụng nhằm hỗ trợ các yêu cầu tuân thủ.

3.5.6 Giám sát, duy trì và cải thiện hiệu quả của hệ thống ISMS

Một tổ chức cần duy trì và cải thiện hệ thống ISMS thông qua giám sát và đánh giá năng lực về các chính sách và mục tiêu của tổ chức và báo cáo kết quả với nhà quản lý để xem xét. Việc soát xét ISMS này sẽ kiểm tra xem hệ thống ISMS có bao gồm các biện pháp kiểm soát đặc thù thích hợp để xử lý rủi ro trong phạm vi hệ thống ISMS hay không. Ngoài ra, dựa trên các bản ghi về khu vực giám sát, sẽ có bằng chứng thẩm tra và theo vết các hành động khắc phục, phòng ngừa và cải thiện.

3.5.7 Cải thiện liên tục

Mục đích của việc cải thiện liên tục một ISMS là để tăng khả năng đạt được các mục tiêu liên quan tới duy trì tính bí mật, tính sẵn sàng và tính toàn vẹn của thông tin. Trọng tâm của việc cải thiện liên tục là tìm kiếm cơ hội để cải thiện và không giả định rằng các hoạt động quản lý hiện tại là đủ tốt hoặc tốt như hệ thống có thể.

Các hành động cải thiện bao gồm:

a) phân tích và đánh giá các tình huống hiện tại để xác định các vùng cần cải thiện;

b) thiết lập các mục tiêu cải thiện;

c) tìm kiếm các giải pháp có thể để đạt được các mục tiêu;

d) đánh giá các giải pháp hiện tại và thực hiện một lựa chọn;

e) triển khai các giải pháp được lựa chọn;

f) đo lường, xác minh, phân tích và đánh giá các kết quả triển khai để xác định rằng các mục tiêu đã được đáp ứng;

g) chính thức hoá các thay đổi;

Kết quả được soát xét là cần thiết để xác định các cơ hội để cải thiện. Bằng cách này, cải thiện là một hoạt động liên tục, có nghĩa là: các hành động được lặp lại thường xuyên. Phản hồi từ khách hàng và các bên quan tâm khác, đánh giá và soát xét hệ thống quản lý an toàn thông tin cũng có thể được sử dụng để xác định các cơ hội cải thiện.

3.6 Các yếu tố quan trọng quyết định thành công của ISMS

Có khá nhiều yếu tố quan trọng cho việc thực hiện thành công một hệ thống ISMS cho phép đáp ứng các mục tiêu kinh doanh của tổ chức. Ví dụ về các yếu tố thành công quan trọng bao gồm:

a) chính sách an toàn thông tin, mục tiêu và các hoạt động phù hợp với mục tiêu;

b) cách thức tiếp cận và bộ khung cho việc thiết kế, thực hiện, giám sát, bảo trì và cải thiện an toàn thông tin phù hợp với văn hóa doanh nghiệp;

c) hỗ trợ và cam kết rõ ràng từ tất cả các cấp quản lý, đặc biệt là từ cấp quản lý cao nhất;

d) hiểu biết về nhu cầu bảo vệ tài sản thông tin đạt được thông qua việc áp dụng quản lý rủi ro an toàn thông tin (xem TCVN 10295);

e) một chương trình nâng cao nhận thức và giáo dục đào tạo an toàn thông tin hiệu quả, thông báo cho tất cả nhân viên và các bên liên quan khác về nghĩa vụ an toàn thông tin của họ đã được xác định trong các chính sách an toàn thông tin, tiêu chuẩn... và động viên họ để có hành động phù hợp;

f) một quy trình quản lý sự cố an toàn thông tin hiệu quả;

g) một cách thức tiếp cận quản lý duy trì liên tục kinh doanh hiệu quả;

h) một hệ thống đo lường được sử dụng để ước lượng hiệu suất trong quản lý an toàn thông tin và ý kiến phản hồi để cải thiện.

Một hệ thống ISMS làm tăng khả năng cho tổ chức luôn đạt được những yếu tố thành công quan trọng cần thiết để bảo vệ tài sản thông tin của mình.

3.7 Lợi ích của họ tiêu chuẩn ISMS

Lợi ích của việc thực hiện một hệ thống ISMS chủ yếu là kết quả của việc giảm thiểu rủi ro an toàn thông tin (tức là giảm khả năng và /hoặc tác động gây ra bởi sự cố an toàn thông tin). Đặc biệt, lợi ích thực tế cho một tổ chức để đạt được thành công bền vững từ việc áp dụng hệ thống tiêu chuẩn ISMS bao gồm:

a) một bộ khung có cấu trúc hỗ trợ quy trình xác định, thực hiện, vận hành và duy trì một hệ thống ISMS toàn diện, hiệu quả, có giá trị, được tích hợp và sắp xếp nhằm đáp ứng nhu cầu của tổ chức trong các hoạt động và tại các địa điểm khác nhau;

b) hỗ trợ nhà quản lý trong việc quản lý thống nhất và hoạt động một cách có trách nhiệm hướng về quản lý an toàn thông tin, trong ngữ cảnh quản lý rủi ro và quản trị doanh nghiệp, bao gồm cả giáo dục đào tạo cho chủ sở hữu hệ thống về quản lý an toàn thông tin toàn diện;

c) thúc đẩy việc chấp nhận toàn cầu về thực hành an toàn thông tin hữu hiệu theo cách không chính tắc, cho phép các tổ chức cơ hội áp dụng và cải thiện các biện pháp kiểm soát liên quan phù hợp với hoàn cảnh cụ thể của họ và để duy trì chúng khi đối mặt với những thay đổi trong nội bộ và từ bên ngoài;

d) cung cấp một ngôn ngữ chung và nền tảng nhận thức về an toàn thông tin, tạo khả năng thuận lợi để tạo sự tin cậy trong các đối tác kinh doanh với một hệ thống ISMS phù hợp, đặc biệt là khi họ yêu cầu giấy chứng nhận phù hợp tiêu chuẩn TCVN ISO/IEC 27001 bởi một cơ quan chứng nhận được công nhận;

e) tăng sự tin tưởng của các bên liên quan với tổ chức;

f) đáp ứng nhu cầu và kỳ vọng của xã hội;

g) quản lý kinh tế hiệu quả hơn với các khoản đầu tư an toàn thông tin.

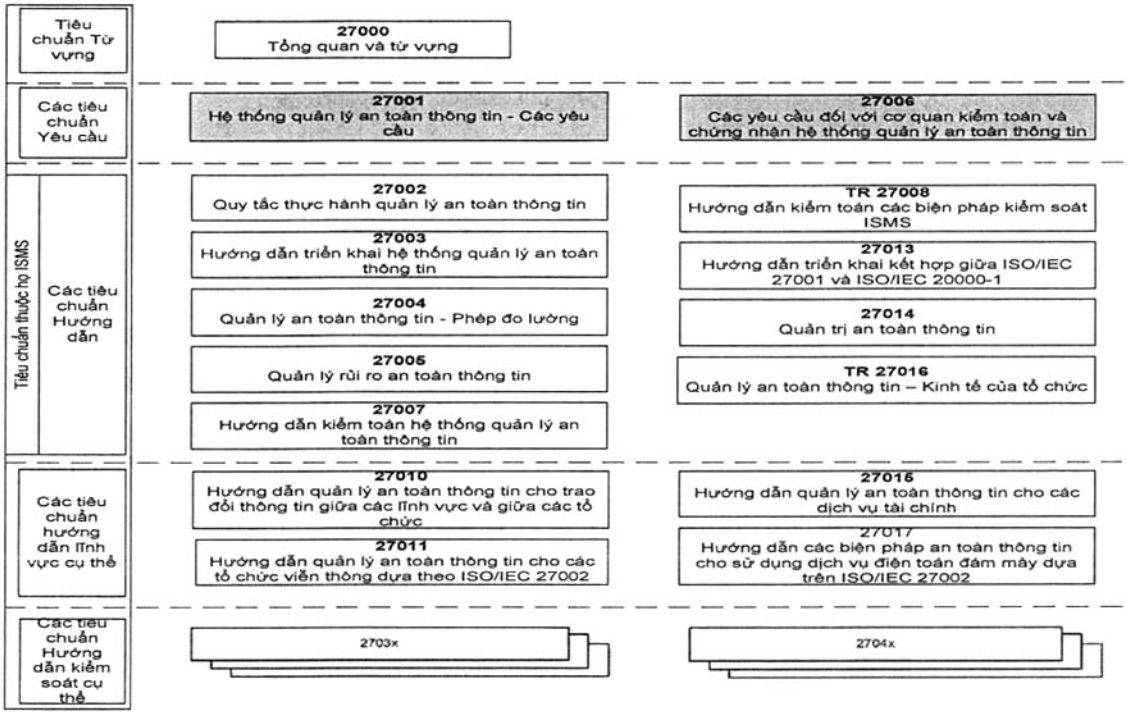
4 Hệ thống tiêu chuẩn ISMS

4.1 Thông tin chung

Họ tiêu chuẩn ISMS bao gồm các tiêu chuẩn liên quan đến nhau, đã được công bố hoặc đang được phát triển, và có chứa một số thành phần cấu trúc quan trọng. Các thành phần này tập trung vào tiêu chuẩn quy định mô tả các yêu cầu hệ thống ISMS (TCVN ISO/IEC 27001) và yêu cầu của cơ quan chứng nhận (ISO/IEC 27006) thực hiện chứng nhận phù hợp với tiêu chuẩn TCVN ISO/IEC 27001. Các tiêu chuẩn khác cung cấp hướng dẫn về các khía cạnh khác nhau khi thực thi một hệ thống ISMS, đề cập một quy trình chung, đưa ra các hướng dẫn liên quan đến biện pháp kiểm soát cũng như hướng dẫn trong các lĩnh vực cụ thể.

Mối quan hệ giữa các tiêu chuẩn ISMS được minh họa trong Hình 1 ([1]).

[1] Trong khi biên soạn tiêu chuẩn này, các tiêu chuẩn ISO/IEC 27007 và 27008 đang được dự thảo



Hình 1 – Mối quan hệ trong hệ thống tiêu chuẩn ISMS

a) Mỗi tiêu chuẩn thuộc họ ISMS được mô tả dưới đây theo kiểu (hoặc vai trò) của tiêu chuẩn đó trong họ tiêu chuẩn ISMS và số tham chiếu của tiêu chuẩn. Các điều áp dụng: các tiêu chuẩn mô tả tổng quan và thuật ngữ (xem 4.2).

b) các tiêu chuẩn xác định các yêu cầu (xem 4.3);

c) các tiêu chuẩn mô tả các hướng dẫn chung (xem 4.4);

d) các tiêu chuẩn mô tả các hướng dẫn cho lĩnh vực cụ thể (xem 4.5).

4.2 Tiêu chuẩn mô tả về tổng quan và từ vựng

4.2.1 TCVN 11238 (ISO/IEC 27000) (tiêu chuẩn này)

Công nghệ thông tin - Các kỹ thuật an toàn - Hệ thống quản lý an toàn thông tin - Tổng quan và từ vựng

Phạm vi: Tiêu chuẩn này cung cấp cho các tổ chức, cá nhân:

a) tổng quan về họ tiêu chuẩn ISMS;

b) giới thiệu về hệ thống quản lý an toàn thông tin (ISMS);

c) thuật ngữ và định nghĩa được sử dụng trong họ tiêu chuẩn ISMS.

Mục tiêu: Tiêu chuẩn TCVN 11238 mô tả các nguyên tắc cơ bản của hệ thống quản lý an toàn thông tin, tạo thành chủ đề của họ tiêu chuẩn ISMS và định nghĩa các thuật ngữ liên quan.

4.3 Các tiêu chuẩn quy định các yêu cầu cụ thể

4.3.1 TCVN ISO/IEC 27001 (ISO/IEC 27001)

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

Phạm vi: Tiêu chuẩn này quy định các yêu cầu cho việc thiết lập, thực hiện, vận hành, giám sát, soát xét, duy trì và cải thiện hệ thống quản lý an toàn thông tin (ISMS) trong ngữ cảnh hoạt động nghiệp vụ tổng thể có rủi ro của tổ chức. Nó xác định các yêu cầu về việc thực hiện các biện pháp kiểm soát an toàn thông tin được tùy chỉnh theo nhu cầu của các tổ chức cụ thể hoặc bộ phận của chúng. Tiêu chuẩn này có thể được sử dụng bởi tất cả các tổ chức, bất kể loại hình, quy mô và tính chất.

Mục tiêu: TCVN ISO/IEC 27001 cung cấp các yêu cầu bắt buộc để phát triển và vận hành một hệ thống ISMS, bao gồm một tập các biện pháp kiểm soát để kiểm soát và giảm thiểu các rủi ro liên quan đến tài sản thông tin mà tổ chức tìm cách bảo vệ thông qua vận hành hệ thống ISMS của mình. Các tổ chức vận hành hệ thống ISMS có thể được đánh giá và chứng nhận về việc tuân thủ. Các mục tiêu kiểm soát và các biện pháp kiểm soát trong Phụ lục A (TCVN ISO/IEC 27001) cần được lựa chọn như là một phần của quy trình ISMS này phải phù hợp để bao quát các yêu cầu đặt ra. Các mục tiêu kiểm soát và biện pháp kiểm soát được liệt kê trong Bảng A.1 (TCVN ISO/IEC 27001) có nguồn gốc trực tiếp và phù hợp với những điều được liệt kê trong tiêu chuẩn TCVN ISO/IEC 27002, Điều 5 đến 18.

4.3.2 ISO/IEC 27006

Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu đối với cơ quan cung cấp đánh giá và chứng nhận hệ thống quản lý an toàn thông tin

Phạm vi: Tiêu chuẩn này quy định các yêu cầu và hướng dẫn cho cơ quan cung cấp đánh giá và chứng nhận ISMS theo tiêu chuẩn TCVN ISO/IEC 27001, ngoài các yêu cầu đã nêu trong ISO / IEC 17021. Nó chủ yếu được dùng để hỗ trợ việc công nhận các cơ quan chứng nhận cung cấp giấy chứng nhận ISMS theo tiêu chuẩn TCVN ISO/IEC 27001.

Mục tiêu: ISO/IEC 27006 bổ trợ cho ISO / IEC 17021 trong việc cung cấp các yêu cầu để tổ chức chứng nhận được công nhận, do đó cho phép các tổ chức này cung cấp chứng nhận tuân thủ nhất quán với các yêu cầu đặt ra trong tiêu chuẩn TCVN ISO/IEC 27001.

4.4 Các tiêu chuẩn mô tả hướng dẫn chung

4.4.1 TCVN ISO/IEC 27002 (ISO/IEC 27002)

Công nghệ thông tin - Các kỹ thuật an toàn - Quy tắc thực hành quản lý an toàn thông tin

Phạm vi: Tiêu chuẩn này cung cấp một danh sách các mục tiêu kiểm soát được chấp nhận rộng rãi và các biện pháp thực hành tốt nhất như là hướng dẫn thực hiện khi lựa chọn và triển khai các biện pháp kiểm soát nhằm đảm bảo an toàn thông tin.

Mục tiêu: TCVN ISO/IEC 27002 đưa ra hướng dẫn về việc thực hiện các biện pháp kiểm soát an toàn thông tin. Cụ thể các Điều 5 đến 18 đưa ra tư vấn triển khai cụ thể và hướng dẫn thực hành tốt nhất để hỗ trợ của các biện pháp kiểm soát quy định tại các điều A.5 đến A.18 của tiêu chuẩn TCVN ISO/IEC 27001.

4.4.2 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

Phạm vi: Tiêu chuẩn này đưa ra hướng dẫn triển khai thực tế và cung cấp thêm thông tin để xác lập, thực hiện, vận hành, giám sát, soát xét, duy trì và cải thiện một hệ thống ISMS theo TCVN ISO/IEC 27001.

Mục tiêu: TCVN 15041 cung cấp một phương pháp tiếp cận theo định hướng quy trình nhằm thực hiện thành công hệ thống ISMS theo TCVN ISO/IEC 27001.

4.4.3 TCVN 10542 (ISO/IEC 27004)

Công nghệ thông tin - Các kỹ thuật an toàn - Quản lý an toàn thông tin - Đo lường

Phạm vi: Tiêu chuẩn này cung cấp hướng dẫn và tư vấn về phát triển và sử dụng các phép đo để đánh giá hiệu lực của hệ thống ISMS, các mục tiêu kiểm soát và các biện pháp kiểm soát được sử dụng để thực hiện và quản lý an toàn thông tin, theo như quy định trong TCVN ISO/IEC 27001.

Mục tiêu: TCVN 10542 cung cấp một bộ khung đo lường cho phép đánh giá hiệu lực của hệ thống ISMS theo TCVN ISO/IEC 27001.

4.4.4 TCVN 10295 (ISO/IEC 27005)

Công nghệ thông tin - Các kỹ thuật an toàn - Quản lý rủi ro an toàn thông tin

Phạm vi: Tiêu chuẩn này cung cấp hướng dẫn quản lý rủi ro an toàn thông tin. Phương pháp tiếp cận mô tả trong tiêu chuẩn này hỗ trợ các khái niệm chung quy định trong TCVN ISO/IEC 27001.

Mục tiêu: TCVN 10295 hướng dẫn triển khai tiếp cận quản lý rủi ro theo định hướng quy trình nhằm hỗ trợ thỏa đáng thực hiện và hoàn thành các yêu cầu về quản lý rủi ro an toàn thông tin của TCVN ISO/IEC 27001.

4.4.5 ISO/IEC 27007

Công nghệ thông tin - Các kỹ thuật an toàn - Hướng dẫn đánh giá hệ thống quản lý an toàn thông tin

Phạm vi: Tiêu chuẩn này cung cấp hướng dẫn về thực hiện đánh giá ISMS, cũng như hướng dẫn về năng lực của các đánh giá viên cho hệ thống quản lý an toàn thông tin, ngoài các hướng dẫn đã có trong TCVN ISO 19011 dành cho hệ thống quản lý nói chung.

Mục tiêu: ISO/IEC 27007 cung cấp hướng dẫn cho các tổ chức cần thực hiện để đánh giá nội bộ hoặc đánh giá độc lập bên ngoài cho hệ thống ISMS hoặc để quản lý một chương trình đánh giá ISMS so với yêu cầu quy định trong TCVN ISO/IEC 27001.

4.4.6 ISO/IEC TR 27008

Công nghệ thông tin - Các kỹ thuật an toàn - Hướng dẫn cho đánh giá viên về các biện pháp kiểm soát an toàn thông tin

Phạm vi: Báo cáo kỹ thuật này cung cấp hướng dẫn về rà soát việc thực hiện và hoạt động của các biện pháp kiểm soát, bao gồm việc kiểm tra tuân thủ kỹ thuật các biện pháp kiểm soát hệ thống thông tin, sự tuân thủ với các tiêu chuẩn an toàn thông tin đã thiết lập trong tổ chức.

Mục tiêu: Báo cáo kỹ thuật này tập trung vào việc rà soát các biện pháp kiểm soát an toàn thông tin, bao gồm cả kiểm tra việc tuân thủ kỹ thuật theo tiêu chuẩn an toàn thông tin đã triển khai trong tổ chức. Tài liệu này không nhằm cung cấp bất kỳ hướng dẫn cụ thể nào về việc kiểm tra tuân thủ liên quan đến đo lường, đánh giá rủi ro hay đánh giá một hệ thống ISMS theo quy định trong ISO/IEC 27004, 27005 hoặc 27007 tương ứng. Báo cáo kỹ thuật này không dành cho đánh giá hệ thống quản lý.

4.4.7 TCVN 9965 (ISO/IEC 27013)

Công nghệ thông tin - Các kỹ thuật an toàn - Hướng dẫn tích hợp triển khai ISO/IEC 27001 và ISO/IEC 20000-1.

Phạm vi: Tiêu chuẩn này cung cấp hướng dẫn về việc kết hợp triển khai ISO / IEC 27001 và ISO / IEC 20000-1 cho các tổ chức có ý định sau đây:

a) triển khai TCVN ISO/IEC 27001 khi đã triển khai ISO/IEC 20000-1 trước đó hoặc ngược lại;

b) triển khai đồng thời cả hai tiêu chuẩn TCVN ISO/IEC 27001 và ISO / IEC 20000-1;

c) đồng bộ các hệ thống quản lý theo TCVN ISO/IEC 27001 và ISO/IEC 20000-1 đã triển khai.

Mục tiêu: Để cung cấp cho các tổ chức thông tin về các đặc điểm tương đồng và khác biệt của tiêu chuẩn TCVN ISO/IEC 27001và ISO / IEC 20000-1 nhằm hỗ trợ lập kế hoạch một hệ thống quản lý tích hợp tuân thủ với cả hai tiêu chuẩn quốc tế.

4.4.8 ISO/IEC 27014

Công nghệ thông tin - Các kỹ thuật an toàn - Quản trị an toàn thông tin

Phạm vi: Tiêu chuẩn này cung cấp hướng dẫn về nguyên tắc, các quy trình quản trị an toàn thông tin, theo đó các tổ chức có thể ước lượng, điều hành và giám sát việc quản lý an toàn thông tin.

Mục tiêu: An toàn thông tin đã trở thành một vấn đề quan trọng cho các tổ chức. Không chỉ có yêu cầu pháp lý tăng mà sự thất bại của các biện pháp an toàn thông tin của một tổ chức có thể có tác động trực tiếp đến uy tín của tổ chức đó. Vì vậy, bộ phận quản trị, với phần trách nhiệm quản lý của họ, đang ngày càng đòi hỏi phải giám sát an toàn thông tin để đảm bảo đạt được các mục tiêu đề ra của tổ chức.

4.4.9 ISO/IEC TR 27016

Công nghệ thông tin - Các kỹ thuật an toàn - Quản lý an toàn thông tin - Kinh tế của tổ chức

Phạm vi: Báo cáo kỹ thuật này cung cấp một phương pháp cho phép các tổ chức hiểu rõ hơn về mặt kinh tế trong việc xác định chính xác hơn giá trị tài sản thông tin cụ thể của họ, giá trị của những rủi ro tiềm tàng đối với tài sản thông tin đó, đánh giá cao những giá trị mà các biện pháp kiểm soát bảo vệ thông tin mang đến cho các tài sản thông tin và xác định mức độ tối ưu các nguồn lực cần được áp dụng cho bảo vệ các tài sản thông tin trên.

Mục tiêu: Báo cáo kỹ thuật này bổ sung cho họ tiêu chuẩn ISMS thông qua cách nhìn từ quan điểm kinh tế trong việc bảo vệ tài sản thông tin của một tổ chức trong môi trường xã hội ngày càng rộng lớn hơn mà tổ chức hoạt động và cung cấp các hướng dẫn về cách áp dụng kinh tế của tổ chức an toàn thông tin thông qua sử dụng các mô hình và ví dụ.

4.5 Các tiêu chuẩn mô tả hướng dẫn theo lĩnh vực cụ thể

4.5.1 TCVN 10543 (ISO/IEC 27010)

Công nghệ thông tin - Các kỹ thuật an toàn - Quản lý an toàn trao đổi thông tin liên tổ chức, liên ngành.

Phạm vi: Tiêu chuẩn này cung cấp hướng dẫn ngoài các hướng dẫn đã được đưa ra trong họ tiêu chuẩn ISO/IEC 27000 để thực hiện quản lý an toàn thông tin trong các cộng đồng chia sẻ thông tin, cung cấp thêm các biện pháp kiểm soát và hướng dẫn cụ thể liên quan đến khởi tạo, triển khai, duy trì và cải thiện an toàn thông tin trong truyền thông tin giữa các lĩnh vực và giữa các tổ chức.

Mục tiêu: Tiêu chuẩn này được áp dụng cho tất cả các hình thức trao đổi và chia sẻ thông tin nhạy cảm, cho cả lĩnh vực công cộng và tư nhân, trong nước và quốc tế, cho các lĩnh vực sản xuất/kinh doanh tương tự hoặc giữa các lĩnh vực. Đặc biệt, nó có thể áp dụng để trao đổi và chia sẻ thông tin liên quan đến việc cung cấp, duy trì và bảo vệ một tổ chức hoặc cơ sở hạ tầng quan trọng của quốc gia.

4.5.2 ISO/IEC 27011

Công nghệ thông tin - Các kỹ thuật an toàn - Hướng dẫn quản lý an toàn thông tin cho các tổ chức viễn thông dựa theo TCVN ISO/IEC 27002

Phạm vi: Tiêu chuẩn này cung cấp hướng dẫn hỗ trợ thực hiện quản lý an toàn thông tin trong các tổ chức viễn thông.

Mục tiêu: ISO/IEC 27011 cung cấp cho các tổ chức viễn thông với một bản gồm các hướng dẫn tương thích với TCVN ISO/IEC 27002, dành riêng cho lĩnh vực viễn thông bao gồm các hướng dẫn bổ sung nhằm hoàn thiện các yêu cầu đã nêu trong TCVN ISO/IEC 27001, Phụ lục A.

4.5.3 ISO/IEC TR 27015

Công nghệ thông tin - Các kỹ thuật an toàn - Hướng dẫn quản lý an toàn thông tin cho các dịch vụ tài chính

Phạm vi: Báo cáo kỹ thuật này cung cấp hướng dẫn bổ sung cho các hướng dẫn đã được đưa ra trong họ tiêu chuẩn ISO / IEC 27000 để khởi tạo, triển khai, duy trì và cải thiện an toàn thông tin trong các tổ chức cung cấp dịch vụ tài chính.

Mục tiêu: Báo cáo kỹ thuật này là một bản bổ sung đặc biệt cho TCVN ISO/IEC 27001 và TCVN ISO/IEC 27002 dùng cho các tổ chức cung cấp dịch vụ tài chính để hỗ trợ trong công tác:

a) Khởi tạo, triển khai, duy trì và cải thiện một hệ thống quản lý an toàn thông tin dựa theo TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005).

b) Thiết kế và thực hiện các biện pháp kiểm soát theo quy định trong TCVN ISO/IEC 27002:2011 (ISO/IEC 27002:2005) hoặc trong tiêu chuẩn này.

4.5.4 ISO/IEC 27799

Tin học y tế - Quản lý an toàn thông tin trong lĩnh vực y tế sử dụng TCVN ISO/IEC 27002

Phạm vi: Tiêu chuẩn này cung cấp hướng dẫn hỗ trợ thực hiện quản lý an toàn thông tin trong các tổ chức y tế.

Mục tiêu: ISO / IEC 27799 cung cấp cho các tổ chức y tế một bản hướng dẫn thực hiện tiêu chuẩn ISO / IEC 27002 dùng riêng cho lĩnh vực này, bổ sung cho các hướng dẫn đã được đưa ra nhằm đáp ứng các yêu cầu trong TCVN ISO/IEC 27001, Phụ lục A.

Phụ lục A
(Tham khảo)
Các từ ngữ diễn tả quy định

Mỗi tài liệu trong họ tiêu chuẩn ISMS không tự nó áp đặt bất cứ ai thực hiện nó. Tuy nhiên, có thể áp đặt việc bắt buộc áp dụng, ví dụ thông qua văn bản pháp luật hoặc hợp đồng. Để có thể yêu cầu tuân thủ theo một tài liệu, người sử dụng cần có khả năng xác định các yêu cầu cần thiết cần được thỏa mãn. Người sử dụng cũng cần có khả năng phân biệt các yêu cầu này so với các khuyến nghị khác, trong đó có các khả năng tự do lựa chọn nhất định.

Bảng dưới đây làm rõ việc một tài liệu trong họ tiêu chuẩn ISMS phải được diễn giải như thế nào đối với các từ ngữ diễn tả hoặc là các yêu cầu hoặc là các khuyến nghị.

Bảng này được dựa trên các quy định của Chỉ thị ISO/IEC, Phần 2, *Quy tắc về cấu trúc và soạn thảo các tiêu chuẩn quốc tế*, Phụ lục H.

CHỈ DẪN	GIẢI THÍCH
Yêu cầu	Các cụm từ "phải" và "không phải" biểu thị các yêu cầu cần phải tuân theo chặt chẽ để đảm bảo tuân thủ với tài liệu và không cho phép sai lệch.
Khuyến nghị	Các cụm từ "nên" và "không nên" biểu thị rằng trong các khả năng có thể, có một khả năng được khuyến nghị là phù hợp hơn, mà không đề cập đến hoặc loại trừ các khả năng khác, hoặc biểu thị một chu trình hành động nhất định nào đó cần được ưu tiên song không cần thiết phải là bắt buộc, hoặc biểu thị (theo nghĩa phủ định) một khả năng hay một chu trình hành động nhất định nào đó bị phản đối nhưng không phải là bị ngăn cấm.
Cho phép	Các cụm từ "có thể" và "không cần" biểu thị một chu trình hành động được phép trong phạm vi tài liệu.
Khả năng	Các cụm từ "có khả năng" và "không có khả năng" biểu thị khả năng một điều gì đó xảy ra.

Phụ lục B
(Tham khảo)
Thuật ngữ và chủ sở hữu thuật ngữ

B.1 Chủ sở hữu thuật ngữ

Chủ sở hữu thuật ngữ trong họ tiêu chuẩn ISO/IEC 27000 là tiêu chuẩn đã khởi tạo định nghĩa thuật ngữ. Chủ sở hữu thuật ngữ cũng có trách nhiệm duy trì định nghĩa, nghĩa là:

- cung cấp;
- soát xét;
- cập nhật, và
- gỡ bỏ.

CHÚ THÍCH 1: TCVN ISO/IEC 27001 không bao giờ được xác định như là chủ sở hữu thuật ngữ của chính nó.

CHÚ THÍCH 2: TCVN ISO/IEC 27001 và ISO/IEC 27006 là các tiêu chuẩn quy định (nghĩa là: chứa đựng các yêu cầu) luôn chiếm ưu thế như là chủ sở hữu thuật ngữ tương ứng.

B.2 Thuật ngữ được sắp xếp theo tiêu chuẩn

B.2.1 TCVN ISO/IEC 27001

Đánh giá (Audit)	2.5	Phép đo (Measurement)	2.48
Tính sẵn sàng (Availability)	2.9	Giám sát (Monitoring)	2.52
Năng lực (Competence)	2.11	Điểm không phù hợp (Nonconformity)	2.53
Tính bí mật (Confidentiality)	2.12	Mục tiêu (Objective)	2.56
Sự phù hợp (Conformity)	2.13	Tổ chức (Organization)	2.57
Cải thiện liên tục (Continual improvement)	2.15	Thuê ngoài (Outsource)	2.58
Kiểm soát (Control)	2.16	Hiệu năng (performance)	2.59
Khắc phục (Corrective)	2.18	Chính sách (Policy)	2.60
Hành động khắc phục (Corrective action)	2.19	Quy trình (Process)	2.61
Thông tin được lập tài liệu (documented information)	2.23	Yêu cầu (Requirement)	2.63
Hiệu quả (Effectiveness)	2.24	Soát xét (Review)	2.65
An toàn thông tin (Information security)	2.33	Rủi ro (Risk)	2.68

Tính toàn vẹn (Integrity)	2.40	Chủ thể rủi ro (Risk owner)	2.78
Bên quan tâm (Interested party)	2.41	Ban quản lý cấp cao (Top management)	2.84
Hệ thống quản lý (Management system)	2.46		

B.2.2 TCVN ISO/IE 27002

Biện pháp kiểm soát truy cập (Access control)	2.1	Sự kiện an toàn thông tin (Information security event)	2.35
Tấn công (Attack)	2.3	Sự cố an toàn thông tin (Information security incident)	2.36
Xác thực (Authentication)	2.7	Quản lý sự cố an toàn thông tin (Information security incident management)	2.37
Tính xác thực (Authenticity)	2.8	Hệ thống thông tin (Information system)	2.39
Mục tiêu của biện pháp kiểm soát (Control objective)	2.17	Chống chối bỏ (Non-repudiation)	2.54
Các phương tiện xử lý thông tin (Information processing facilities)	2.32	Tính tin cậy (Reliability)	2.62
Tính liên tục an toàn thông tin (Information security continuity)	2.34		

B.2.3 TCVN 10541

Dự án ISMS (ISMS project)	2.43		

B.2.4 TCVN 10542

Mô hình phân tích (Analytical model)	2.2	Hàm đo lường (Measurement function)	2.49
Thuộc tính (Attribute)	2.4	Phương pháp đo lường (Measurement method)	2.50
Số đo cơ bản (Base measure)	2.10	Kết quả đo lường (Measurement results)	2.51
Dữ liệu (Data)	2.20	Đối tượng (Object)	2.55
Tiêu chí quyết định (Decision criteria)	2.21	Thang đo (Scale)	2.80
Số đo dẫn xuất (Derived measure)	2.22	Đơn vị đo lường (Unit of measurement)	2.86
Chỉ báo (Indicator)	2.30	Kiểm tra tính hợp lệ (Validation)	2.87
Nhu cầu thông tin (Information need)	2.31	Sự xác minh (Verification)	2.88

Số đo (Measure)	2.47

B.2.5 TCVN 10295

Hậu quả (Consequence)	2.14	Tư vấn và truyền thông rủi ro (Risk communication and consultation)	2.72
Sự kiện (Event)	2.25	Tiêu chí rủi ro (Risk criteria)	2.73
Ngữ cảnh bên ngoài (External context)	2.27	Đánh giá rủi ro (Risk evaluation)	2.74
Ngữ cảnh bên trong (Internal context)	2.42	Nhận biết rủi ro (Risk identification)	2.75
Mức rủi ro (Level of risk)	2.44	Quản lý rủi ro (Risk management)	2.76
Khả năng xảy ra (Likelihood)	2.45	Quy trình quản lý rủi ro (Risk management process)	2.77
Rủi ro tồn đọng (Residual risk)	2.64	Xử lý rủi ro (Risk treatment)	2.79
Chấp nhận rủi ro (Risk acceptance)	2.69	Mối đe dọa (Threat)	2.83
Phân tích rủi ro (Risk analysis)	2.70	Điểm yếu (Vulnerability)	2.89
Đánh giá rủi ro (Risk assessment)	2.71		

B.2.6 ISO/IEC 27006

Chứng nhận (Certificate)			
Tổ chức chứng nhận (Certification body)		Dấu (Mark)	
Tài liệu chứng nhận (Certification document)		Tổ chức (Organization)	

B.2.7 ISO/IEC 27007

Phạm vi đánh giá (Audit scope)	2.6

B.2.8 ISO/IEC 27008

Đối tượng soát xét (Review object)	2.66	Chuẩn thực thi an toàn (Security implementation standard)	2.81
Mục tiêu soát xét (Review objective)	2.67		

B.2.9 TCVN 10543

Cộng đồng chia sẻ thông tin (Information sharing community)	2.38	Thực thể thông tin truyền thông tin cậy (Trusted information communication entity)	2.85

B.2.10 ISO/IEC 27011

Kết hợp theo thứ tự (Collocation)	Phương tiện viễn thông (Telecommunications facilities)
Trung tâm truyền thông (Communication centre)	Tổ chức viễn thông (Telecommunications organizations)
Truyền thông cần thiết (Essential communications)	Bản ghi viễn thông (Telecommunication records)
Chống tiết lộ trong truyền thông (Non-disclosure of communications)	Dịch vụ viễn thông (Telecommunications services)
Thông tin cá nhân (Personal information)	Khách hàng dịch vụ viễn thông (Telecommunications service customer)
Cuộc gọi ưu tiên (Priority call)	Người dùng dịch vụ viễn thông (Telecommunications service user)
Ứng dụng viễn thông (Telecommunications applications)	Phương tiện đầu cuối (Terminal facilities)
Nghiệp vụ viễn thông (Telecommunications business)	Người dùng (User)
Phòng thiết bị viễn thông (Telecommunications equipment room)	

B.2.11 ISO/IEC 27014

Bộ phận quản lý thực thi (Exucutive management)	2.26	Cơ quan điều hành (Governing body)	2.29
Quản trị an toàn thông tin (Governance of information security)	2.28	Bên liên quan (Stakeholder)	2.82

B.2.12 ISO/IEC 27015

Các dịch vụ tài chính (Financial services)

B.2.13 ISO/IEC 27016

Tính toán giá trị tổn thất hàng năm (Annulized Loss Expectancy (ALE))	Tổn thất (Loss)
Giá trị trực tiếp (Direct value)	Giá trị thị trường (Market value)

Phép so sánh kinh tế (Economic comparison)

Nhân tố kinh tế (Economic factor)

Biện minh kinh tế (Economic justification)

Giá trị kinh tế gia tăng (Economic value added)

Kinh tế học (Economics)

Giá trị mong đợi (Expected value)

Giá trị mở rộng (Extended value)

Giá trị gián tiếp (Indirect value)

Kinh tế học an toàn thông tin (Information security economics)

Quản lý an toàn thông tin IMS (Information security management IMS)

Giá trị hiện tại thuần (Net present value)

Lợi nhuận phi kinh tế (Non economic benefit)

Giá trị hiện tại (Present value)

Chi phí cơ hội (Opportunity cost)

Giá trị cơ hội (Opportunity value)

Các yêu cầu quản lý (Regulatory requirements)

Tỉ lệ hoàn vốn đầu tư (Return on investment)

Giá trị xã hội (Societal value)

Giá trị (Value)

Quản trị rủi ro (Value-at-risk)

Thư mục tài liệu tham khảo

[1] TCVN ISO/IEC 17021:2011, Đánh giá sự phù hợp - Yêu cầu đối với tổ chức đánh giá và chứng nhận hệ thống quản lý.

[2] ISO 9000:2005, Quality management systems - Fundamentals and vocabulary (Các hệ thống quản lý an toàn thông tin - Tổng quan và từ vựng).

[3] TCVN ISO 19011:2013, Hướng dẫn đánh giá hệ thống quản lý.

[4] TCVN ISO/IEC 27001, Công nghệ thông tin - Hệ thống quản lý an toàn thông tin - Các yêu cầu.

[5] TCVN ISO/IEC 27002, Công nghệ thông tin - Các kỹ thuật an toàn - Quy tắc thực hành quản lý an toàn thông tin.

[6] TCVN 10541:2014, Công nghệ thông tin - Kỹ thuật an toàn - Hướng dẫn triển khai hệ thống quản lý an toàn thông tin.

[7] TCVN 10542:2014, Công nghệ thông tin - Kỹ thuật an toàn - Quản lý an toàn thông tin - Đo lường.

[8] TCVN 10295:2014, Công nghệ thông tin - Kỹ thuật an toàn - Quản lý rủi ro an toàn thông tin.

[9] ISO/IEC 27006:2011, Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems. (Công nghệ thông tin - Các kỹ thuật an toàn - Các yêu cầu đối với cơ quan đánh giá và chứng nhận hệ thống quản lý an toàn thông tin).

[10] ISO/IEC 27007:2011, Information technology - Security techniques - Guidelines for information security management systems auditing (Công nghệ thông tin - Các kỹ thuật an toàn - Hướng dẫn đánh giá hệ thống quản lý an toàn thông tin).

[11] ISO/IEC TR 27008:2011, Information technology - Security techniques Guidelines for auditors on information security controls (Công nghệ thông tin - Các kỹ thuật an toàn - Hướng dẫn cho đánh giá viên về biện pháp kiểm soát hệ thống quản lý an toàn thông tin).

[12] TCVN 10543:2014, Công nghệ thông tin - Kỹ thuật an toàn - Quản lý an toàn trao đổi thông tin liên tổ chức, liên ngành.

[13] ISO/IEC 27011:2008, Information technology - Security techniques - Information security management guidelines for telecommunications organisations based on ISO/IEC 27002 (Công nghệ thông tin - Các kỹ thuật an toàn - Hướng dẫn quản lý an toàn thông tin cho các tổ chức viễn thông dựa trên TCVN ISO 27002).

[14] TCVN 9965:2013, Công nghệ thông tin - Kỹ thuật an toàn - Hướng dẫn tích hợp triển khai TCVN ISO/IEC 27001 và ISO/IEC 20000-1.

[15] ISO/IEC 27014:2013, Information technology - Security techniques - Governance of information security (Công nghệ thông tin - Các kỹ thuật an toàn - Quản lý an toàn thông tin).

[16] ISO/IEC 27015, Information technology - Security techniques - Information security management guidelines for financial services (Công nghệ thông tin - Các kỹ thuật an toàn - Hướng dẫn quản lý an toàn thông tin cho các dịch vụ tài chính)

[17] ISO/IEC TR 27016, Information technology - Security techniques - Information security management - Organizational economics (Công nghệ thông tin - Các kỹ thuật an toàn - Quản lý an toàn thông tin - Kinh tế của tổ chức).

[18] ISO 27799:2008, Health informatics - Information security management in health using ISO/IEC 27002 (Tin học y tế - Quản lý an toàn thông tin trong y tế sử dụng ISO/IEC 27002).

[19] TCVN 9788:2013, Quản lý rủi ro - Từ vựng.

[20] ISO/IEC 15939:2007, Systems and software engineering - Measurement process (Hệ thống và kỹ nghệ phần mềm - quá trình đo).

[21] ISO/IEC 20000-1, Information technology – Service management – Part 1: Service management system requirements (Công nghệ thông tin – Quản lý dịch vụ - Phần 1: Các yêu cầu đối với hệ thống quản lý dịch vụ).