ĐẠI HỌC QUỐC GIA HÀ NỘI

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

PHÙNG THỊ LIÊN

NGHIÊN CỨU TIÊU CHUẨN ISO 27001 VÀ ỨNG DỤNG

LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN

HÀ NỘI - 2016

ĐẠI HỌC QUỐC GIA HÀ NỘI

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

PHÙNG THỊ LIÊN

NGHIÊN CỨU TIÊU CHUẨN ISO 27001 VÀ ỨNG DỤNG

Ngành:	Công nghệ thông tin
Chuyên ngành:	Hệ thống thông tin
Mã số:	60 48 01 04

LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN

NGƯỜI HƯỚNG DẪN KHOA HỌC: PGT.TS. TRỊNH NHẬT TIẾN

HÀ NỘI – 2016

LỜI CAM ĐOAN

Tôi xin cam đoan báo cáo luận văn này được viết bởi tôi dưới sự hướng dẫn của cán bộ hướng dẫn khoa học, thầy giáo, PGS.TS. Trịnh Nhật Tiến. Tất cả các kết quả đạt được trong luận văn là quá trình tìm hiểu, nghiên cứu của riêng tôi. Nội dung trình bày trong luận văn là của cá nhân tôi hoặc là được tổng hợp từ nhiều nguồn tài liệu tham khảo khác đều có xuất xứ rõ ràng và được trích dẫn hợp pháp.

Tôi xin hoàn toàn chịu trách nhiệm và chịu mọi hình thức kỷ luật theo quy định cho lời cam đam của mình.

Hà Nội, ngày 10 thán 05 năm 2016

Người cam đoan

Phùng Thị Liên

LỜI CẢM ƠN

Đầu tiên, tôi xin gửi lời cảm ơn chân thành và sâu sắc nhất tới thầy Trịnh Nhật Tiến – Người đã trực tiếp hướng dẫn nhiệt tình và giúp đỡ tôi, cho tôi cơ hội được tiếp xúc với các tài liệu tham khảo, góp ý cho tôi trong quá trình nghiên cứu để hoàn thành đề tài này.

Tôi cũng muốn bày tỏ lời cảm ơn chân thành tới các thầy cô giáo đã giảng dạy tôi trong suốt thời gian tôi học tại trường như PGS.TS. Hà Quang Thụy, PGS.TS. Đỗ Trung Tuấn, PGS.TS Nguyễn Ngọc Hóa, TS. Phan Xuân Hiếu, TS. Bùi Quang Hưng, TS. Trần Trúc Mai, TS. Võ Đình Hiếu, TS. Nguyễn Văn Vinh cùng các thầy cô giáo khác trong khoa.

Cuối cùng, tôi xin gửi lời cảm ơn sâu sắc tới Bố, Mẹ, Chồng, cùng Con trai tôi và tất cả những người thân trong gia đình, bạn bè và đồng nghiệp tôi. Họ đã luôn ủng hộ tôi với tình yêu thương, luôn động viên và là động lực để tôi vượt qua tất cả những khó khăn trong cuộc sống.

Hà Nội, ngày 10 tháng 5 năm 2016

Học viên thực hiện luận văn

Phùng Thị Liên

MỤC LỤC

LỜI CAM ĐOAN i

LỜI CẢM ƠN ii

DANH MỤC TỪ VIẾT TẮT v

DANH MỤC BẢNG BIỂU vi

DANH MỤC HÌNH VẼ vii

MỞ ĐẦU 1

Chương 1. TRÌNH BÀY TỔNG QUAN VỀ AN TOÀN THÔNG TIN 2

1.1. CÁC KHÁI NIỆM LIÊN QUAN ĐẾN AN TOÀN THÔNG TIN 2

1.2. CÁC NGUY CƠ RỦI RO MẤT AN TOÀN 3

1.3. NHU CẦU CẤP THIẾT CẦN PHẢI XÂY DỰNG MỘT HỆ THỐNG AN TOÀN THÔNG TIN ĐÁP ỨNG TIÊU CHUẨN QUỐC TẾ. 7

Chương 2. TRÌNH BÀY VỀ TIÊU CHUẨN QUỐC TẾ ISO 27001 8

2.1. TỔNG QUAN VỀ TIÊU CHUẨN ISO 27001 8

2.1.1. Giới thiệu họ tiêu chuẩn ISMS 8

2.1.2. Khái niệm ISO 27001 10

2.1.3. Lịch sử phát triển của ISO 27001 11

2.1.4. Tiếp cận quá trình 11

2.1.5. Thiết lập, kiểm soát, duy trì và cải tiến ISMS 12

2.1.6. Phạm vi áp dụng 15

2.2. HỆ THỐNG QUẢN LÝ AN TOÀN THÔNG TIN 15

2.2.1. Thuật ngữ và định nghĩa 15

2.2.2. Bối cảnh của tổ chức 18

2.2.3. Lãnh đạo 19

2.2.4. Hoạch định 20

2.2.5. Hỗ trợ 23

2.2.6. Điều hành 25
2.2.7. Đánh giá kết quả 25
2.2.8. Cải tiến 27
2.2.9. Trình bày về phụ lục A của tiêu chuẩn 28
2.3. Mười lý do để chứng nhận ISO 27001 47
2.4. Thực trạng và triển vọngphát triển ISO 27001 48
2.4.1. Thực trạng triển khai tại Việt Nam 48
2.4.2. Triển vọng phát triển ISO 27001 tại Việt Nam 49
Chương 3. XÂY DỰNG HỆ THỐNG QUẢN LÝ HỆ THỐNG AN TOÀN THÔNG TIN CHO DOANH NGHIỆP 51
3.1. PHÁT BIỂU BÀI TOÁN 51
3.2. XÂY DỰNG CHƯƠNG TRÌNH 51
3.2.1. Phương pháp xác định rủi ro 51
3.2.2. Quản lý tài sản 53
3.2.3. Xác định các nguy cơ và điểm yếu của hệ thống 56
3.2.4. Lựa chọn các mục tiêu kiểm soát 63
3.2.5. Chương trình thử nghiệm 64
KẾT LUẬN 68
A. NHỮNG VẤN ĐỀ GIẢI QUYẾT ĐƯỢC TRONG LUẬN VĂN NÀY 68
B. KIẾN NGHỊ VÀ HƯỚNG NGHIÊN CỨU TRONG TƯƠNG LAI 69

DANH MỤC TỪ VIẾT TẮT

Từ tiếng việt	Từ viết tắt	Từ tiếng Anh
Hệ thống quản lý an toàn thông tin	ISO	International Organization for Standardization
	IEC	International Electrotechnical Commission
Hệ thống quản lý an toàn thông tin	ISMS	Information Security Management System
Công nghệ thông tin	CNTT	Information Technology

DANH MỤC BẢNG BIỂU

Bảng 3.1: Ma trận tính giá trị rủi ro.....53
Bảng 3.2: Đánh giá tài sản về độ bảo mật.....55
Bảng 3.3: Đánh giá tài sản về độ toàn vẹn.....56
Bảng 3.4: Đánh giá tài sản về độ sẵn sàng.....56
Bảng 3.5: Danh sách nguy cơ.....57
Bảng 3.6: Danh sách điểm yếu.....61

DANH MỤC HÌNH VẼ

Hình 1.1: Đặc tính cơ bản của an toàn thông tin 2
Hình 2.1: Họ tiêu chuẩn ISMS 8
Hình 2.2: Lịch sử phát triển của ISO 27001.....11
Hình 3.1: Tài sản 54
Hình 3.2: Các module của hệ thống 64
Hình 3.3: Tài liệu.....65
Hình 3.4: Kiểm soát.....65
Hình 3.5: Nguy cơ 65
Hình 3.6: Điểm yếu 66
Hình 3.7: Đánh giá rủi ro.....66
Hình 3.8: Tuyên bố áp dụng 66

MỞ ĐẦU

Hiện nay, với sự phát triển như nhanh chóng của các lĩnh vực công nghệ, xuất hiện nhiều cuộc tấn công mạng, cuộc tấn công từ hacker, các nguy cơ gây mất an toàn thông tin xảy ra với tần xuất nhiều hơn, nghiêm trọng hơn. Bên cạnh đó các doanh nghiệp trên thế giới nói chung và Việt Nam nói riêng đang phát triển đa dạng các ngành nghề lĩnh vực. Mỗi ngành nghề lĩnh vực đòi hỏi thông tin trong đó cần phải được bảo mật, xác thực và toàn vẹn, vừa giúp cho doanh nghiệp đó phát triển, thông tin được bảo vệ, hạn chế tấn công, vừa giúp cho doanh nghiệp đó có được hình ảnh uy tín cũng như được các bên đối tác đánh giá và tin tưởng khi hợp tác với các doanh nghiệp có được sự bảo vệ thông tin một cách an toàn. Như vậy vấn đề an toàn thông tin lại càng quan trọng và là nhu cầu cấp thiết đối với các doanh nghiệp. Vậy làm thế nào để giúp các doanh nghiệp thực hiện được điều đó. Để trả lời cho câu hỏi này, trong luận văn *"Nghiên cứu tiêu chuẩn ISO 27001 và ứng dụng"* tôi đã nghiên cứu và tìm hiểu cách xây dựng một hệ thống an toàn thông tin cho doanh nghiệp, giúp cho doanh nghiệp quản lý, bảo vệ thông tin của mình một cách an toàn và hiệu quả nhất.

Luận văn của tôi được chia làm 3 chương:

- Chương 1: Trình bày tổng quan về an toàn thông tin. Chương này trình bày về các khái niệm liên quan đến an toàn thông tin, các nguy cơ mất rủi ro mất an toàn.
- Chương 2: Trình bày tiểu chuẩn quốc tế ISO 27001. Chương này trình bày về tổng quan ISO 27001, trình bày chi tiết hệ thống an toàn thông tin và thực trạng triển khai ISO 27001.
- Chương 3: Xây dựng hệ thống quản lý hệ thống an toàn thông tin cho doanh nghiệp**.** Sau quá trình nghiên cứu và tìm hiểu về ISO 27001. Trong chương này tôi xin trình bày về phần mềm quản lý hệ thống an toàn thông tin và xây dựng các chính sách, quy định, quy trình cho doanh nghiệp.

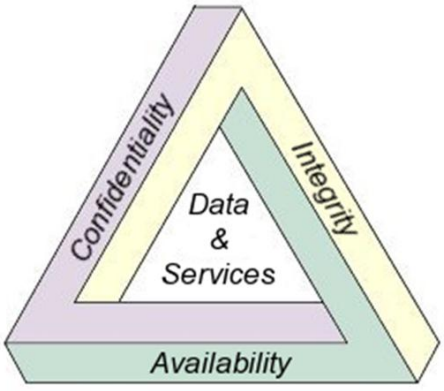
CHƯƠNG 1. TRÌNH BÀY TỔNG QUAN VỀ AN TOÀN THÔNG TIN

1.1. CÁC KHÁI NIỆM LIÊN QUAN ĐẾN AN TOÀN THÔNG TIN

Theo tài liệu ISO 17799 định nghĩa về an toàn thông tin (Information Security) như sau: "*Thông tin là một tài sản quí giá cũng như các loại tài sản khác của các tổ chức cũng như các doanh nghiệp và cần phải được bảo vệ trước vô số các mối đe doạ từ bên ngoài cũng như bên trong nội bộ để bảo đảm cho hệ thống hoạt động liên tục, giảm thiểu các rủi ro và đạt được hiệu suất làm việc cao nhất cũng như hiệu quả trong đầu tư*".

An toàn thông tin bao gồm các hoạt động quản lý, nghiệp vụ và kỹ thuật đối với hệ thống thông tin nhằm bảo vệ, khôi phục các hệ thống, các dịch vụ và nội dung thông tin đối với nguy cơ tự nhiên hoặc do con người gây ra. Việc bảo vệ thông tin, tài sản và con người trong hệ thống thông tin nhằm bảo đảm cho các hệ thống thực hiện đúng chức năng, phục vụ đúng đối tượng một cách sẵn sàng, chính xác và tin cậy. An toàn thông tin bao hàm các nội dung bảo vệ và bảo mật thông tin, an toàn dữ liệu, an toàn máy tính và an toàn mạng.

An toàn thông tin mang nhiều đặc tính, những đặc tính cơ bản của an toàn thông tin bao gồm: Tính bảo mật (Confidentiality), tính toàn vẹn (Integrity) và tính sẵn sàng (Availability). Ba đặc tính này còn được gọi là tam giác bảo mật CIA. Các đặc tính này cũng đúng với mọi tổ chức, không lệ thuộc vào việc chúng chia sẻ thông tin như thế nào.



Hình 1.1: Đặc tính cơ bản của an toàn thông tin

Tính bảo mật: Là tâm điểm chính của mọi giải pháp an ninh cho sản phẩm/hệ thống CNTT. Giải pháp an ninh là tập hợp các quy tắc xác định quyền được truy cập đến thông tin, với một số lượng người sử dụng thông tin nhất định cùng số lượng thông tin nhất định. Trong trường hợp kiểm soát truy cập cục bộ, nhóm người truy cập sẽ được kiểm soát xem là họ đã truy cập những dữ liệu nào và đảm bảo rằng các kiểm soát truy cập có hiệu lực, loại bỏ những truy cập trái phép vào các khu vực là độc quyền của cá

nhân, tổ chức. Tính bảo mật rất cần thiết (nhưng chưa đủ) để duy trì sự riêng tư của người có thông tin được hệ thống lưu giữ.

Tính toàn vẹn: Không bị sửa đổi là đặc tính phức hợp nhất và dễ bị hiểu lầm của thông tin. Đặc tính toàn vẹn được hiểu là chất lượng của thông tin được xác định căn cứ vào độ xác thực khi phản ánh thực tế. Số liệu càng gần với thực tế bao nhiêu thì chất lượng thông tin càng chuẩn bấy nhiêu. Để đảm bảo tính toàn vẹn cần một loạt các biện pháp đồng bộ nhằm hỗ trợ và đảm bảo sự kịp thời và đầy đủ, cũng như sự bảo mật hợp lý cho thông tin.

Tính sẵn sàng: Đảm bảo độ sẵn sàng của thông tin, tức là thông tin có thể được truy xuất bởi những người được phép vào bất cứ khi nào họ muốn. Ví dụ, nếu một server bị ngừng hoạt động hay ngừng cung cấp dịch vụ trong vòng 5 phút trên một năm thì độ sẵn sàng của nó là 99.9999%. Đây là một đặc tính quan trọng, nó là khía cạnh sống còn của an ninh thông tin, đảm bảo cho thông tin đến đúng địa chỉ (người được phép sử dụng) khi có nhu cầu hoặc được yêu cầu. Tính sẵn sàng đảm bảo độ ổn định đáng tin cậy của thông tin, cũng như đảm nhiệm là thước đo, phạm vi tới hạn của một hệ thông tin.

Các tổ chức, doanh nghiệp muốn đảm bảo an toàn thông tin thì luôn cần phải duy trì được sự cân bằng của ba yếu tố trên, ngoài ra các thuộc tính khác như tính xác thực, trách nhiệm giải trình, tính thừa nhận và tính tin cậy cũng có thể liên quan.

1.2. CÁC NGUY CƠ RỦI RO MẤT AN TOÀN

Với sự phát triển của thế giới nói chung và Việt Nam nói riêng, xã hội càng phát triển càng kéo thêm nhiều nguy cơ mất an toàn thông tin. Đặc biệt là vấn đề đe dọa thông tin trên các đường truyền internet, qua máy tính, những chiếc điện thoại thông minh, những thiết bị thông minh khác đều để lại những nguy cơ tiềm ẩn. Tình trạng rất đáng lo ngại trước hành vi thâm nhập vào hệ thống, phá hoại các hệ thống mã hóa, các phần mềm xử lý thông tin tự động gây thiệt hại vô cùng lớn. Sau đây là một số nguy cơ rủi ro mất an toàn thông tin:

Nguy cơ mất an toàn thông tin về khía cạnh vật lý: Nguy cơ mất an toàn thông tin về khía cạnh vật lý là nguy cơ do mất điện, nhiệt độ, độ ẩm không đảm bảo, hỏa hoạn, thiên tai, thiết bị phần cứng bị hư hỏng.

Nguy cơ bị mất, hỏng, sửa đổi nội dung thông tin: Người dùng có thể vô tình để lộ mật khẩu hoặc không thao tác đúng quy trình tạo cơ hội cho kẻ xấu lợi dụng để lấy cắp hoặc làm hỏng thông tin.

Nguy cơ bị tấn công bởi các phần mềm độc hại: Các phần mềm độc hại tấn công bằng nhiều phương pháp khác nhau để xâm nhập vào hệ thống với các mục đích khác

nhau như: Virus, sâu máy tính (Worm), phần mềm gián điệp (Spyware, Trojan, Adware).

Nguy cơ xâm nhập từ lỗ hổng bảo mật: Lỗi do lập trình, lỗi hoặc sự cố phần mềm, nằm trong một hoặc nhiều thành phần tạo nên hệ điều hành hoặc trong chương trình cài đặt trên máy tính.

Nguy cơ xâm nhập do bị tấn công bằng cách phá mật khẩu: Những kẻ tấn công có rất nhiều cách khác phức tạp hơn để tìm mật khẩu truy nhập. Những kẻ tấn công có trình độ đều biết rằng luôn có những khoản mục người dùng quản trị chính.

Nguy cơ mất an toàn thông tin do sử dụng e-mail: Tấn công có chủ đích bằng thư điện tử là tấn công bằng email giả mạo giống như email được gửi người quen, có thể gắn tập tin đính kèm nhằm làm cho thiết bị bị nhiễm virus. Cách thức tấn công này thường nhằm vào một cá nhân hay một tổ chức cụ thể. Thư điện tử đính kèm tập tin chứa virus được gửi từ kẻ mạo danh là một đồng nghiệp hoặc một đối tác nào đó. Người dùng bị tấn công bằng thư điện tử có thể bị đánh cắp mật khẩu hoặc bị lây nhiễm virus.

Nguy cơ mất an toàn thông tin trong quá trình truyền tin: Trong quá trình lưu thông và giao dịch thông tin trên mạng internet nguy cơ mất an toàn thông tin trong quá trình truyền tin là rất cao do kẻ xấu chặn đường truyền và thay đổi hoặc phá hỏng nội dung thông tin rồi gửi tiếp tục đến người nhận.

Mặt khác, ngày nay Internet/Intranet là môi trường tiện lợi cho việc trao đổi thông tin giữa các tổ chức và giữa các cá nhân trong tổ chức với nhau. Các giao dịch trao đổi thư tín điện tử (email), các trao đổi thông tin trực tuyến giữa cơ quan nhà nước và công dân, tìm kiếm thông tin, … thông qua mạng internet không ngừng được mở rộng và ngày càng phát triển.

Bên cạnh các lợi ích mà Internet/Intranet mang lại thì đây cũng chính là môi trường tiềm ẩn các nguy cơ gây mất an toàn an ninh cho các hệ thống mạng của các tổ chức có tham gia giao dịch trên Internet/Intranet. Một vấn đề đặt ra cho các tổ chức là làm sao bảo vệ được các nguồn thông tin dữ liệu như các số liệu trong công tác quản lý hành chính nhà nước, về tài chính kế toán, các số liệu về nguồn nhân lực, các tài liệu về công nghệ, sản phẩm…., trước các mối đe dọa trên mạng Internet hoặc mạng nội bộ có thể làm tổn hại đến sự an toàn thông tin và gây ra những hậu quả nghiêm trọng khó có thể lường trước được.

Hiện nay, cùng với sự phát triển của công nghệ thông tin, các phương thức tấn công cũng ngày càng tinh vi và đa dạng, nó thực sự đe dọa tới sự an toàn của hệ thống thông tin nếu chúng ta không có sự nhận thức đúng đắn về vấn đề này để có những giải pháp hiệu quả để bảo vệ hệ thống của mình.Theo thống kê được từ một số tờ báo của Việt

Nam, thấy được rằng các vụ tấn công mạng vào nước ta không còn lẻ tẻ và quy mô nhỏ nữa, các vụ tấn công đã xảy ra được xác định là có chủ đích, có tổ chức và kế hoạch rõ ràng. Dưới đây là một số thông tin về các vụ tấn công thống kê được từ các trang mạng xã hội:

Chỉ số an toàn thông tin trung bình của Việt Nam là 46,5%, tuy ở dưới mức trung bình và vẫn còn sự cách biệt với các nước như Hàn Quốc (hơn 60%), song so với năm 2014 thì đã có bước tiến rõ rệt (tăng 7,4%)[1].

Theo một báo cáo của Trung tâm ứng cứu khẩn cấp máy tính Việt Nam (VNCERT), tính từ 21/12/2014 tới 21/12/2015, đơn vị này đã ghi nhận được tổng số 31.585 sự cố an ninh thông tin tại Việt Nam. Trong đó, có 5.898 sự cố tấn công lừa đảo, 8.850 sự cố tấn công thay đổi giao diện và 16.837 sự cố cài mã độc.

Con số này lớn hơn khá nhiều so với các sự cố của Việt Nam được ghi nhận trong những năm trước đó. Cụ thể, năm 2010 là 271 sự cố; 2011 là 757 sự cố; 2012 là 2179 sự cố; 2013 là 4.810 sự cố và 2014 là 28.186 sự cố. Tình hình an toàn, an ninh thông tin ở Việt Nam vẫn diễn ra khá phức tạp với các loại hình tấn công mã độc, tấn công có chủ đích APT, lừa đảo qua mạng, qua tin nhắn rác, các mã độc phát tán qua email rác…

Năm 2015 nổi lên tình trạng lừa đảo thông tin qua mạng xã hội. Kẻ xấu luôn luôn tìm cách đưa ra những hình thức, thủ đoạn mới để lừa những người sử dụng nhằm thực hiện hành vi đánh cắp thông tin, thu lợi bất chính.

Sau đó xuất hiện hình thức biến đổi lừa đảo mới khi hacker tạo ra những website giả mạo có giao diện rất giống những website chính thống. Khi người sử dụng thực hiện theo chỉ dẫn trong website để có thể nhân giá trị thẻ cào lên, mã thẻ cào được nhập vào website giả mạo này sẽ bị đánh cắp.

Ngoài xu hướng tấn công trên mạng xã hội, hình thức tấn công thông qua cài mã độc để đánh cắp thông tin với mục đích kinh tế thì mục tiêu chính trị vẫn được ghi nhận xuất hiện nhiều ở Việt Nam trong năm 2015.

Trong tháng 5/2015, hãng bảo mật FireEye đã công bố nhóm tin tặc APT 30 được đặt tại Trung Quốc theo dõi các mục tiêu, trong đó có Việt Nam… Chưa kể đến hàng loạt các cuộc tấn công nhằm vào các doanh nghiệp… Tội phạm thiên về sử dụng mã độc đang gây ra những hậu quả khủng khiếp cho các chính phủ, cá nhân và các hoạt động kinh doanh, đặc biệt là lĩnh vực tài chính. Các mã độc đang gia tăng theo cấp số nhân về cả số lượng, hình thức chủng loại cũng như mức độ đe dọa, gây ra những thiệt hại khó lường.

[1]http://kenh14.vn/bi-quyet-bien-minh-thanh-nhan-su-cao-cap-voi-cntt-20160413235759302.chn

An ninh mạng tại Việt Nam đang trong tình trạng đáng báo động, đòi hỏi các tổ chức và doanh nghiệp phải gấp rút hơn trong việc tìm ra các giải pháp CNTT phù hợp để bảo vệ mình. Thị trường an toàn thông tin quốc gia trong năm 2015 diễn biến khá phức tạp. Tại Việt Nam, cùng với sự phát triển mạnh mẽ ứng dụng công nghệ thông tin, các cuộc tấn công, xâm nhập trái phép vào hệ thống mạng của các cơ quan nhà nước, các tổ chức, doanh nghiệp để phá hoại hoặc thu thập lấy cắp thông tin ngày càng gia tăng. Báo cáo của hãng bảo mật Kaspersky cho biết Việt Nam đứng số 1 thế giới về tỷ lệ lây nhiễm mã độc qua thiết bị lưu trữ ngoài như USB, thẻ nhớ, ổ cứng di động. Theo đó, 70,83% máy tính tại Việt Nam đang bị lây nhiễm mã độc và 39,55% người dùng hiện đang phải đối mặt với mã độc từ Internet. Thống kê trong năm 2015 cho thấy có hơn 10.000 trang, cổng thông tin điện tử sở hữu tên miền .vn bị tấn công, chiếm quyền điều khiển, thay đổi giao diện, cài mã độc, tăng 68% so với năm 2014. Trong số đó, có 224 trang thuộc quản lý của các cơ quan nhà nước, giảm 11% so với năm 2014. Báo cáo cho biết hệ thống trang tin, cổng thông tin điện tử của Việt Nam bị tấn công nhiều nhất trong tháng 6/2015 với số lượng các trang tin bị tấn công lên đến hơn 1.700 trang, trong đó có 56 trang tên miền .gov.vn.[2]

Theo số liệu thống kê về hiện trạng bảo mật mới nhất công bố của Symantec, Việt Nam đứng thứ 11 trên toàn cầu về các hoạt động đe dọa tấn công mạng. Những xu hướng đe dọa bảo mật ngày càng gia tăng nổi bật hiện nay mà các tổ chức tại Việt Nam cần quan tâm là: Tấn công có chủ đích cao cấp, các mối đe dọa trên thiết bị di động, những vụ tấn công độc hại và mất cắp dữ liệu. Thực tế, nguy cơ mất an ninh an toàn mạng máy tính còn có thể phát sinh ngay từ bên trong. Nguy cơ mất an ninh từ bên trong xảy ra thường lớn hơn nhiều, nguyên nhân chính là do người sử dụng có quyền truy nhập hệ thống nắm được điểm yếu của hệ thống hay vô tình tạo cơ hội cho những đối tượng khác xâm nhập hệ thống.[3]

Nguy cơ mất an toàn thông tin do nhiều nguyên nhân, đối tượng tấn công đa dạng. Thiệt hại từ những vụ tấn công mạng là rất lớn, đặc biệt là những thông tin thuộc về kinh tế, an ninh, quốc phòng,và một số nuyên nhân như: Do cơ sở hạ tầng thông tin không đủ mạnh, lỗ hổng bảo mật của phần mềm. Do nhận thức và kiến thức về an toàn thông tin còn yếu và hạn chế. Thiếu chính sách, thủ tục an ninh, an toàn thông tin.

[2] http://vtv.vn/cong-nghe/viet-nam-tro-thanh-muc-tieu-tan-cong-hang-dau-cua-cac-nhom-tin-tac-20160329202117902.htm.
[3] http://voer.edu.vn/c/nghien-cuu-mot-so-giai-phap-bao-dam-an-ninh-mang-thu-nghiem-ap-dung-cho-trung-tam-tich-hop-du-lieu-tinh-tuyen-quang/5ad3fdec

1.3. NHU CẦU CẤP THIẾT CẦN PHẢI XÂY DỰNG MỘT HỆ THỐNG AN TOÀN THÔNG TIN ĐÁP ỨNG TIÊU CHUẨN QUỐC TẾ.

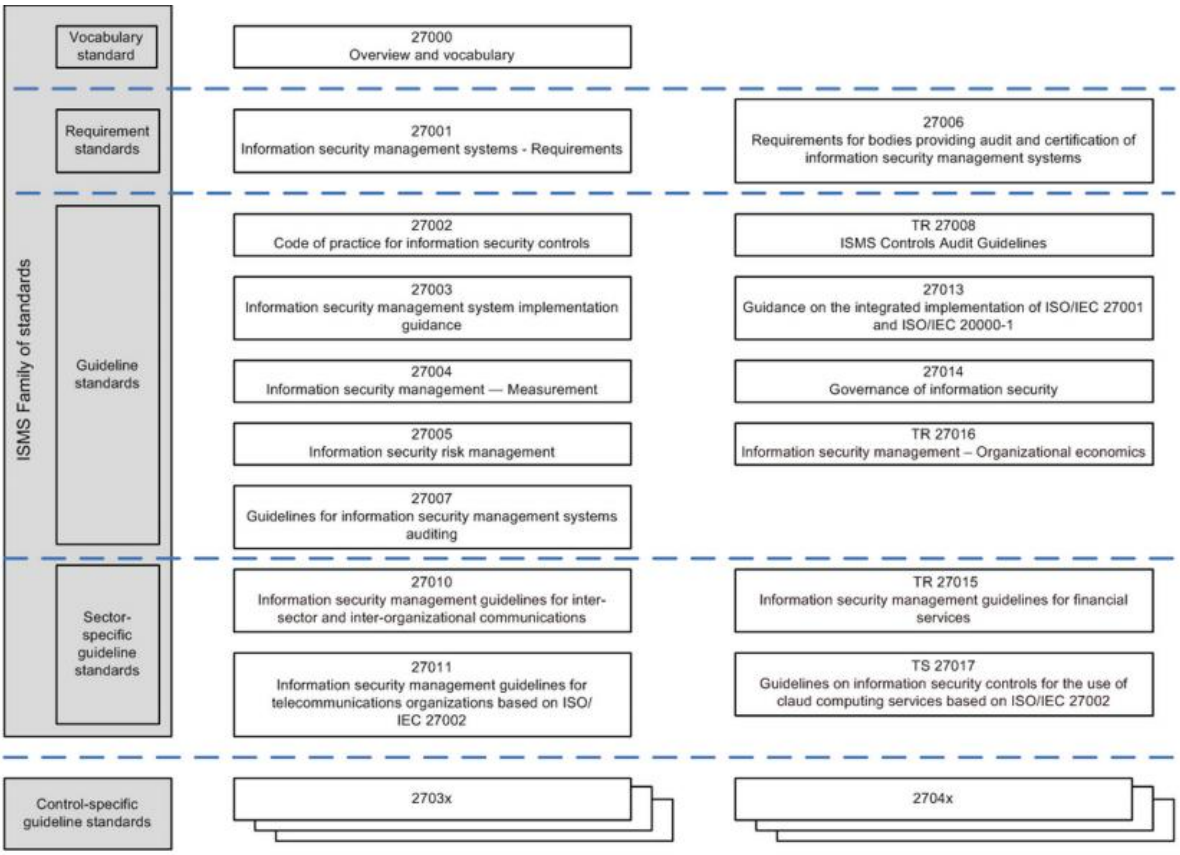
Từ những nguy cơ rủi ro mất an toàn thông tin như trên cho ta thấy, nhu cầu cần thiết phải thiết lập một chính sách an ninh thông tin dựa trên nền tảng một hệ thống quản lý an toàn thông tin (ISMS – Information Security Management System) chuẩn hóa là vô cùng cần thiết. ISO 27001 là một tiêu chuẩn quốc tế có thể đáp ứng nhu cầu này. Nó cung cấp một khuôn khổ, bộ quy tắc cho việc khởi đầu, thiết lập, quản lý và duy trì an ninh thông tin trong tổ chức để thiết lập một nền tảng vững chắc cho chính sách an toàn thông tin, bảo vệ các tài sản của tổ chức, doanh nghiệp một cách thích hợp.

Chương 2. TRÌNH BÀY VỀ TIÊU CHUẨN QUỐC TẾ ISO 27001

2.1. TỔNG QUAN VỀ TIÊU CHUẨN ISO 27001

2.1.1. Giới thiệu họ tiêu chuẩn ISMS

Họ tiêu chuẩn ISMS bao gồm các tiêu chuẩn có mối quan hệ với nhau, đã xuất bản hoặc đang phát triển, và chứa một số thành phần cấu trúc quan trọng. Các thành phần này tập trung chủ yếu vào mô tả các yêu cầu ISMS (ISO/IEC 27001) và tiêu chuẩn dùng để chứng nhận (ISO/IEC 27006) cho sự phù hợp của tiêu chuẩn ISO/IEC 27001 mà tổ chức áp dụng. Các tiêu chuẩn khác cung cấp hướng dẫn cho khía cạnh khác nhau thực thi ISMS, giải quyết một quá trình chung, hướng dẫn kiểm soát liên quan và hướng dẫn cụ thể theo ngành [7].



Hình 2.1: Họ tiêu chuẩn ISMS

- Trong đó tiêu chuẩn ISO/IEC 27000 – Công nghệ thông tin – Các kỹ thuật an toàn – Hệ thống quản lý ATTT – Tổng quan và từ vựng, là tiêu chuẩn mô tả một cái nhìn tổng quan và các thuật ngữ, cung cấp cho tổ chức và các cá nhân:
  - Tổng quan họ tiêu chuẩn ISMS.
  - Giới thiệu về hệ thống an toàn thông tin.
  - Thuật ngữ và định nghĩa đã sử dụng trong các tiêu chuẩn trong bộ tiêu chuẩn ISMS này.
- Những tiêu chuẩn xác định các yêu cầu:

- ISO/IEC 27001: Cung cấp bản quy phạm các yêu cầu cho sự phát triển và hoạt động của ISMS, bao gồm thiết lập điều khiển cho kiểm soát và giảm thiểu các rủi ro liên quan với thông tin tài sản mà tổ chức tìm cách bảo vệ bằng cách điều hành ISMS của nó.
- ISO/IEC 27006: Tiêu chuẩn này đặc tả yêu cầu và cung cấp hướng dẫn đánh giá và chứng chỉ ISMS trong mọi trường hợp với ISO/IEC 27001, thêm vào yêu cầu nêu trong ISO/IEC 17021. Nó chủ yếu nhằm mục đích để hỗ trợ các công nhận của cơ quan cấp giấy chứng nhận cung cấp chứng nhận ISMS theo tiêu chuẩn ISO/IEC 27001.

- Tiêu chuẩn mô tả hướng dẫn chung:
  - ISO/IEC 27002: Tiêu chuẩn này cung cấp một danh sách phổ biến mục tiêu kiểm soát được chấp nhận và hoạt động điều khiển tốt nhất để sử dụng như một hướng dẫn thực hiện khi lựa chọn và thực hiện điều khiển để đạt được an ninh thông tin.
  - ISO/IEC 27003 – Công nghệ thông tin – Các kỹ thuật an toàn – Hướng dẫn áp dụng hệ thống quản lý an toàn thông tin: Đây là tiêu chuẩn cung cấp hướng dẫn thực hiện hoạt động và cung cấp thêm thông tin cho thiết lập, thực thi, hoạt động, kiểm soát, xem xét, duy trì cải tiến một ISMS theo tiêu chuẩn ISO/IEC 27001.
  - ISO/IEC 27004 – Công nghệ thông tin – Các kỹ thuật an toàn – Quản lý an toàn thông tin – Đo lường: Tiêu chuẩn này cung cấp hướng dẫn và tư vấn về phát triển và sử dụng các phép đo để đánh giá hiệu quả của ISMS, mục tiêu kiểm soát và điều khiển sử dụng để thực hiện và quản lý an toàn thông tin theo quy định tại tiêu chuẩn ISO/IEC 27001.
  - ISO/IEC 27005 – Công nghệ thông tin – Các kỹ thuật an toàn – Quản lý rủi ro an toàn thông tin: Tiêu chuẩn này cung cấp hướng dẫn cho quản lý rủi ro an ninh thông tin. Các phương pháp mô tả trong tiêu chuẩn này hỗ trợ các khái niệm chung quy định tại ISO/IEC 27001.
  - ISO/IEC 27007 – Công nghệ thông tin – Các kỹ thuật an toàn – Hướng dẫn đánh giá hệ thống quản lý an toàn thông tin: Cung cấp hướng dẫn cho các tổ chức cần phải thực đánh giá nội bộ hay bên ngoài của một ISMS hoặc để quản lý một chương trình đánh giá ISMS áp vào các yêu cầu quy định tại ISO/IEC 27001.
  - ISO/IEC 27008 – Công nghệ thông tin – Các kỹ thuật an toàn – Hướng dẫn đối với chuyên gia đánh giá kiểm soát an toàn thông tin: Báo cáo kỹ thuật này tập trung vào các ý kiến của kiểm soát an toàn thông tin, bao gồm cả kiểm tra việc tuân thủ kỹ thuật, so với một tiêu chuẩn thực hiện an ninh thông tin, được thành lập bởi tổ chức. Nó không cung cấp bất kỳ hướng dẫn cụ thể về kiểm tra việc

tuân thủ liên quan đến đo lường, đánh giá rủi ro hay đánh giá một ISMS như quy định trong tiêu chuẩn ISO/IEC 27004, ISO/IEC 27005 hoặc ISO/IEC 27007 tương ứng. Báo cáo kỹ thuật này không dùng cho đánh giá hệ thống quản lý.

- ISO/IEC 27013: Để cung cấp cho các tổ chức với một sự hiểu biết tốt hơn về các đặc điểm, tương đồng và khác biệt của tiêu chuẩn ISO/IEC 27001 và ISO/IEC 20000-1 để hỗ trợ trong việc lập kế hoạch của một hệ thống quản lý tích hợp mà phù hợp với cả hai tiêu chuẩn quốc tế.
- ISO/IEC 27014: Tiêu chuẩn này sẽ cung cấp các hướng dẫn về nguyên tắc, quy trình quản trị an ninh thông tin, do đó các tổ chức có thể đánh giá, chỉ đạo và giám sát việc quản lý.
- ISO/IEC 27016: Báo cáo kỹ thuật này sẽ bổ sung cho họ tiêu chuẩn ISMS bằng cách một quan điểm kinh tế trong việc bảo vệ tài sản thông tin của một tổ chức trong bối cảnh của môi trường xã hội rộng rãi, trong đó một tổ chức hoạt động và cung cấp hướng dẫn làm thế nào để áp dụng kinh tế tổ chức an toàn thông tin thông qua việc sử dụng các mô hình và ví dụ.

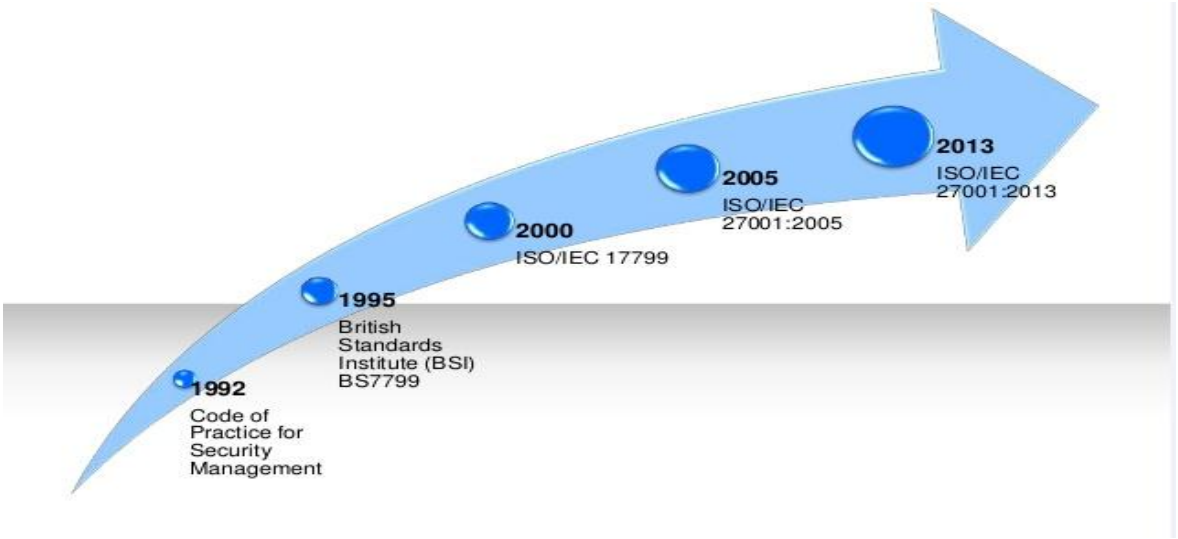
- Tiêu chuẩn mô tả các hướng dẫn cụ thể theo ngành
  - ISO/IEC 27010: Tiêu chuẩn này cung cấp những hướng dẫn thêm vào hướng dẫn cho bộ ISO/IEC 27000 của các tiêu chuẩn cho việc thực hiện quản lý an ninh thông tin trong các cộng đồng chia sẻ thông tin và cung cấp thêm các điều khiển và hướng dẫn cụ thể liên quan đến khởi xướng, thực hiện, duy trì và cải tiến an ninh thông tin trong truyền thông liên tổ chức và liên ngành.
  - ISO/IEC 27011: ISO/IEC 27011 cung cấp các tổ chức viễn thông với một sự thích nghi của ISO/IEC 27002 hướng dẫn duy nhất cho ngành công nghiệp của họ mà bổ sung cho các hướng dẫn được cung cấp nhằm thực hiện các yêu cầu của tiêu chuẩn ISO/IEC 27001, Phụ lục A.
  - ISO/IEC TR 27015: Báo cáo kỹ thuật này cung cấp hướng dẫn ngoài các hướng dẫn được đưa ra trong bộ tiêu chuẩn ISO/IEC 27000, để bắt đầu, thực hiện, duy trì, và cải tiến an ninh thông tin trong các tổ chức cung cấp dịch vụ tài chính.
  - ISO/IEC 27799: Tiêu chuẩn này cung cấp các hướng dẫn hỗ trợ việc thực hiện các thông tin quản lý an ninh trong các tổ chức y tế.

2.1.2. Khái niệm ISO 27001

ISO/IEC 27001 (Information Security Management System – ISMS) là tiêu chuẩn quy định các yêu cầu đối với việc xây dựng và áp dụng hệ thống quản lý an toàn thông tin nhằm đảm bảo tính bảo mật, tính toàn vẹn và tính sẵn sàng đối với tài sản thông tin của các tổ chức. Việc áp dụng một hệ thống quản lý an toàn thông tin sẽ giúp các tổ chức ngăn ngừa, hạn chế các tổn thất trong sản xuất, kinh doanh liên quan tới việc hư hỏng, mất mát các thông tin, dữ liệu quan trọng [8].

ISO/IEC 27001 là một tiêu chuẩn trong bộ tiêu chuẩn ISO/IEC 27000 về quản lý an toàn thông tin. Bộ tiêu chuẩn này được xây dựng dựa trên các tiêu chuẩn về quản lý an toàn thông tin BS 7799 của Viện Tiêu chuẩn Anh (British Standards Institute - BSI).

2.1.3. Lịch sử phát triển của ISO 27001



Hình 2.2: Lịch sử phát triển của ISO 27001

- Năm 1992: Phòng thương mại và công nghiệp Anh đã cho ra đời "Bộ quy tắc chuẩn cho hoạt động quản lý an toàn thông tin".
- Năm 1995: Bộ quy tắc trên được chỉnh sửa, bổ sung và tái bản bởi viện chuẩn hóa của Anh với cái tên là BS7799 (phần 1).
- Năm 1999: BS7799 được chỉnh sửa, cải tiến lần thứ nhất.
- Năm 2000: BS7799 được ISO công nhận và đặt tên là ISO/IEC 17799.
- Năm 2002: BS7799 phần 2 ra đời.
- Tháng 10 năm 2005 BS7799 phần 2 được ISO công nhận và đổi thành ISO 27001:2005.
- Có rất nhiều thay đổi của thế giới an ninh thông tin về các mối đe dọa, điểm yếu kỹ thuật và rủi ro liên quan đến điện toán đám mây, dữ liệu lớn và nhất là an ninh mạng đã gần 8 năm. Hơn 2 năm qua, các tổ chức tiêu chuẩn quốc gia trên toàn thế giới đã tổ chức cuộc họp với các chuyên gia chuyên ngành tìm kiếm các điểm cải tiến cho tiêu chuẩn ISO/IEC 27001:2013 và ISO/IEC 27002:2013. Kết quả đã rất tích cực và sẽ tinh giản quá trình áp dụng bằng cách bổ sung một số mức độ an ninh trước đây chưa có. Vì vậy tiêu chuẩn ISO/ IEC 27001: 2013 ra đời và được công bố tháng 10 năm 2013 [7].

2.1.4. Tiếp cận quá trình

Tổ chức phải xác định và quản lý nhiều hoạt động có thứ tự hiệu quả và có kết quả. Bất cứ hoạt động sử dụng tài nguyên cần được quản lý để cho phép biến đổi đầu vào

thành đầu ra sử dụng một thiết lập có tương quan với nhau hoặc những hoạt động ảnh hưởng lẫn nhau – đây được hiểu như một quá trình. Đầu ra của quá trình này có thể trực tiếp tạo thành đầu vào cho quá trình khác và thường biến đổi này được thực hiện theo lập kế hoạch và điều kiện kiểm soát.

Cách tiếp cận quá trình cho ISMS hiện trong họ tiêu chuẩn ISMS dựa trên nguyên tắc điều hành thông qua các tiêu chuẩn hệ thống quản lý phổ biến đã biết như Plan – Do – Check – Act:

- **Plan**: lập kế hoạch, xác định mục tiêu, phạm vi, nguồn lực để thực hiện, thời gian và phương pháp đạt mục tiêu.
- **Do**: Đưa kế hoạch vào thực hiện.
- **Check**: Dựa theo kế hoạch để kiểm tra kết quả thực hiện.
- **Act**: Thông qua các kết quả thu được để đề ra những tác động điều chỉnh thích hợp nhằm bắt đầu lại chu trình với những thông tin đầu vào mới [7].

2.1.5. Thiết lập, kiểm soát, duy trì và cải tiến ISMS

2.5.1.1. Tổng quan

Tổ chức cần làm theo các bước thiết lập, kiểm soát, duy trì và cải tiến ISMS của tổ chức:

a) Xác định thông tin tài sản và liên kết yêu cầu an toàn thông tin của tổ chức;
b) Đánh giá rủi ro an toàn thông tin và giải quyết rủi ro an toàn thông tin.
c) Lựa chọn và thực hiện điều khiển liên quan để quản lý những rủi ro không chấp nhận được.
d) Kiểm soát, duy trì và cải tiến hiệu quả liên kết với tài sản thông tin của tổ chức.

Để đảm bảo các ISMS được hiệu quả bảo vệ tài sản thông tin của tổ chức trên cơ sở liên tục, nó là cần thiết cho các bước (a) - (d) được liên tục lặp đi lặp lại để xác định những thay đổi trong những rủi ro hoặc trong chiến lược và mục tiêu của tổ chức [7].

2.5.1.2. Xác định yêu cầu an toàn thông tin

Trong phạm vi tất cả chiến lược và mục tiêu kinh doanh của tổ chức, quy mô và mở rộng địa lý, yêu cầu an toàn thông tin phải được xác định thông qua:

a) Xác định tài sản thông tin và giá trị của chúng;
b) Doanh nghiệp cần xử lý kinh doanh, lưu trữ và truyền thông; và
c) Quy định, các quy phạm pháp luật, và những yêu cầu ràng buộc.

Tiến hành đánh giá phương pháp của rủi ro liên quan đến tài sản thông tin của tổ chức sẽ bao gồm phân tích: mối đe dọa đến tài sản thông tin; lỗ hổng và khả năng của một mối đe dọa cụ thể hoá các tài sản thông tin; và các tác động tiềm năng của bất kỳ sự cố

an toàn thông tin đối với tài sản thông tin. Chi phí liên quan đến các kiểm soát dự tính sẽ tương ứng với ảnh hưởng đến nhận thức kinh doanh của rủi ro hiện ra [7].

2.5.1.3. Đánh giá rủi ro an toàn thông tin

Quản lý rủi ro an toàn thông tin yêu cầu đánh giá và phương pháp quản lý rủi ro phù hợp có thể bao gồm ước lượng chi phí và lợi ích, yêu cầu luật pháp, liên quan đến những người liên quan, và những đầu vào khác và thay đổi thích hợp.

Sự đánh giá rủi ro phải được xác định, định lượng và ưu tiên tiêu chí phòng chống rủi ro cho mục tiêu và sự chấp nhận rủi ro liên quan đến tổ chức. Kết quả phải hướng dẫn và xác định hoạt động quản lý thích hợp và ưu tiên đến quản lý rủi ro an toàn thông tin và thực hiện kiểm soát lựa chọn bảo vệ chống lại rủi ro.

Đánh giá rủi ro phải bao gồm phương pháp tự động ước lượng tầm quan trọng của rủi ro (phân tích rủi ro) và quá trình so sánh các rủi ro ước tính chống lại các tiêu chí rủi ro để xác định ý nghĩa của những rủi ro (đánh giá rủi ro).

Đánh giá rủi ro phải được thực hiện định kỳ để gửi thay đổi trong những yêu cầu an toàn thông tin và trong tình huống rủi ro, ví dụ: trong tài sản, nguy cơ, lỗ hổng, ảnh hưởng, đánh giá rủi ro và khi thay đổi quan trọng xảy ra. Đánh giá rủi ro phải được cam kết trong một cách có phương pháp có khả năng so sánh và sinh ra kết quả.

Đánh giá rủi ro an toàn thông tin phải có xác định phạm vi rõ ràng có thứ tự hiệu quả và phải bao gồm mối quan hệ với đánh giá rủi ro trong các vùng khác nhau, nếu thích hợp.

ISO/IEC 27005 cung cấp hướng dẫn quản lý an toàn thông tin, bao gồm hướng dẫn trong đánh giá rủi ro, giải quyết rủi ro, chấp nhận rủi ro, báo cáo rủi ro, kiểm soát rủi ro và xem xét rủi ro. Ví dụ của phương pháp đánh giá rủi ro được bao gồm là tốt [10].

2.5.1.4. Giải quyết rủi ro an toàn thông tin

Trước khi cân nhắc giải quyết rủi ro, tổ chức phải quyết định tiêu chí xác định rủi ro có được chấp nhận hay không. Rủi ro có thể được chấp nhận nếu, ví dụ, nó được đánh giá rằng rủi ro là thấp hoặc chi phí giải quyết rủi ro không có lợi cho tổ chức. Quyết định này nên được ghi lại.

Cho từng rủi ro được xác định sau khi đánh giá rủi ro một quyết định xử lý rủi ro cần phải được thực hiện. Lựa chọn giải quyết rủi ro bao gồm:

a) Áp dụng kiểm soát thích hợp để giảm thiểu rủi ro;

b) Hiểu biết và mục tiêu chấp nhận rủi ro, cung cấp rõ ràng chính sách của tổ chức và tiêu chí 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 liên kết rủi ro đến các bên khác, ví dụ công ty bảo hiểm hoặc nhà cung ứng.

Những nơi quyết định giải quyết rủi ro để áp dụng kiểm soát thích hợp, những kiểm soát phải được lựa chọn và thực hiện [7].

2.1.5.5. Lựa chọn và thực hiện kiểm soát

Một yêu cầu an toàn thông tin được xác định, những rủi ro an toàn thông tin để nhận biết thông tin tài sản được xác định và đánh giá và quyết định giải quyết rủi ro an toàn thông tin được làm, sau đó lựa chọn và thực hiện kiểm soát áp dụng giảm thiểu rủi ro.

Kiểm soát phải đảm bảo rằng rủi ro được giảm thiểu để một mức độ chấp nhận được tính đến:

a) Yêu cầu và ràng buộc của dân tộc và quy định và luật pháp quốc gia;

b) Mục tiêu của tổ chức;

c) Ràng buộc và yêu cầu hoạt động;

d) Chi phí của tổ chức thực hiện và hoạt động trong mối liên hệ với rủi ro được giảm, và tỷ lệ còn lại đối với những yêu cầu và ràng buộc của tổ chức;

e) Họ phải thực hiện để giám sát, đánh giá và cải tiến hiệu quả và kiểm soát an toàn thông tin hiệu quả để hỗ trợ mục đích của tổ chức. Sự lựa chọn và sự thực hiện hiện các kiểm soát nên được ghi chép trong một tuyên bố của ứng dụng để hỗ trợ các yêu cầu tuân thủ.

f) Sự cần thiết để cân bằng đầu tư trong việc thực hiện và hoạt động của điều khiển so với khả năng mất là kết quả của sự cố an toàn thông tin [7].

2.1.5.6. Giám sát, duy trì và cải tiến hiệu quả ISMS

Một tổ chức cần duy trì và cải tiến ISMS thông qua giám sát và đánh giá thực hiện chống lại chính sách và mục tiêu của tổ chức, và báo cáo kết quả cho quản lý xem xét. Sự xem xét ISMS này sẽ kiểm tra xem ISMS bao gồm kiểm soát đặc biệt phù hợp để giải quyết rủi ro trong phạm vi ISMS. Hơn thế nữa, dựa trên bản ghi theo dõi khu vực, nó sẽ cung cấp bằng chứng xác thực, và truy xuất khắc phục, phòng ngừa và những hoạt động cải tiến để có cơ hội tìm kiếm cải tiến và không đảm đương hoạt động quản lý tồn tại đều đủ tốt hoặc tốt như chúng có thể.

Hoạt động cho cải tiến bao gồm:

a) Phân tích và ước lượng thực trạng hiện tại để xác định khu vực cải tiến;

b) Thiết lập mục tiêu để cải tiến;

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

d) Ước lượng giải pháp và lựa chọn;

e) Thực hiện lựa chọn giải pháp;

f) Đo lường, xác thực, phân tích và đánh giá kết quả thực hiện để xác định mục tiêu đã đạt được;

g) Thay đổi chính thức.

Kết quả được xem xét, là cần thiết, để xác định cơ hội cải tiến. Trong cách này, cải tiến là một hoạt động liên tục, ví dụ hoạt động được lặp lại thường xuyên. Phản hồi từ khách hàng và các bên liên quan khác, đánh giá và xem xét hệ thống quản lý an toàn thông tin có thể cũng được sử dụng để xác định cơ hội cải tiến [7].

2.1.5.7. Cải tiến liên tục

Mục tiêu cải tiến liên tục của tổ chức ISMS để tăng xác suất đạt được mục tiêu liên quan đến duy trì tính bảo mật, tính xác thực, tính toàn vẹn của thông tin. Tập trung cái tiến liên tục [7].

2.1.6. Phạm vi áp dụng

Tiêu chuẩn Quốc tế này định rõ các yêu cầu cho việc thiết lập, thực hiện, duy trì và cải tiến liên tục một hệ thống quản lý an toàn thông tin trong bối cảnh của tổ chức. Tiêu chuẩn Quốc tế này cũng bao gồm các yêu cầu cho việc đánh giá và xử lý các rủi ro an toàn thông tin tương ứng với nhu cầu của tổ chức. Các yêu cầu nêu ra trong Tiêu chuẩn Quốc tế này có tính tổng quát và nhắm đến việc áp dụng cho tất cả các tổ chức, không phân biệt loại hình, quy mô hay bản chất. Việc loại trừ bất kỳ yêu cầu nào trong phạm vi từ điều 2.2.2 đến điều 2.2.8 là không thể chấp nhận được khi một tổ chức tuyên bố phù hợp với Tiêu chuẩn Quốc tế này [8].

2.2. HỆ THỐNG QUẢN LÝ AN TOÀN THÔNG TIN

2.2.1. Thuật ngữ và định nghĩa

Tiêu chuẩn ISO 27001 áp dụng các thuật ngữ và định nghĩa nêu trong ISO 27000 và được trình bày dưới đây:

2.2.1.1. Đánh giá

Có hệ thống, độc lập và quá trình đưa ra tài liệu cho việc thu thập bằng chứng đánh giá hiện hành và đánh giá nó một cách khách quan để xác định mức độ mà các tiêu chí đánh giá được hoàn thành.

Chú ý 1: Một đánh giá có thể là đánh giá nội bộ (bên thứ nhất) hoặc đánh giá bên ngoài (bên thứ hai hoặc bên thứ ba).

Chú ý 2: “Bằng chứng đánh giá” và “tiêu chí đánh giá” được định nghĩa trong ISO 19011.

2.2.1.2. Tính sẵn sàng

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

2.2.1.3. Tính bảo mật

Tính chất đảm bảo rằng thông tin không được cung cấp hoặc tiết lộ đối với các cá nhân, thực thể và các quá trình trái phép.

2.2.1.4. Tính toàn vẹn

Tính chất bảo vệ sự chính xác và sự toàn vẹn của các tài sản

2.2.1.5. Thẩm quyền

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

2.2.1.6. Phù hợp

Sự đáp ứng một yêu cầu.

2.2.1.7. Cải tiến liên tục

Hoạt động định kỳ để nâng cao hiệu năng.

2.2.1.8. Kiểm soát

Biện pháp quản lý rủi ro, bao gồm các chính sách, các quy trình, các hướng dẫn, thực hành hoặc cơ cấu tổ chức, trong đó có thể là hành chính, kỹ thuật, quản lý, hoặc tính chất pháp lý.

2.2.1.9. Khắc phục

Hành động để loại bỏ sự không phù hợp được phát hiện.

2.2.1.10. Hành động khắc phục

Hành động để loại bỏ nguyên nhân của sự không phù hợp và để phòng ngừa phát sinh.

2.2.1.11. Tài liệu thông tin

Thông tin yêu cầu phải được kiểm soát và duy trì bởi tổ chức và phương tiện mà nó được chứa.

Chú ý 1: Tài liệu thông tin có thể có bất kỳ định dạng và phương tiện truyền thông và từ bất kỳ nguồn nào

Chú ý 2: Tài liệu thông tin có thể đề cập đến:

- Hệ thống quản lý, bao gồm các quá trình liên quan.
- Thông tin được tạo ra trong trật tự cho tổ chức để hoạt động (tài liệu).
- Đánh giá kết quả đạt được (hồ sơ).

2.2.1.12. Hiệu quả

Quy mô mà lên kế hoạch hoạt động được thực hiện và dự kiến kết quả đạt được.

2.2.1.13. An toàn thông tin

Sự duy trì tính bảo mật, tính toàn vẹn và tính sẵn sàng của thông tin; ngoài ra có thể bao hàm tính chất xác thực, kiểm soát, chống chối bỏ và tin cậy.

2.2.1.14. Các bên liên quan

Cá nhân hoặc tổ chức có thể ảnh hưởng, bị ảnh hưởng, hoặc tự lĩnh hội khi bị ảnh hưởng bởi một quyết định hoặc hoạt động.

2.2.1.15. Hệ thống quản lý

Thiết lập những yếu tố có quan hệ với nhau hoặc ảnh hưởng lẫn nhau của một tổ chức để thiết lập chính sách, mục tiêu và quá trình để đạt được những mục tiêu đó.

2.2.1.16. Đo lường

Quá trình xác định giá trị.

Chú ý: Trong bối cảnh an ninh thông tin, quá trình xác định giá trị yêu cầu thông tin về tính hiệu quả của một hệ thống quản lý an ninh thông tin và kiểm soát liên kết của chúng sử dụng phương pháp đo lường, chức năng đo lường, mô hình phân tích và tiêu chí quyết định.

2.2.1.17. Kiểm tra

Xác định trạng thái của hệ thống, quá trình hoặc hoạt động.

Chú ý: Để xác định trạng thái đó có thể cần kiểm tra, giám sát hoặc quan sát.

2.2.1.18. Không phù hợp.

Không hoàn thành một yêu cầu.

2.2.1.19. Mục tiêu

Là kết quả đạt được.

2.2.1.20. Tổ chức

Cá nhân hoặc nhóm người có chức vụ riêng của mình với trách nhiệm, quyền hạn và các mối quan hệ.

2.2.1.21. Thuê ngoài

Thực hiện thỏa thuận với một tổ chức bên ngoài thực hiện một phần chức năng của tổ chức.

2.2.1.22. Thành quả

Kết quả đo được.

2.2.1.23. Chính sách

Mục đích và phương hướng của một tổ chức thể hiện bởi lãnh đạo cao nhất.

2.2.1.24. Quá trình

Tập hợp các hoạt động ảnh hưởng lẫn nhau hoặc tác động lẫn nhau thay đổi đầu vào thành đầu ra.

2.2.1.25. Yêu cầu

Nhu cầu hay mong muốn được tuyên bố, thường bao hàm hoặc bắt buộc.

2.2.1.26. Xem xét

Hoạt động được thực hiện để xác định sự phù hợp, đầy đủ và hiệu quả của những đề tài chính.

2.2.1.27. Rủi ro

Ảnh hưởng đến mục tiêu.

2.2.1.28. Quản lý rủi ro

Cá nhân hoặc tổ chức có trách nhiệm và thẩm quyền để quản lý rủi ro

2.2.1.29. Lãnh đạo cao nhất

Cá nhân hoặc nhóm người định hướng và kiểm soát tổ chức ở cấp cao nhất.

2.2.2. Bối cảnh của tổ chức

Làm rõ bối cảnh của tổ chức để xác định phạm vi của hệ thống ISMS.

2.2.2.1. Hiểu tổ chức và bối cảnh của nó

Tổ chức phải xác định các vấn đề bên ngoài và nội bộ có liên quan đến mục đích và có ảnh hưởng đến khả năng đạt được (các) đầu ra dự kiến của hệ thống quản lý an toàn thông tin.

Chú thích: Việc xác định những vấn đề này đề cập đến thiết lập bối cảnh nội bộ và bên ngoài của tổ chức được xem xét tại điều khoản 5.3 ISO 31000

2.2.2.2. Hiểu các nhu cầu và mong đợi của các bên quan tâm

Tổ chức phải xác định:

Các bên liên quan đến hệ thống quản lý an toàn thông tin và các yêu cầu của họ đến hệ thống quản lý an toàn thông tin.

Chú thích: Các yêu cầu của các bên liên quan này có thể bao gồm các yêu cầu luật định, quy định và các yêu cầu bắt buộc theo hợp đồng.

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

Tổ chức phải xác định những đường biên giới và áp dụng hệ thống quản lý an toàn thông tin để thiết lập phạm vi.

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

a) Các vấn đề bên ngoài và nội bộ nêu tại 2.2.2.1;

b) Các yêu cầu nêu tại 2.2.2.2; và

c) Sự tương tác và độc lập giữa các hoạt động thực hiện bởi tổ chức và các hoạt động được thực hiện bởi các tổ chức khác. Phạm vi phải sẵn có ở dạng thông tin dạng văn bản.

2.2.2.4. Hệ thống quản lý an toàn thông tin

Tổ chức phải thiết lập, thực hiện, duy trì và cải tiến liên tục một hệ thống quản lý an toàn thông tin, trong mọi trường hợp với các yêu cầu của Tiêu chuẩn quốc tế này.

2.2.3. Lãnh đạo

2.2.3.1. Lãnh đạo và cam kết

Lãnh đạo cao nhất phải chứng minh được vai trò lãnh đạo và cam kết đối với hệ thống quản lý an toàn thông tin bằng cách:

Đảm bảo chính sách an toàn thông tin và các mục tiêu an toàn thông tin được thiết lập và phù hợp với chiến lược định hướng của tổ chức.

Đảm bảo tích hợp các yêu cầu của hệ thống quản lý an toàn thông tin và các quá trình của tổ chức.

Đảm bảo rằng các nguồn lực cần thiết đối với hệ thống quản lý an toàn thông tin là sẵn có.

Truyền đạt tầm quan trọng của ảnh hưởng hệ thống quản lý an toàn thông tin và của sự phù hợp đối với các yêu cầu của hệ thống quản lý an toàn thông tin;

Đảm bảo rằng hệ thống quản lý an toàn thông tin đạt được (các) đầu ra dự kiến của nó.

Chỉ dẫn và hỗ trợ nhân sự đóng góp đối với tính hiệu lực của hệ thống quản lý an toàn thông tin.

Thúc đẩy cải tiến liên tục; và

Hỗ trợ các vai trò quản lý liên quan khác để chứng minh vai trò lãnh đạo của họ khi nó được áp dụng trong phạm vi trách nhiệm của mình.

2.2.3.2. Chính sách

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

a) Phù hợp với mục đích của tổ chức;
b) Bao gồm các mục tiêu an toàn thông tin hoặc cung cấp khuôn khổ cho việc thiết lập các mục tiêu an toàn thông tin;
c) Bao gồm một cam kết thỏa mãn các yêu cầu liên quan đến an toàn thông tin; và
d) Bao gồm một cam kết cải tiến liên tục hệ thống quản lý an toàn thông tin;

Chính sách an toàn thông tin phải:

e) Sẵn có ở dạng văn bản;
f) Được truyền đạt trong tổ chức; và
g) Sẵn có cho các bên quan tâm, khi thích hợp.

2.2.3.3. Vai trò tổ chức, trách nhiệm và quyền hạn

Lãnh đạo cao nhất phải đảm bảo các trách nhiệm và quyền hạn cho các vai trò liên quan đến an toàn thông tin được chỉ định và được truyền đạt.

Lãnh đạo cao nhất phải chỉ định trách nhiệm và quyền hạn để:

a) Đảm bảo rằng hệ thống quản lý an toàn thông tin phù hợp với yêu cầu của Tiêu chuẩn Quốc tế này; và
b) Báo cáo kết quả thực hiện của hệ thống quản lý an toàn thông tin đến lãnh đạo cao nhất.

Chú thích: Lãnh đạo cao nhất có thể cũng chỉ định các trách nhiệm và quyền hạn cho việc báo cáo kết quả của hệ thống quản lý an toàn thông tin trong tổ chức.

2.2.4. Hoạch định

2.2.4.1. Hành động và cơ hội giải quyết rủi ro

2.2.4.1.1. Khái quát

Khi hoạch định hệ thống quản lý an toàn thông tin, tổ chức phải xem xét các vấn đề nêu tại 2.2.2.1 và các yêu cầu nêu tại 2.2.2.2 xác định các rủi ro và các cơ hội được giải quyết để:

a) Đảm bảo hệ thống quản lý an toàn thông tin có thể đạt được (các) đầu ra dự kiến của mình;
b) Ngăn ngừa, hoặc giảm thiểu, các ảnh hưởng không mong muốn; và
c) Đạt được cải tiến liên tục.

Tổ chức phải lập kế hoạch:

d) Các hành động nhằm giải quyết các rủi ro và cơ hội này; và

e) Làm thế nào để:

1) Tích hợp và thực hiện các hành động vào bên trong các quá trình của hệ thống an toàn thông tin của mình; và

2) Đánh giá hiệu lực của các hành động này.

2.2.4.1.2. Đánh giá rủi ro an toàn thông tin

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

a) Thiết lập và duy trì các chuẩn mực an toàn thông tin bao gồm:

1) Chuẩn mực chấp nhận rủi ro; và

2) Chuẩn mực đối với việc thực hiện đánh giá rủi ro an toàn thông tin;

b) Đảm bảo rằng các đánh giá rủi ro an toàn thông tin lặp lại được thực hiện nhất quán, có cơ sở và đưa đến các kết quả so sánh được;

c) Nhận diện các rủi ro an toàn thông tin:

1) Áp dụng quá trình đánh giá rủi ro an toàn thông tin để xác định các rủi ro liên quan đến việc mất an ninh, toàn vẹn và sẵn có của thông tin trong phạm vi của hệ thống quản lý an toàn thông tin; và

2) Nhận biết chủ sở hữu rủi ro;

d) Phân tích rủi ro an toàn thông tin:

1) Đánh giá các hậu quả tiềm ẩn đưa đến nếu rủi ro được nhận diện tại 2.2.4.2 c) 1) xảy ra.

2) Đánh giá khả năng xảy ra của những rủi ro đã nhận diện tại 2.2.4.2 c) 1); và

3) Xác định các mức độ rủi ro;

e) Đánh giá rủi ro an toàn thông tin:

1) So sánh kết quả phân tích rủi ro với các chuẩn mực rủi ro đã thiết lập ở 2.2.4.2 a); và

2) Ưu tiên các rủi ro được phân tích cho việc xử lý rủi ro.

Tổ chức phải duy trì thông tin dạng văn bản về quá trình đánh giá rủi ro an toàn thông tin.

2.2.4.1.3. Giải quyết rủi ro an toàn thông tin

Tổ chức phải xác định và áp dụng một quá trình giải quyết rủi ro an toàn thông tin để:

a) Lựa chọn giải quyết rủi ro an toàn thông tin phù hợp, tính đến cả kết quả đánh giá rủi ro;

b) Xác định tất cả các kiểm soát cần thiết để thực hiện sự lựa chọn giải quyết rủi ro an toàn thông tin;

Chú ý: Tổ chức có thể thiết kế kiểm soát như yêu cầu, hoặc định nghĩa chúng từ bất kỳ nguồn nào.

c) So sánh những kiểm soát được xác định trong 2.2.4.3 b) dưới với phụ lục A và xác minh rằng không có kiểm soát cần thiết bị bỏ qua;

Chú ý 1: Phụ lục A chứa một danh sách toàn diện các mục tiêu kiểm soát và điều khiển. Người sử dụng của tiêu chuẩn quốc tế hướng đến phụ lục A để đảm bảo rằng không có kiểm soát cần thiết bị bỏ qua.

Chú ý 2: Mục tiêu kiểm soát hoàn toàn được bao gồm trong các điều khiển chọn. Mục tiêu kiểm soát và điều khiển được liệt kê trong phụ lục A là chưa đầy đủ và bổ sung mục tiêu kiểm soát và điều khiển có thể là cần thiết.

d) Quy trình trong tuyên bố áp dụng chứa điều khiển cần thiết (xem 2.2.4.3 b và c) và chứng minh được bao gồm, dù họ có thực hiện hay không, và chứng minh bao gồm của kiểm soát từ phụ lục A;

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

f) Đạt được sự phê duyệt của quản lý rủi ro của các kế hoạch xử lý rủi ro an ninh thông tin và chấp nhận rủi ro an toàn thông tin còn lại.

Tổ chức phải giữ lại thông tin tài liệu về quá trình xử lý rủi ro an toàn thông tin.

Chú ý: Quá trình đánh giá và giải quyết rủi ro trong tiêu chuẩn quốc tế này gắn với các nguyên tắc và hướng dẫn chung trong ISO 31000.

2.2.4.2. Các mục tiêu an toàn thông tin và hoạch định để đạt được chúng

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

Các mục tiêu an toàn thông tin phải:

a) Nhất quán với chính sách an toàn thông tin;

b) Đo lường được;

c) Xem xét đến việc áp dụng các yêu cầu an toàn thông tin, và kết quả đánh giá và xử lý rủi ro;

d) Được truyền đạt; và

e) Được cập nhật khi thích hợp.

Tổ chức phải duy trì thông tin dạng văn bản về các mục tiêu an toàn thông tin.

Khi hoạch định cách thức để đạt được các mục tiêu an toàn thông tin của mình, tổ chức phải xác định:

f) Điều gì sẽ được hoàn thành;

g) Các nguồn lực gì sẽ được yêu cầu;

h) Ai sẽ chịu trách nhiệm;

i) Khi nào nó sẽ được hoàn thành; và

j) Các kết quả được đánh giá thế nào;

2.2.5. Hỗ trợ

2.2.5.1. Các nguồn lực

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

2.2.5.2. Năng lực

Tổ chức phải:

a) Xác định năng lực cần thiết của (những) người làm việc dưới sự kiểm soát của mình có ảnh hưởng đến kết quả an toàn thông tin của tổ chức.
b) Đảm bảo rằng những người có năng lực dựa trên cơ sở giáo dục, đào tạo hoặc kinh nghiệm thích hợp.
c) Khi áp dụng, thực hiện các hành động để đạt được năng lực cần thiết, và đánh giá hiệu lực của các hành động được thực hiện; và
d) Duy trì các thông tin dạng văn bản như là bằng chứng về năng lực.

Chú thích: Các hành động có thể áp dụng có thể bao gồm, ví dụ như: Cung cấp đào tạo, cố vấn, tái bổ nhiệm nhân sự hiện tại; hoặc thuê mướn hoặc hợp đồng với những người có năng lực.

2.2.5.3. Nhận thức

Những người làm việc dưới sự kiểm soát của tổ chức phải có nhận thức về:

a) Chính sách an toàn thông tin;
b) Đóng góp của họ vào tính hiệu lực của hệ thống quản lý thông tin, bao gồm cả các lợi ích của kết quả an toàn thông tin được cải tiến; và
c) Những tác động của sự không phù hợp với các yêu cầu của hệ thống quản lý an toàn thông tin.

2.2.5.4. Trao đổi thông tin

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

a) Về điều gì cần trao đổi;
b) Khi nào trao đổi;
c) Trao đổi với ai;
d) Ai phải trao đổi; và
e) Các quá trình trao đổi thông tin phải bị ảnh hưởng.

2.2.5.5. Thông tin dạng văn bản

2.2.5.5.1. Khái quát

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

a) Thông tin dạng văn bản được yêu cầu bởi Tiêu chuẩn Quốc tế này; và

b) Thông tin dạng văn bản được tổ chức xác định là cần thiết đối với tính hiệu lực của hệ thống quản lý an toàn thông tin.

Chú thích: Mức độ của thông tin dạng văn bản đối với hệ thống quản lý có thể khác nhau giữa các tổ chức khác nhau vì:

1) Quy mô và loại hình hoạt động, các quá trình, sản phẩm và dịch vụ của tổ chức;
2) Tính phức tạp của các quá trình và sự tương tác của chúng; và
3) Năng lực nhân sự

2.2.5.5.2. Tạo vào cập nhật

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

a) Nhận biết và mô tả (ví dụ một tiêu đề, ngày, tác giả hoặc số tham chiếu);

b) Định dạng (ví dụ: ngôn ngữ, phiên bản phần mềm, hình ảnh) và dạng thể hiện (ví dụ: bản in, bản điện tử); và

c) Xem xét và phê duyệt sự đầy đủ và phù hợp.

2.2.5.5.3. Kiểm soát thông tin dạng văn bản

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

a) Nó phải sẵn có và phù hợp cho việc sử dụng, ở đâu và khi nào nó cần thiết; và

b) Nó phải được bảo vệ thỏa đáng (ví dụ khỏi mất tính bảo mật, sử dụng trái phép, hoặc mất tính toàn vẹn).

Để kiểm soát thông tin dạng văn bản, tổ chức phải chỉ rõ các hoạt động bên dưới, khi có thể áp dụng:

c) Phân phối, truy cập, truy xuất và sử dụng;
d) Bảo quản và bảo tồn, bao gồm cả bảo tồn sự rõ ràng;
e) Kiểm soát sự thay đổi (ví dụ kiểm soát phiên bản); và
f) Lưu trữ và hủy bỏ.

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

Chú thích: Sự truy cập ngụ ý một quyết định liên quan đến sự cho phép chỉ được xem thông tin dạng văn bản, hoặc được phép và có quyền xem và thay đổi thông tin dạng văn bản,…

2.2.6. Điều hành

2.2.6.1. Hoạch định điều hành và kiểm soát

Tổ chức phải lập kế hoạch, thực hiện và kiểm soát các quá trình cần thiết để đáp ứng các yêu cầu an toàn thông tin, và để thực hiện các hành động đã xác định trong 2.2.4.1. Tổ chức cũng phải thực hiện các kế hoạch để đạt được các mục tiêu an toàn thông tin đã xác định ở 2.2.4.2.

Tổ chức phải duy trì thông tin dạng văn bản đủ mức cần thiết để tin rằng các quá trình đã thực hiện theo đúng hoạch định.

Tổ chức phải kiểm soát các thay đổi theo hoạch định và xem xét các hậu quả của những thay đổi ngoài ý muốn, thực hiện các hành động nhằm giảm nhẹ các ảnh hưởng xấu, khi cần thiết.

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

2.2.6.2. Đánh giá rủi ro an toàn thông tin

Tổ chức phải thực hiện các đánh giá rủi ro an toàn thông tin ở một tần suất đã hoạch định hoặc khi có thay đổi đáng kể được đề nghị hoặc đã xảy ra, sử dụng các tiêu chí đã thiết lập ở 2.2.4.1.2 a).

Tổ chức phải duy trì các thông tin dạng văn bản về các kết quả đánh giá rủi ro an toàn thông tin.

2.2.6.3. Xử lý rủi ro an toàn thông tin

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

Tổ chức phải duy trì các thông tin dạng văn bản về kết quả xử lý rủi ro an toàn thông tin.

2.2.7. Đánh giá kết quả

2.2.7.1. Theo dõi, đo lường, phân tích và đánh giá

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

Tổ chức phải xác định:

a) Điều gì cần được theo dõi và đo lường, bao gồm các quá trình an toàn thông tin và các biện pháp kiểm soát;

b) Các phương pháp theo dõi, đo lường, phân tích và đánh giá, khi có thể áp dụng, phải đảm bảo các kết quả đúng;

Chú thích: Các phương pháp được chọn nên tạo ra các kết quả so sánh được và có thể tái tạo các kết quả được xem là hợp lệ.

c) Khi nào việc theo dõi và đo lường phải được thực hiện;

d) Ai phải theo dõi và đo lường;

e) Khi nào các kết quả từ việc theo dõi và đo lường phải được phân tích và đánh giá; và;

f) Ai phải phân tích và đánh giá các kết quả này.

Tổ chức phải duy trì các thông tin dạng văn bản như là bằng chứng của các kết quả theo dõi và đo lường.

2.2.7.2. Đánh giá nội bộ

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

a) Có phù hợp với:

1) Các yêu cầu của chính tổ chức đối với hệ thống quản lý an toàn thông tin của mình; và

2) Các yêu cầu của Tiêu chuẩn Quốc tế này;

b) Được thực hiện và được duy trì một cách có hiệu lực.

Tổ chức phải:

c) Lập kế hoạch, thiết lập, thực hiện và duy trì chương trình đánh giá, bao gồm tần suất, phương pháp, các trách nhiệm, các yêu cầu hoạch định và báo cáo.

Các chương trình đánh giá phải xem xét đến tầm quan trọng của các quá trình liên quan và các kết quả đánh giá trước đó.

d) Xác định chuẩn mực và phạm vi đánh giá cho mỗi lần đánh giá;

e) Lựa chọn chuyên gia và thực hiện đánh giá đảm bảo tính khách quan và công bằng của quá trình đánh giá;

f) Đảm bảo rằng các kết quả đánh giá được báo cáo đến các cấp lãnh đạo liên quan; và

g) Duy trì thông tin dạng văn bản như là bằng chứng của (các) chương trình đánh giá và kết quả đánh giá.

2.2.7.3. Xem xét của lãnh đạo

Lãnh đạo cao nhất phải xem xét hệ thống quản lý an toàn thông tin của tổ chức ở một tần suất đã hoạch định để đảm bảo nó liên tục phù hợp, đầy đủ và có hiệu lực.

Xem xét của lãnh đạo phải bao gồm các xem xét về:

a) Tình trạng của các hành động và có được từ lần xem xét trước

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

c) Các phản hồi về kết quả an toàn thông tin, bao gồm xu hướng của:

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

2) Các kết quả theo dõi và đo lường;

3) Các kết quả đánh giá; và

4) Mức độ đạt được của các mục tiêu an toàn thông tin;

d) Phản hồi từ các bên quan tâm;

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

f) Các cơ hội cải tiến liên tục.

Các đầu ra của xem xét của lãnh đạo phải bao gồm các quyết định liên quan đến các cơ hội cải tiến liên tục và mọi nhu cầu thay đổi đối với hệ thống quản lý an toàn thông tin.

Tổ chức phải duy trì thông tin dạng văn bản làm bằng chứng về kết quả xem xét của lãnh đạo.

2.2.8. Cải tiến

2.2.8.1. Sự không phù hợp và hành động khắc phục

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

a) Phản ứng lại với sự không phù hợp, và khi áp dụng:

1) Thực hiện các biện pháp kiểm soát và khắc phục nó; và

2) Giải quyết các hậu quả;

b) Đánh giá nhu cầu thực hiện hành động nhằm loại bỏ nguyên nhân của sự không phù hợp, theo cách để nó không tái diễn hoặc không xảy ra, bằng cách:

1) Xem xét sự không phù hợp;

2) Xác định các nguyên nhân gốc rễ của sự không phù hợp; và

3) Xác định xem liệu các sự không phù hợp tương tự có tồn tại không, hoặc có thể xảy ra không;

c) Thực hiện mọi hành động cần thiết;

d) Xem xét tính hiệu lực của các hành động khắc phục được thực hiện; và

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

Các hành động phải thích hợp với tác động của sự không phù hợp gặp phải.

Tổ chức phải duy trì thông tin dạng văn bản như là bằng chứng của:

f) Bản chất của sự không phù hợp và bất kỳ hành động tiếp theo nào được thực hiện.

g) Các kết quả của mọi hành động khắc phục.

2.2.8.2. Cải tiến liên tục

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

2.2.9. Trình bày về phụ lục A của tiêu chuẩn

A.5 Chính sách an toàn thông tin		
A.5.1 Hướng quản lý chính sách an toàn thông tin Mục tiêu: Để cung cấp hướng quản lý và hỗ trợ an toàn thông tin theo những yêu cầu doanh nghiệp và những phép tắc và những quy định liên quan		
A.5.1.1	Chính sách an toàn thông tin	*Kiểm soát* Một bộ chính sách an toàn thông tin phải được xác định, phê duyệt bởi quản lý, công bố và truyền đạt đến tất cả nhân viên và những tổ chức liên quan.
A.5.1.2	Xem xét chính sách an toàn thông tin	*Kiểm soát* Chính sách an toàn thông tin phải được xem xét theo kế hoạch hoặc nếu xuất hiện những thay đổi đáng kể để đảm bảo nó luôn thích hợp, đầy đủ và hiệu quả.
A.6 Tổ chức của an toàn thông tin		
A.6.1 Tổ chức nội bộ		
Mục tiêu: Để thiết lập một nền tảng quản lý đến khởi đầu và kiểm soát thực hiện và hoạt động của an toàn thông tin giữa tổ chức.		
A.6.1.1	Vai trò và trách nhiệm an toàn thông tin	*Kiểm soát* Tất cả các trách nhiệm an toàn thông tin phải được xác định và phân bổ.
A.6.1.2	Sự phân chia nhiệm vụ	*Kiểm soát* Nhiệm vụ đối lập và phạm vi trách nhiệm phải được

		phân chia để giảm thiểu thời cơ trái phép hoặc sự thay đổi không được định trước hoặc lạm dụng các tài sản của tổ chức.
A.6.1.3	Liên hệ với các cơ quan có liên quan	*Kiểm soát* Liên hệ phù hợp với các cơ quan liên quan phải được duy trì.
A.6.1.4	Liên hệ với nhóm lợi ích đặc biệt	*Kiểm soát* Liên hệ phù hợp với các nhóm lợi ích đặc biệt hoặc các diễn đàn an ninh chuyên môn khác và hiệp hội nghề nghiệp phải được duy trì.
A.6.1.5	An toàn thông tin trong quản lý dự án	*Kiểm soát* An toàn thông tin phải được giải quyết trong quản lý dự án, không phụ thuộc vào loại của dự án.
A.6.2 Các thiết bị di động và làm việc từ xa		
Mục tiêu: Để đảm bảo an toàn thiết bị làm việc từ xa và sử dụng thiết bị di động		
A.6.2.1	Chính sách thiết bị di động	*Kiểm soát* Một chính sách và hỗ trợ các biện pháp an ninh phải được thông qua để quản lý các rủi ro được giới thiệu bằng cách sử dụng các thiết bị di động.
A.6.2.2	Thiết bị làm việc từ xa	*Kiểm soát* Một chính sách và hỗ trợ các biện pháp an ninh phải được thực hiện để bảo vệ truy cập thông tin, xử lý và lưu trữ tại nơi chứa các thiết bị làm việc từ xa.
A.7 Bảo vệ nguồn nhân lực		
A.7.1 Trước khi làm việc		
Mục tiêu: Để đảm bảo rằng những nhân viên và nhà thầu hiểu được trách nhiệm của họ, và đồng bộ cho vai trò mà họ được cân nhắc.		
A.7.1.1	Sàng lọc	*Kiểm soát*

		Kiểm tra nền tảng của tất cả những người được coi là thích hợp cho nhân viên phải được tiến hành trong mọi trường hợp liên quan đến phép tắc, những quy định và nội quy và phải tương xứng với những yêu cầu doanh nghiệp, phân loại thông tin để truy cập và nhận biết được những rủi ro
A.7.1.2	Điều khoản và điều kiện làm việc	*Kiểm soát* Các thỏa thuận hợp đồng với những nhân viên và những nhà thầu phải nêu tình trạng của họ và trách nhiệm của tổ chức an toàn thông tin.
A.7.2 Trong quá trình làm việc		
Mục tiêu: Để đảm bảo rằng những nhân viên, nhà thầu nhận biết và thực hiện trách nhiệm an ninh thông tin của mình.		
A.7.2.1	Trách nhiệm quản lý	*Kiểm soát* Quản lý phải yêu cầu tất cả nhân viên và nhà thầu áp dụng bảo vệ thông tin trong mọi trường hợp với những chính sách và quy trình của tổ chứcđược thiết lập.
A.7.2.2.	Nhận thức giáo dục, đào tạo an toàn thông tin	*Kiểm soát* Tất cả nhân viên của tổ chức và, nơi có liên quan, những nhà thầu phải thu nhận được sự nhận thức giáo dục và đào tạo và cập nhật thường xuyên các chính sách và quy trình tổ chức, cũng như liên quan với chức năng công việc của họ.
A.7.2.3.	Quá trình kỷ luật	*Kiểm soát* Đây sẽ là một quá trình xử lý kỷ luật hình thức và truyền đạt tại chỗ để hành động áp vào người lao động mà họ đã vi phạm an toàn thông tin
A.7.3 Chấm dứt hoặc thay đổi nhân sự		
Mục tiêu: Để bảo vệ các tổ chức liên quan như một phần của quy trình thay đổi hoặc chấm dứt hợp đồng.		

A.7.3.1	Chấm dứt hoặc thay đổi trách nhiệm công việc	*Kiểm soát* Trách nhiệm bảo vệ thông tin và nhiệm vụ mà vẫn có hiệu lực hoặc thay đổi việc làm phải được xác định, thông báo đến nhân viên hoặc nhà thầu và yêu cầu tuân theo.
A.8 Quản lý tài sản		
A.8.1 Trách nhiệm đối với tài sản		
Mục tiêu: Để xác định tài sản của tổ chức và xác định trách nhiệm bảo vệ phù hợp.		
A.8.1.1	Kiểm kê tài sản	*Kiểm soát* Những tài sản liên quan đến thông tin và cơ sở hạ tầng thông tin phải được xác định và một bản kiểm kê tài sản phải được vẽ lại và bảo quản.
A.8.1.2	Quyền sở hữu tài sản	*Kiểm soát* Tài sản được duy trì trong kiểm kê phải được sở hữu.
A.8.1.3	Chấp nhận sử dụng tài sản	*Kiểm soát* Quy tắc cho chấp nhận sử dụng thông tin và những tài sản liên quan với cơ sở xử lý thông tin phải được xác định, dẫn chứng bằng tài liệu và thực hiện.
A 8.1.4	Trả lại tài sản	*Kiểm soát* Tất cả nhân viên và những người dùng bên ngoài phải trả lại tất cả tài sản của tổ chức mà họ sở hữu khi chấm dứt hợp đồng, việc làm hoặc thỏa thuận của họ.
A.8.2 Phân loại thông tin		
Mục tiêu: Để đảm bảo rằng thông tin nhận được một mức độ bảo vệ phù hợp trong mọi trường hợp với tầm quan trọng của nó đối với tổ chức		
A.8.2.1	Phân loại thông tin	*Kiểm soát* Thông tin phải được phân loại dựa trên giá trị của

		nó, những yêu cầu hợp pháp, độ nhạy cảm tiết lộ trái phép và sửa đổi.
A.8.2.2	Nhãn của thông tin	*Kiểm soát* Một thiết lập thích hợp của quy trình cho nhãn thông tin phải được phát triển và thực hiện trong mọi trường hợp với sơ đồ phân loại thông tin thông qua bởi tổ chức
A.8.2.3	Xử lý tài sản	*Kiểm soát* Quy trình cho xử lý tài sản phải được phát triển và thực hiện trong mọi trường hợp với sơ đồ phân loại thông tin bởi tổ chức.
A.8.3 Xử lý phương tiện truyền thông		
Mục tiêu: Để tránh truy cập trái phép, thay đổi, xóa hoặc phá hủy các thông tin được lưu trữ trên truyền thông.		
A.8.3.1	Quản lý thay thế được truyền thông	*Kiểm soát* Những quy trình phải được thực hiện để quản lý truyền thông trong mọi trường hợp với sơ đồ phân loại thông tin bởi tổ chức.
A.8.3.2	Xử lý truyền thông	*Kiểm soát* Truyền thông được xử lý một cách an toàn khi không còn cần thiết, sử dụng các quy trình chính thức.
A.8.3.3	Xử lý truyền thông vật lý	*Kiểm soát* Truyền thông chứa thông tin phải được bảo vệ chống lại truy cập trái phép, lạm dụng hoặc hư hỏng trong quá trình truyền dẫn.
A.9 Kiểm soát truy cập		
A.9.1 Kiểm soát truy cập những yêu cầu giao dịch		
Mục tiêu: Để truy cập giới hạn đến thông tin và cơ sở xử lý thông tin		

A.9.1.1	Chính sách kiểm soát truy cập	*Kiểm soát* Một chính sách kiểm soát truy cập phải được thiết lập, dẫn chứng bằng tài liệu và xem xét dựa trên giao dịch và yêu cầu an toàn thông tin.
A.9.1.2	Truy cập đến mạng và dịch vụ mạng	*Kiểm soát* Người sử dụng chỉ được quyền truy cập đến mạng và dịch vụ mạng mà họ đã được ủy quyền đặc biệt để sử dụng.
A.9.2 Quản lý truy cập người sử dụng		
Mục tiêu: Để đảm bảo cho phép người sử dụng truy cập và ngăn chặn trái phép vào hệ thống và dịch vụ		
A.9.2.1	Người sử dụng đăng ký và hủy đăng ký	*Kiểm soát* Một quy trình chính thức đăng ký và xóa đăng ký người sử dụng phải được thực hiện để cho phép gán quyền truy cập
A.9.2.2	Người sử dụng truy cập dữ liệu	*Kiểm soát* Một người sử dụng chính thức truy cập quy trình phải được thực hiện để gán hoặc hủy bỏ quyền truy cập cho tất cả các loại người sử dụng đến tất cả những hệ thống và những dịch vụ.
A.9.2.3	Quản lý quyền truy cập đặc quyền.	*Kiểm soát* Cấp phát và sử dụng quyền truy cập đặc quyền phải được hạn chế và kiểm soát.
A.9.2.4	Quản lý an toàn thông tin cho người sử dụng	*Kiểm soát* Phân bổ thông tin xác thực an toàn phải được kiểm soát thông qua một quy trình quản lý chính thức.
Â.9.2.5	Xem xét truy cập người sử dụng	*Kiểm soát* Chủ tài sản phải thường xuyên xem xét quyền truy cập của người sử dụng

A.9.2.6	Hủy bỏ hoặc điều chỉnh quyền truy cập	*Kiểm soát* Quyền truy cập của tất cả các nhân viên và những người sử dụng bên ngoài đến thông tin và cơ sở xử lý thông tin phải được hủy bỏ khi chấm dứt công việc, hợp đồng hoặc thỏa thuận, hoặc điều chỉnh khi thay đổi.
A.9.3 Trách nhiệm của người sử dụng		
Mục tiêu: Để làm cho người dùng có trách nhiệm đảm bảo an toàn thông tin xác thực của họ		
A.9.3.1	Sử dụng thông tin xác thực bảo mật	*Kiểm soát* Người sử dụng phải được yêu cầu để theo dõi hoạt động tổ chức trong sử dụng thông tin xác thực bảo mật
A.9.4 Kiểm soát truy cập hệ thống và ứng dụng		
Mục tiêu: Để ngăn chặn truy cập trái phép vào hệ thống và ứng dụng.		
A.9.4.1	Sự hạn chế truy cập thông tin	*Kiểm soát* Truy cập đến thông tin ứng dụng và hệ thống phải bị hạn chế trong mọi trường hợp với chính sách kiểm soát truy cập.
A.9.4.2	Thủ tục đăng nhập an toàn	*Kiểm soát* Nơi được yêu cầu bởi chính sách kiểm soát truy cập, truy cập đến hệ thống và ứng dụng phải được kiểm soát bởi thủ tục đăng nhập an toàn.
A.9.4.3	Hệ thống quản lý mật khẩu	*Kiểm soát* Hệ thống quản lý mật khẩu phải được tương tác và phải đảm bảo chất lượng mật khẩu
A.9.4.4	Sử dụng các chương trình tiện ích đặc quyền	*Kiểm soát* Sử dụng các chương trình tiện ích đó có thể là khả năng kiểm soát vượt qua hệ thống và ứng dụng phải

		được hạn chế và kiểm soát chặt chẽ
A.9.4.5	Truy cập kiểm soát đến mã nguồn chương trình	*Kiểm soát* Truy cập đến mã nguồn chương trình phải được hạn chế
A.10 Mã hóa		
A.10.1 Kiểm soát mã hóa		
Mục tiêu: Đảm bảo sử dụng mã hóa đúng và hiệu quả để bảo vệ tính an ninh, xác thực và/hoặc toàn vẹn của thông tin.		
A.10.1.1	Chính sách về sử dụng kiểm soát mã hóa	*Kiểm soát* Một chính sách về sử dụng kiểm soát mã hóa cho việc bảo vệ của thông tin phải được phát triển và thực hiện.
A.10.1.2	Quản lý khóa	*Kiểm soát* Một chính sách về sử dụng, bảo vệ và tuổi thọ của các khóa mã hóa phải được phát triển và thực hiện thông qua chu kỳ sống của chúng
A.11 An toàn vật lý và môi trường		
A.11.1 Phạm vi an toàn		
Mục tiêu: Để tránh truy cập vật lý trái phép, thiệt hại và can dự vào thông tin và cơ sở xử lý thông tin của tổ chức.		
A.11.1.1	Chu vi an ninh vật lý	*Kiểm soát* Chu vi an ninh phải được xác định và sử dụng để bảo vệ các phạm vi chứa hoặc thông tin chính xác hoặc thông tin phê bình và cơ sở xử lý thông tin
A.11.1.2	Kiểm soát lối vào vật lý	*Kiểm soát* Phạm vi an toàn phải được bảo vệ bởi kiếm soát lối vào thích hợp để đảm bảo rằng chỉ cá nhân được ủy quyền được cho phép truy cập.

A.11.1.3	Đảm bảo các văn phòng, các phòng và các thiết bị	*Kiểm soát* Bảo vệ vật lý cho các văn phòng, các phòng và các thiết bị phải được thiết kế và ứng dụng
A.11.1.4	Bảo vệ chống lại các mối đe dọa từ bên ngoài và môi trường	*Kiểm soát* Bảo vệ vật lý chống lại thiên tai, cuộc tấn công hoặc tai nạn độc hại phải được thiết kế và áp dụng.
A.11.1.5	Làm việc trong phạm vi an toàn	*Kiểm soát* Quy trình làm việc trong phạm vi an toàn phải được thiết kế và áp dụng.
A.11.1.6	Khu vực chứa hàng và phân phối	*Kiểm soát* Truy cập những điểm như là phân phối và khu vực chứa hàng và những điểm khác nơi người không có quyền có thể xâm nhập phải được kiểm soát và, nếu có thể, bị cô lập từ cơ sở xử lý thông tin để tránh truy cập trái phép.
A.11.2 Thiết bị		
Mục tiêu: Ngăn chặn sự mất mát, thiệt hại, trộm cắp hoặc thỏa hiệp và sự gián đoạn hoạt động của tổ chức.		
A.11.2.1	Sự chọn địa điểm và sự bảo vệ thiết bị	*Kiểm soát* Thiết bị phải được chọn địa điểm và bảo vệ để giảm bớt rủi ro từ mối đe dọa và những nguy hiểm từ môi trường, và những cơ hội truy cập trái phép.
A.11.2.2	Hỗ trợ các tiện ích	*Kiểm soát* Thiết bị phải được bảo vệ khi mất điện và gián đoạn khác gây ra bởi sự thiếu sót trong các tiện ích hỗ trợ
A.11.2.3	Sự đặt cáp bảo an toàn	*Kiểm soát* Cáp viễn thông mang dữ liệu hoặc hỗ trợ các dịch vụ thông tin được bảo vệ từ sự nghe trộm, nhiễu hoặc hư hỏng.

A.11.2.4	Bảo trì thiết bị	*Kiểm soát* Thiết bị phải được duy trì đúng để đảm bảo luôn tiện lợi và có sẵn.
A.11.2.5	Hủy bỏ tài sản	*Kiểm soát* Thiết bị, thông tin hoặc phần mềm không được thực hiện bên ngoài mà không có sự cho phép trước
A.11.2.6	Bảo vệ thiết bị và những tài sản ra khỏi chỗ	*Kiểm soát* Bảo vệ phải được áp dụng đối với tài sản bên ngoài có tính đến rủi ro khác nhau làm việc bên ngoài cơ sở tổ chức
A.11.2.7	Hủy bỏ an toàn hoặc tái sử dụng thiết bị	*Kiểm soát* Tất cả các hạng mục của thiết bị chứa phương tiện ghi lưu trữ phải được kiểm tra để đảm bảo bất cứ dữ liệu nhạy cảm và phần mềm bản quyền được xóa hoặc ghi đè an toàn trước khi xóa hoặc tái sử dụng
A.11.2.8	Thiết bị người dùng không giám sát	*Kiểm soát* Người sử dụng phải đảm bảo rằng thiết bị không giám sát có sự bảo vệ thích hợp.
A.11.2.9	Chính sách bàn làm việc sạch và màn hình máy tính sạch.	*Kiểm soát* Một chính sách bàn làm việc sạch với những giấy tờ và xóa phương tiện ghi lưu trữ và chính sách màn hình máy tính sạch cho cơ sở xử lý thông tin phải được thừa nhận.
A.12 Bảo vệ quá trình hoạt động		
A.12.1 Quy trình hoạt động và trách nhiệm		
Mục tiêu: Để đảm bảo đúng và sử dụng an toàn của cơ sở xử lý thông tin		
A.12.1.1	Cung cấp tư liệu vận hành các quy trình	*Kiểm soát* Vận hành quy trình phải được cung cấp và làm sẵn cho tất cả những người sử dụng cần đến chúng.

A.12.1.2	Quản lý thay đổi	*Kiểm soát* Thay đổi tổ chức, quy trình doanh nghiệp, cơ sở xử lý thông tin và hệ thống an toàn thông tin hiệu quả phải được kiểm soát.
A.12.1.3	Quản lý năng lực	*Kiểm soát* Sử dụng tài nguyên phải được theo dõi, điều chỉnh và phản chiếu được yêu cầu năng lực tương lai để đảm bảo yêu cầu thực thi hệ thống.
A.12.1.4	Sự tách phát triển, thử nghiệm và môi trường hoạt động	*Kiểm soát* Phát triển, thử nghiệm, và môi trường hoạt động phải được tách ra để giảm rủi ro của truy cập trái phép hoặc thay đổi đến môi trường hoạt động.
A.12.2 Bảo vệ khỏi phần mềm độc hại		
Mục tiêu: Để đảm bảo rằng thông tin và cơ sở xử lý thông tin được bảo vệ chống lại phần mềm độc hại		
A.12.2.1	Kiểm soát chống lại phần mềm độc hại	*Kiểm soát* Kiểm soát phát hiện, phòng ngừa và phục hồi để bảo vệ chống lại phần mềm độc hại phải được thực hiện, kết hợp với nhận thức đúng đắn của người sử dụng.
A.12.3 Sao lưu		
Mục tiêu: Để bảo vệ chống mất mát dữ liệu		
A.12.3.1	Sao lưu thông tin	*Kiểm soát* Các bản sao lưu thông tin, phần mềm và ảnh hệ thống phải được thực hiện và kiểm tra thường xuyên trong mọi trường hợp với một chính sách sao lưu thích hợp.
A.12.4 Đăng nhập và kiểm soát		
Mục tiêu: Ghi các sự kiện và sinh ra bằng chứng		

A.12.4.1	Sự kiện đăng nhập	*Kiểm soát* Sự kiện đăng nhập ghi lại hoạt động của người sử dụng, ngoại lệ, khuyết điểm và sự kiện bảo vệ thông tin phải được sinh ra, lưu giữ và xem xét thường xuyên.
A.12.4.2	Bảo vệ thông tin đăng nhập	*Kiểm soát* Phương tiện đăng nhập và thông tin đăng nhập phải được bảo vệ chống lại can thiệp và truy cập trái phép.
A.12.4.3	Người quản trị và người vận hành đăng nhập	*Kiểm soát* Quản trị hệ thống và hoạt động điều hành hệ thống phải được đăng nhập và bảo vệ đăng nhập và xem xét thường xuyên.
A.12.4.4	Khóa đồng bộ	*Kiểm soát* Khóa của tất cả hệ thống xử lý thông tin liên quan giữa tổ chức hoặc miền an toàn phải được đồng bộ đế tham chiếu đến nguồn thời gian riêng lẻ.
A.12.5 Kiểm soát phần mềm hoạt động		
Mục tiêu: Để đảm bảo tính toàn vẹn của hệ thống hoạt động.		
A.12.5.1	Cài đặt phần mềm trên hệ thống hoạt động	*Kiểm soát* Thủ tục phải được thực thi để kiểm soát cài đặt phần mềm trên hệ thống hoạt động.
A.12.6 Quản lý lỗ hổng kỹ thuật		
Mục tiêu: Để tránh khai thác lỗ hổng kỹ thuật		
A.12.6.1	Quản lý lỗ hổng kỹ thuật	*Kiểm soát* Thông tin về lỗ hổng kỹ thuật của hệ thống thông tin được sử dụng phải có kịp thời, sự khẳng định của tổ chức để đánh giá lỗ hổng và các phép đo thích hợp thực hiện để liên kết các rủi ro.

A.12.6.2	Hạn chế cài đặt phần mềm	*Kiểm soát* Quy tắc điều hành cài đặt của phần mềm bởi người sử dụng phải được thiết lập và thực thi.
A.12.7 Xem xét đánh giá hệ thống thông tin		
Mục tiêu: Giảm đến mức tối thiểu tác động của hoạt động đánh giá trên hệ thống hoạt động.		
A.12.7.1	Kiểm soát đánh giá hệ thống thông tin	*Kiểm soát* Những yêu cầu đánh giá và những hoạt động bao gồm xác thực hoạt động hệ thống phải lập kế hoạch cẩn thận và phù hợp để giảm đến mức tối hiểu sự gián đoạn đến quá trình kinh doanh.
A.13 An ninh truyền thông		
A.13.1 Quản lý an ninh mạng		
Mục tiêu: Để đảm bảo an ninh thông tin trong mạng và cơ sở xử lý hỗ trợ thông tin		
A.13.1.1	Kiểm soát mạng	*Kiểm soát* Mạng phải được quản lý và kiểm soát để bảo vệ thông tin trong hệ thống và ứng dụng
A.13.1.2	Bảo vệ dịch vụ mạng	*Kiểm soát* Cơ chế bảo vệ, mức độ dịch vụ và yêu cầu quản lý của tất cả dịch vụ mạng phải được xác định và bao gồm trong thỏa thuận dịch vụ mạng, cho dù các dịch vụ này được cung cấp trong nhà hoặc thuê ngoài.
A.13.1.3	Sự chia ra trong mạng	*Kiểm soát* Nhóm thông tin dịch vụ, người sử dụng và hệ thống thông tin phải được chia ra trên mạng.
A.13.2 Sự truyền thông tin		
Mục tiêu: Để duy trì sự an toàn của thông tin được truyền giữa một tổ chức và với bất kỳ thực thể bên ngoài.		

A.13.2.1	Thủ tục và chính sách truyền thông tin	*Kiểm soát* Hình thức truyền chính sách, thủ tục và kiểm soát phải được thực hiện để bảo vệ sự truyền thông tin thông qua sử dụng của tất cả các loại cơ sở truyền thông
A.13.2.2	Sự thỏa thuận trên sự truyền thông tin	*Kiểm soát* Sự thỏa thuận phải được truyền an toàn của thông tin doanh nghiệp giữa tổ chức và các bên liên quan
A.13.2.3	Tin nhắn điện tử	*Kiểm soát* Thông tin liên quan đến tin nhắn điện tử được bảo vệ một cách thích hợp.
A.13.2.4	Thỏa thuận bí mật hoặc không tiết lộ	*Kiểm soát* Yêu cầu cho bí mật hoặc thỏa thuận không tiết lộ phản ánh nhu cầu của tổ chức cho việc bảo vệ thông tin phải được xác định, kiểm soát và dẫn chứng thường xuyên
A.14.2 Tiếp nhận hệ thống, phát triển và bảo trì		
Mục tiêu: Để đảm bảo rằng an ninh thông tin được thiết kế và thực thi trong chu trình phát triển của hệ thống		
A.14.2.1	Chính sách phát triển an toàn	*Kiểm soát* Những quy tắc cho sự phát triển của phần mềm và hệ thống phải được thiết lập và ứng dụng để phát triển trong tổ chức
A.14.2.2	Thủ tục kiểm soát hệ thống thay đổi	*Kiểm soát* Thay đổi hệ thống trong chu trình phải triển phải được kiểm soát bởi sử dụng thủ tục kiểm soát thay đổi chính thức.
A.14.2.3	Xem xét công nghệ của ứng dụng sau khi thay	*Kiểm soát* Khi nền tảng hoạt động thay đổi, ứng dụng tiêu chí doanh nghiệp phải được xem xét và kiểm tra để đảm

	đổi nền tảng hoạt động	bảo không có ảnh hưởng bất lợi đến an ninh hoặc hoạt động của tổ chức
A.14.2.4	Sự hạn chế thay đổi gói phần mềm	*Kiểm soát* Thay đổi đến gói phần mềm phải được khuyến khích, giới hạn những thay đổi cần thiết và tất cả những thay đổi phải được kiểm soát một cách chặt chẽ.
A.14.2.5	Nguyên tắc an toàn hệ thống kỹ thuật	*Kiểm soát* Nguyên tắc cho kỹ thuật an toàn hệ thống phải được thiết lập, dẫn chứng, duy trì và áp dụng cho bất cứ hệ thống thông tin thực thi hiệu quả.
A.14.2.6	Môi trường phát triển an toàn	*Kiểm soát* Tổ chức phải thiết lập và bảo vệ an toàn môi trường phát triển cho phát triển hệ thống và tích hợp lực bao gồm nguyên vòng đời phát triển hệ thống
A.14.2.7	Phát triển thuê ngoài	*Kiểm soát* Tổ chức phải giám sát và theo dõi hoạt động của phát triển hệ thống thuê ngoài
A.14.2.8	Kiểm tra hệ thống an ninh	*Kiểm soát* Kiểm tra chức năng an toàn phải được tiến hành trong phát triển
A.14.2.9	Kiểm tra chấp nhận hệ thống	*Kiểm soát* Chấp nhận kiểm tra chương trình và tiêu chuẩn liên quan phải được thiết lập cho những hệ thống thông tin mới, nâng cấp và những phiên bản mới.
A.14.3 Kiểm tra dữ liệu		
Mục tiêu: Để đảm bảo dữ liệu được sử dụng cho việc kiểm tra		
A.14.3.1	Bảo vệ dữ liệu kiểm tra	*Kiểm soát* Dữ liệu kiểm tra phải được lựa chọn cẩn thận, được

		bảo vệ và kiểm soát
A.15 Mối quan hệ với nhà cung ứng		
A.15.1 Bảo vệ thông tin trong mối quan hệ với nhà cung ứng		
Mục tiêu: Để đảm bảo bảo vệ tài sản của tổ chức đó có thể truy cập bởi nhà cung ứng		
A.15.1.1	Chính sách an toàn thông tin cho mối quan hệ với nhà cung ứng	*Kiểm soát* An toàn thông tin yêu cầu giảm nhẹ liên kết rủi ro với truy cập của nhà cung ứng đến tài sản của tổ chức phải được dẫn chứng và thỏa thuận với nhà cung ứng.
A.15.1.2	Địa chỉ hóa an toàn trong phạm vi thỏa thuận với nhà cung ứng	*Kiểm soát* Tất cả các yêu cầu an ninh thông tin liên quan phải được thiết lập và thỏa thuận với mỗi bên cung ứng để có thể truy cập, xử lý, lưu trữ, giao tiếp, hoặc cung cấp cho thành phần cơ sở hạ tầng IP cho thông tin của tổ chức.
A.15.1.3	Thông tin và kênh cung ứng công nghệ truyền thông	*Kiểm soát* Thỏa thuận với những nhà cung ứng phải bao gồm những yêu cầu để giải quyết liên kết rủi ro an toàn thông tin với thông tin và dịch vụ công nghệ truyền thông và kênh cung cấp sản phẩm.
A.15.2 Quản lý phân phối nhà cung cấp dịch vụ		
Mục tiêu: Để duy trì một mức độ thỏa thuận an toàn thông tin và cung cấp dịch vụ phù hợp với các thỏa thuận cung cấp		
A.15.2.1	Giám sát và xem xét dịch vụ cung ứng	*Kiểm soát* Tổ chức phải giám sát, xem xét và đánh giá sự phân phối dịch vụ cung ứng một cách thường xuyên.
A.15.2.2	Quản lý thay đổi đến nhà cung cấp dịch vụ	*Kiểm soát* Thay đổi sự cung cấp dịch vụ bởi nhà cung ứng, bao gồm duy trì và cải tiến chính sách an ninh thông tin

		đang tồn tại, quy trình và sự kiểm soát phải được quản lý, có tính quan trọng của các thông tin kinh doanh, bao gồm hệ thống và quy trình và đánh giá lại rủi ro.
A.16 Quản lý sự cố an toàn thông tin		
A.16.1 Quản lý sự cố an toàn thông tin và cải tiến		
Mục tiêu: Để đảm bảo phương pháp tiếp cận hiệu quả và nhất quán để quản lý sự cố an toàn thông tin, bao gồm truyền thông về sự kiện an toàn và khuyết điểm		
A.16.1.1	Thủ tục và trách nhiệm	*Kiểm soát* Trách nhiệm và thủ tục quản lý phải được thiết lập để đảm bảo nhanh, hiệu quả và phản hồi có thứ tự đến sự cố an ninh thông tin.
A.16.1.2	Báo cáo sự cố an ninh thông tin	*Kiểm soát* Sự cố an ninh thông tin phải được báo cáo thông qua các kênh thích hợp một cách nhanh nhất có thể.
A.16.1.3	Báo cáo khuyết điểm an ninh thông tin	*Kiểm soát* Nhân viên và nhà thầu sử dụng hệ thống và dịch vụ hệ thống thông tin của tổ chức phải được yêu cầu để chú ý và báo cáo bất cứ khuyết điểm an ninh thông tin đã được tìm ra hoặc quan sát được trong hệ thống và dịch vụ.
A.16.1.4	Đánh giá và quyết định sự kiện an toàn thông tin	*Kiểm soát* Sự kiện an toàn thông tin phải được đánh giá và nó phải được quyết định nếu chúng đã được phân loại như những sự cố an toàn thông tin.
A.16.1.5	Phản hồi từ sự cố an ninh thông tin	*Kiểm soát* Sự cố an ninh thông tin phải được phản hồi trong mọi trường hợp với thủ tục dẫn chứng bằng tư liệu.
A.16.1.6	Học từ những sự cố an toàn thông	*Kiểm soát* Kiến thức thu được từ phân tích và giải quyết sự cố

	tin	an ninh thông tin phải được giảm khả năng hoặc tác động của sự cố trong tương lai.
A.16.1.7	Tập hợp đánh giá	*Kiểm soát* Tổ chức phải xác định và áp dụng các quy trình cho việc xác định, lựa chọn, mua và bảo quản thông tin, có thể phục vụ như là bằng chứng.
A.17 Hướng bảo vệ thông tin của quản lý doanh nghiệp liên tục		
A.17.1 Bảo vệ thông tin liên tục		
Mục tiêu: Bảo vệ thông tin liên tục phải được nhúng vào hệ thống quản lý liên tục doanh nghiệp tổ chức.		
A.17.1.1	Kế hoạch bảo vệ thông tin liên tục	*Kiểm soát* Tổ chức phải xác định được yêu cầu cho bảo vệ thông tin và tiếp tục quản lý bảo vệ thông tin trong tình hình bất lợi, ví dụ trong một cuộc khủng hoảng hay thiên tai.
A.17.1.2	Thực thi bảo vệ thông tin liên tục	*Kiểm soát* Tổ chức phải thiết lập, dẫn chứng, thực hiện và duy trì quy trình, thủ tục và kiểm soát mức độ cần thiết của tính liên tục cho an ninh thông tin trong một tình huống bất lợi.
A.17.1.3	Kiểm chứng, xem xét và đánh giá tính liên tục bảo vệ thông tin	*Kiểm soát* Tổ chức phải kiểm chứng thiết lập và thực hiện kiểm soát tính liên tục an ninh thông tin một cách thường xuyên theo thứ tự để đảm bảo chúng hợp lệ và hiệu quả trong những tình huống bất lợi.
A.18 Sự tuân thủ		
A.18.1 Tuân thủ pháp lý và yêu cầu hợp đồng		
Mục tiêu: Để tránh vi phạm luật pháp, pháp định, điều chỉnh hoặc mối liên quan ràng buộc hợp đồng đến an toàn thông tin của bất cứ yêu cầu an ninh nào.		

A.18.1.1	Phân biệt điều lệ áp dụng và những yêu cầu ràng buộc hợp đồng	*Kiểm soát* Tất cả luật định, quy định, yêu cầu hợp đồng có liên quan và cách tiếp cận của tổ chức để đáp ứng những yêu cầu đó phải được xác định rõ ràng, dẫn chứng bằng tài liệu và lưu giữ đến ngày cho mỗi hệ thống thông tin và tổ chức.
A.18.1.2	Quyền sở hữu trí tuệ	*Kiểm soát* Thủ tục thích hợp phải được thực hiện để đảm bảo phù hợp với luật định, quy định và những yêu cầu hợp đồng có liên quan đến quyền sở hữu trí tuệ và sử dụng sản phẩm phần mềm độc quyền.
A.18.1.3	Sự bảo vệ các hồ sơ	*Kiểm soát* Các hồ sơ phải được bảo vệ khỏi tổn thất, sự phá hoại, sự giả mạo, truy cập trái phép và phát hành trái phép, trong mọi trường hợp với quy định, luật định, những yêu cầu hợp đồng và doanh nghiệp.
A.18.1.4	Sự riêng biệt và bảo vệ thông tin cá nhân	*Kiểm soát* Sự riêng biệt và bảo vệ thông tin cá nhân phải đảm bảo được cũng như yêu cầu luật định và quy định liên quan nơi áp dụng được.
A.18.1.5	Quy định kiểm soát mật mã	*Kiểm soát* Kiểm soát mật mã phải được sử dụng phù hợp với tất cả hợp đồng, quy tắc và những quy định liên quan.
A.18.2 Xem xét an toànthông tin		
Mục tiêu: Để đảm bảo rằng an toàn thông tin được thực thi và vận hành trong mọi trường hợp với chính sách và quy trình của tổ chức.		
A.18.2.1	Độc lập xem xét an toàn thông tin	*Kiểm soát* Cách tiếp cận của tổ chức để quản lý an toàn thông tin và thực hiện nó (ví dụ: kiểm soát mục tiêu, điều khiển, chính sách, quá trình và quy trình cho an ninh thông tin) phải được xem xét độc lập theo kế hoạch

		hoặc khi thay đổi xảy ra đáng kể.
A.18.2.2	Phù hợp với chính sách và tiêu chuẩn an ninh	*Kiểm soát* Những người quản lý phải được xem xét sự phù hợp của quá trình và quy trình thông tin một cách thường xuyên trong phạm vi trách nhiệm của họ với chính sách, tiêu chuẩn an ninh thích hợp và bất cứ yêu cầu an ninh khác.
A.18.2.3	Xem xét phù hợp với kỹ thuật	*Kiểm soát* Hệ thống thông tin phải được xem xét thường xuyên cho phù hợp với chính sách và tiêu chuẩn an toàn thông tin của tổ chức.

2.3. Mười lý do để chứng nhận ISO 27001[4]

Thông tin đúng: Có được thông tin đúng là yếu tố sống còn của bất kỳ tổ chức hay doanh nghiệp nào. Tuy nhiên, việc nắm bắt được và kiểm soát thông tin đúng thường khó và không bền vững. Do vậy, ISO 27001 sẽ giúp các tổ chức hay doanh nghiệp quản lý thông tin của mình một cách hiệu quả hơn.

Thúc đẩy quan hệ đối tác: Các tổ chức hay doanh nghiệp ngày càng ý thức được việc thiếu kiểm soát của mình, đặc biệt là công tác thông tin tới nhà cung cấp và khách hàng của mình. Do đó, họ đang tìm kiếm các quy tắc và sự tin tưởng nhờ hệ thống đánh giá theo tiêu chuẩn ISO 27001 đem lại.

Cắt giảm chi phí trong chuỗi cung ứng: ISO 27001 được coi như sáng kiến giúp giảm thiểu các hoạt động trùng lặp của công ty hay doanh nghiệp bạn, chẳng hạn như kiểm tra lượng hàng nhập vào và xuất ra. Tiêu chuẩn này cũng được coi là sáng kiến nhằm giảm dữ liệu đầu vào cho doanh nghiệp.

Không đơn thuần về an ninh thông tin: Ngoài đảm bảo an ninh thông tin, ISO 27001 còn cung cấp các giải pháp quản lý bảo mật, tính toàn vẹn và sẵn có của thông tin. Đồng nghĩa với đó là hỗ trợ quản lý rủi ro cho các tổ chức doanh nghiệp.

Hoạt động trên quy trình và hệ thống nhất quán: ISO 27001 giúp huy động các nguồn lực then chốt nhằm đề ra các hành động cần thiết để giảm thiểu sự cố thông tin và quản lý rủi ro thông tin cho các tổ chức doanh nghiệp.

Không chỉ riêng bộ phận CNTT: Trước kia, ISO 27001 được biết đến là tiêu chuẩn đánh giá trong lĩnh vực công nghệ thông tin (CNTT). Tuy nhiên, hiện nay tiêu chuẩn

[4]http://acsregistrars.vn/top-10-ly-do-de-chung-nhan-iso-27001

này đã được mở rộng và bao quát toàn bộ tổ chức hay doanh nghiệp từ nhân viên vệ sinh đến giám đốc điều hành.

Được đánh giá bởi Tổ chức chứng nhận được công nhận Quốc tế (ví dụ như Tổ chức Công nhận Vương quốc Anh - UKAS). Điều này không chỉ đảm bảo cho công ty hay doanh nghiệp bạn duy trì và cải tiến hoạt động của mình mà còn giúp xác định năng lực và tìm kiếm các cơ hội hợp tác.

Tăng khả năng trúng thầu và cơ hội ký kết hợp đồng: Khách hàng thường bị hạn chế về nguồn lực để tìm hiểu các đối tác hay nhà cung cấp của mình. Thông thường họ sử dụng ISO 27001 và các tiêu chuẩn quản lý khác làm thước đo xác định xem tổ chức hay doanh nghiệp bạn có phải là đối tác tin cậy hay không để từ đó tiếp tục xem xét hồ sơ bỏ thầu của doanh nghiệp bạn.

Cải thiện lợi nhuận: Các sự cố và vụ việc nghiêm trọng như sự cố đều khiến tổ chức hay doanh nghiệp bạn lãng phí thời gian và tiền bạc. Do vậy, điều quan trọng là làm thể nào xác định được các sự cố và rủi ro tiềm ẩn và triển khai hành động phòng ngừa sự cố đó. Sẽ không ngạc nhiên nếu tổ chức hay doanh nghiệp bạn phải bỏ thời gian và tiền bạc để khắc phục các sự cố an ninh thông tin mà nguyên nhân là không chủ động xác định các sự cố và rủi ro tiềm ẩn. Trên cơ sở đó, ISO 27001 hướng tới giúp các doanh nghiệp đảm bảo thông tin đúng được cung cấp đúng chỗ, đúng lúc và đúng người.

Liên tục cải tiến: Môi trường kinh doanh hiện đang không ngừng thay đổi. Do vậy, các tổ chức hay doanh nghiệp cũng cần phải cải tiến và thay đổi để phù hợp với xu thế. Để tăng tính hiệu quả cho các doanh nghiệp, ISO 27001 hỗ trợ họ giám sát các chỉ số quan trọng của mình và đưa ra quyết định và hành động phù hợp với thực tế.

2.4. Thực trạng và triển vọng phát triển ISO 27001[5]

2.4.1. Thực trạng triển khai tại Việt Nam

Từ năm 2006, nhiều tổ chức, cơ quan ở Việt Nam đã quan tâm đến ISO 27001, có thể thấy điều đó qua một số sự kiện sau:

Tháng 2/2006: Tổng cục Tiêu chuẩn Đo lường Chất lượng Việt Nam đã ban hành tiêu chuẩn TCVN 7562:2005 – Công nghệ thông tin – Mã thực hành quản lý an toàn thông tin, (tương đương với tiêu chuẩn ISO/IEC 17799: 2000). Tiêu chuẩn này đề ra các hướng dẫn thực hiện hệ thống quản lý an ninh thông tin làm cơ sở cho ISO 27001.

Tháng 1/2007: Công ty CSC Việt Nam (Computer Sciences Corporation) đã trở thành đơn vị đầu tiên có được chứng nhận ISO 27001.

[5]http://antoanthongtin.vn/QualityDetail.aspx?CatID=5a918474-446c-47ca-8e21-a889bc2c8fd3&NewsID=969464bf-2206-43e5-9d02-72ce68dd64d7

Tháng 3/2007: Công ty Hệ thống Thông tin FPT (FPT-IS) đạt được chứng nhận ISO 27001.

Tháng 11/2007: Giáo sư Ted Humphreys, người được coi là "cha đẻ" của ISO 27001 đã đến Việt Nam tham dự hội thảo "Quản lý bảo mật thông tin" do 2 công ty TUVRheinland và ECCI (Philippines) phối hợp tổ chức.

Đồng thời, một số đơn vị cung cấp dịch vụ tư vấn và cấp chứng nhận ISO 27001 đã có mặt tại Việt Nam như: BVC, TUV SUD, TUV NORD và TUVRheinland. Đến nay ở Việt Nam có 5 đơn vị (CSC Vietnam, FPT IS, FPT Soft, GHP FarEast, ISB Corporation Vietnam…) đã đạt chứng nhận ISO 27001 và hơn 10 đơn vị (HPT Soft, VietUnion, Quantic…) đang trong quá trình triển khai ứng dụng tiêu chuẩn này.

Qua các số liệu nêu trên có thể thấy, hầu hết các đơn vị, doanh nghiệp đã và đang áp dụng ISO 27001 đều có vốn đầu tư hoặc có đối tác chính là các công ty nước ngoài. Một trong những nguyên nhân chính thúc đẩy các doanh nghiệp này thực hiện và áp dụng ISO 27001 là yêu cầu bắt buộc từ phía công ty chính hãng, đối tác khách hàng nước ngoài, là những nơi đã thực hiện và áp dụng ISO 27001.

Cũng qua số liệu này, chúng ta có thể thấy số đơn vị đạt chứng nhận ISO 27001 tại Việt Nam khá khiêm tốn so với Nhật Bản (2668 chứng nhận), Trung Quốc (100 chứng nhận), Philippines (10 chứng nhận) và Thái Lan (9 chứng nhận). Một trong những nguyên nhân của tình trạng này là chi phí để đạt chứng nhận ISO 27001 khá cao, bao gồm các chi phí về tư vấn, cấp chứng nhận và đặc biệt là chi phí doanh nghiệp phải bỏ ra để thực hiện các biện pháp kiểm soát rủi ro. Chi phí cho áp dụng ISO 27001 ước lớn gấp khoảng 2 - 3 lần so với thực hiện ISO 9000. Bên cạnh đó, trình độ về CNTT, nhận thức về an ninh thông tin của người sử dụng chưa cao cũng gây những trở ngại, khó khăn khi triển khai ISO 27001. Tuy nhiên, đối với những doanh nghiệp, đơn vị mà nguồn lực tài chính chưa đủ để tiến hành áp dụng ISO 27001 trong phạm vi rộng thì có thể thực hiện triển khai áp dụng từng bước với phạm vi mở rộng dần, với một lộ trình hợp lý. Ngoài ra, có một lựa chọn cho nhiều doanh nghiệp để giảm chi phí là tự áp dụng ISO 27001 nhưng không tiến hành xin đánh giá cấp chứng nhận.

2.4.2. Triển vọng phát triển ISO 27001 tại Việt Nam

Theo đánh giá của một số chuyên gia, triển vọng áp dụng ISO 27001 tại Việt Nam là khá cao. ISO 27001 đã được các cơ quan chuyên trách của chính phủ (Tổng cục Tiêu chuẩn Đo lường chất lượng, Bộ Thông tin và Truyền thông…) khuyến cáo áp dụng rộng rãi trong cả nước. Ngoài ra, yêu cầu về đảm bảo an ninh thông tin của khách hàng, đối tác cũng ngày một cao hơn, đòi hỏi các tổ chức, doanh nghiệp phải áp dụng ISO 27001 để tăng cường sức cạnh tranh và nâng cao thương hiệu cho chính mình. Trong thời gian tới đây, ISO 27001 sẽ thu hút được sự quan tâm của các doanh nghiệp,

tổ chức thuộc lĩnh vực tài chính (ngân hàng, chứng khoán, bảo hiểm) và các tổ chức, cơ quan Nhà nước trong lĩnh vực quốc phòng, an ninh. ISO 27001 được kỳ vọng sẽ tạo được sự quan tâm như ISO 9000 trong thập niên 90.

Chương 3. XÂY DỰNG HỆ THỐNG QUẢN LÝ HỆ THỐNG AN TOÀN THÔNG TIN CHO DOANH NGHIỆP

3.1. PHÁT BIỂU BÀI TOÁN

Nhằm xây dựng một môi trường làm việc với hệ thống máy tính, thông tin được an toàn giúp cho việc khai thác thông tin hiệu quả thì cần phải hiểu rõ về các nguy cơ, điểm yếu của hệ thống. Hiểu rõ về nguy cơ giúp chúng ta cân bằng được giữa rủi ro đối với cơ hội, lợi ích tiềm năng của nó mang lại. Để thực hiện việc này được hiệu quả chúng ta bắt buộc phải tuân theo các giải pháp được nghiên cứu và xác lập như đánh giá hệ thống, tập trung vào việc đảm bảo an toàn thông tin. Là một nhân viên đảm bảo chất lượng của một công ty phát triển phần mềm. Hiểu được tầm quan trọng về việc xây dựng một hệ thống an toàn thông tin góp phần thúc đẩy sự phát triển và đảm bảo tài sản của công ty được an toàn. Sau đây tôi xin giới thiệu về chương trình quản lý hệ thống an toàn thông tin và một số tài liệu tôi đã viết dựa trên thực tiễn làm việc trong công ty để nhằm đảm bảo an toàn thông tin, hạn chế rủi ro, lỗ hổng của tài sản công ty có thể xảy ra.

Luận văn xây dựng hệ thống ISMS theo tiêu chuẩn ISO 27001:2013 nhằm thực hiện quản lý tài sản thông tin, quản lý rủi ro, các chính sách, quy định và quy trình để giảm thiểu rủi ro, đảm bảo an ninh thông tin và sự liên tục trong các hoạt động sản xuất kinh doanh của doanh nghiệp.

3.2. XÂY DỰNG CHƯƠNG TRÌNH

3.2.1. Phương pháp xác định rủi ro

Thực hiện việc xem xét phân tích rủi ro một cách chi tiết đối với tất cả những hệ thống thông tin của công ty. Công tác này bao gồm việc đánh giá và xác định tài sản, đánh giá những đe dọa tới tài sản và đánh giá những điểm yếu. Kết quả từ những hoạt động này sẽ được sử dụng để đánh giá những rủi ro và lựa chọn những phương pháp kiểm soát rủi ro. Việc phân tích rủi ro được thực hiện bằng phương pháp xem xét tài liệu quản lý an ninh thông tin hoặc phỏng vấn tại chỗ để thu thập thông tin. Nhóm an toàn bảo mật thông tin (ISMS) chịu trách nhiệm thiết lập danh sách đe dọa và điểm yếu. Danh sách này sẽ được phê duyệt bởi Ban lãnh đạo công ty trước khi đánh giá rủi ro.

Danh sách nguy cơ và điểm yếu sẽ bao gồm:

- Tất cả các nguy cơ và điểm yếu được xác định, xem xét bởi đội ngũ ISMS và được phê duyệt bởi Ban lãnh đạo Công ty.
- Danh sách sách này phải được rà soát định kỳ 6 tháng một lần bởi đội ISMS. Trong trường hợp có sự thay đổi thì phải được phê duyệt bởi Ban lãnh đạo Công ty.

Những tài sản có mức độ quan trọng thấp thì không cần phải đánh giá rủi ro.

Có 2 phương pháp để đánh giá rủi ro là đánh giá rủi ro định tính và định lượng[6]:

- Phương pháp đánh giá định lượng là việc gán một giá trị cụ thể tới các mất mát có thể xảy ra.
- Phương pháp đánh giá định tính đưa ra giá trị chưa xác định đối với việc mất mát dữ liệu chứ không chú trọng vào những thiệt hại về kinh tế đơn thuần.

Rủi ro là kết hợp của khả năng xảy ra rủi ro và ảnh hưởng của rủi ro. Khả năng xảy ra rủi ro cho biết xác suất một điểm yếu của thể bị khai thác trong nguy cơ. Ảnh hưởng của rủi ro thể hiện sự mất mát của Công ty từ một nguy cơ.

Mức độ ảnh hưởng = Nguy cơ * Điểm yếu[7]

Mức độ rủi ro đối với một tài sản thông tin thể hiện qua xác suất/tần suất và mức độ ảnh hưởng nếu sự việc diễn ra. Đánh giá mức độ rủi ro dựa theo công thức bên dưới:

Giá trị rủi ro = Xác suất xảy ra * Mức độ ảnh hưởng * Giá trị tài sản[8]

Để xác định giá trị rủi ro công ty cần phải xác định xác suất xảy ra, nguy cơ, điểm yếu, giá trị tài sản:

+ Giả sử định mức xác suất xảy ra: Rất cao 5; Cao 4; Trung bình 3; Thấp 2; Rất thấp 1.

+ Giả sử định mức cho các nguy cơ: Mức đặc biệt 5; mức cao 4; mức trung bình 3; mức thấp 2; mức rất thấp 1

+ Giả sử định mức cho các điểm yếu: Mức đặc biệt 5; mức cao 4; mức trung bình 3; mức thấp 2; mức rất thấp 1

+ Giả sử định mức giá trị tài sản từ 1-5 theo thuộc tính C, I, A

[6]https://dnasecurity.com.vn/truyen-thong/tin-tuc-trong-nganh/164-qun-ly-va-xac-nh-ri-ro-risk-identification-a-management-p2.html
[7]Công thức do chuẩn ISO ban hành
[8]Công thức do chuẩn ISO ban hành

Bảng 3.1: Ma trận tính giá trị rủi ro

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA
Giá trị tài sản		1	1	1	1	1	2	2	2	2	2	3	3	3	3	3	4	4	4	4	4	5	5	5	5	5
Tần suất xảy ra		1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
Nguy cơ	Điểm yếu																									
1	1	1	2	3	4	5	2	4	6	8	10	3	6	9	12	15	4	8	12	16	20	5	10	15	20	25
1	2	2	4	6	8	10	4	8	12	16	20	6	12	18	24	30	8	16	24	32	40	10	20	30	40	50
1	3	3	6	9	12	15	6	12	18	24	30	9	18	27	36	45	12	24	36	48	60	15	30	45	60	75
1	4	4	8	12	16	20	8	16	24	32	40	12	24	36	48	60	16	32	48	64	80	20	40	60	80	100
1	5	5	10	15	20	25	10	20	30	40	50	15	30	45	60	75	20	40	60	80	100	25	50	75	100	125
2	1	2	4	6	8	10	4	8	12	16	20	6	12	18	24	30	8	16	24	32	40	10	20	30	40	50
2	2	4	8	12	16	20	8	16	24	32	40	12	24	36	48	60	16	32	48	64	80	20	40	60	80	100
2	3	6	12	18	24	30	12	24	36	48	60	18	36	54	72	90	24	48	72	96	120	30	60	90	120	150
2	4	8	16	24	32	40	16	32	48	64	80	24	48	72	96	120	32	64	96	128	160	40	80	120	160	200
2	5	10	20	30	40	50	20	40	60	80	100	30	60	90	120	150	40	80	120	160	200	50	100	150	200	250
3	1	3	6	9	12	15	6	12	18	24	30	9	18	27	36	45	12	24	36	48	60	15	30	45	60	75
3	2	6	12	18	24	30	12	24	36	48	60	18	36	54	72	90	24	48	72	96	120	30	60	90	120	150
3	3	9	18	27	36	45	18	36	54	72	90	27	54	81	108	135	36	72	108	144	180	45	90	135	180	225
3	4	12	24	36	48	60	24	48	72	96	120	36	72	108	144	180	48	96	144	192	240	60	120	180	240	300
3	5	15	30	45	60	75	30	60	90	120	150	45	90	135	180	225	60	120	180	240	300	75	150	225	300	375
4	1	4	8	12	16	20	8	16	24	32	40	12	24	36	48	60	16	32	48	64	80	20	40	60	80	100
4	2	8	16	18	32	40	16	32	36	64	80	24	48	72	96	120	32	64	96	128	160	40	80	120	160	200
4	3	12	24	36	48	60	24	48	72	96	120	36	72	108	144	180	48	96	144	192	240	60	120	180	240	300
4	4	16	32	48	64	80	32	64	96	128	160	48	96	144	192	240	64	128	192	256	320	80	160	240	320	400
4	5	20	40	60	80	100	40	80	120	160	200	60	120	180	240	300	80	160	240	320	400	100	200	300	400	500
5	1	5	10	15	20	25	10	20	30	40	50	15	30	45	60	75	20	40	60	80	100	25	50	75	100	125
5	2	10	20	30	40	50	20	40	60	80	100	30	60	90	120	150	40	80	120	160	200	50	100	150	200	250
5	3	15	30	45	60	75	30	60	90	120	150	45	90	135	180	225	60	120	180	240	300	75	150	225	300	375
5	4	20	40	60	80	100	40	80	120	160	200	60	120	180	240	300	80	160	240	320	400	100	200	300	400	500
5	5	25	50	75	100	125	50	100	150	200	250	75	150	225	300	375	100	200	300	400	500	125	250	375	500	625

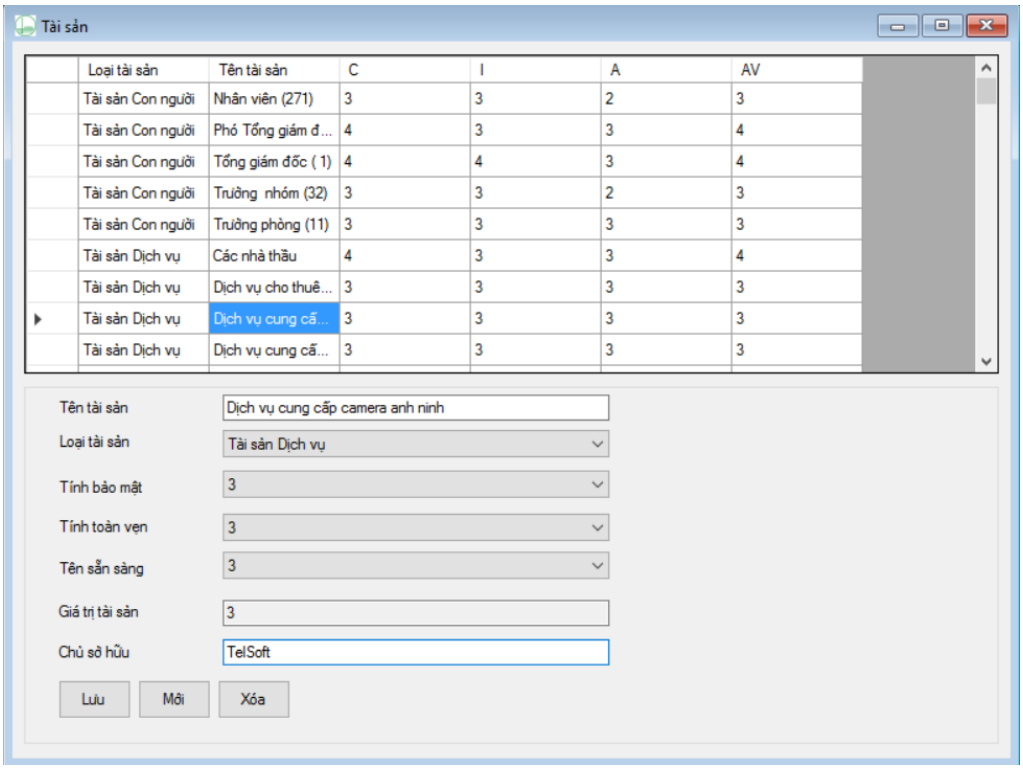
Mức độ rủi ro an toàn có giá trị từ 1-16.

3.2.2. Quản lý tài sản

Trưởng các phòng ban trong công ty chịu trách nhiệm thực hiện việc phân loại tài sản và định kỳ xem xét lại. Khi tiến hành phân loại, cần phải cân nhắc phù hợp với yêu cầu của công việc, mức độ quan trọng, mức độ nhạy cảm đối với tổ chức, các quy định của Pháp luật và Bộ, ngành về các nội dung liên quan.

Việc đánh giá và phân loại tài sản thông tin dựa trên mức độ ảnh hưởng tới Công ty trong trường hợp xảy ra sự cố.

Đánh giá giá trị tài sản và mức độ ảnh hưởng đối với tổ chức dựa trên định tính và định lượng. Đánh giá định tính dựa trên mức độ ảnh hưởng tới hoạt động kinh doanh, uy tín, hình ảnh của Công ty. Đánh giá định lượng dựa trên giá trị có thể tính bằng tiền (Ví dụ : Thiết bị hỏng mất tiền để thay thế, sửa chữa hoặc mất kết nối dẫn đến không giao dịch được gây mất doanh thu trong một ngày có thể tính ra được là mất bao nhiêu tiền…).



Hình 3.1: Tài sản

Tài sản bao gồm các loại sau:

Tài sản thông tin:

- Tài sản thông tin là loại hình tài sản của Công ty áp dụng đối với các loại tài sản hữu hình và vô hình. Tài sản thông tin bao gồm:
- Các cơ sở dữ liệu và các file dữ liệu, các bản ghi âm
- Các tài liệu, hồ sơ về bí quyết, bản quyền, về dự án, kỹ thuật và tiêu chuẩn công nghệ, phát triển hệ thống thông tin, hoạt động của hệ thống, bảo trì hệ thống.
- Văn bản về hệ thống, thông tin tìm kiếm, hướng dẫn sử dụng, tài liệu tập huấn, các thủ tục khai thác hoặc hỗ trợ, các kế hoạch nghiệp vụ. Các thông tin kiểm toán, và thông tin thu thập được.
- Hợp đồng và thỏa thuận, thông tin khách hàng

Tài sản phần cứng/ vật lý:

- Phần cứng và vật lý là loại hình tài sản của Công ty áp dụng đối với tất cả các phần cứng hoặc thiết bị vật lý đang được sử dụng phục vụ sản xuất, kinh doanh và các hoạt động nghiệp vụ khác của Công ty.
- Bao gồm máy tính, thiết bị truyền thông, thiết bị di động, máy in, máy photocopy, máy fax, máy chủ, cơ sở hạ tầng (phòng, đồ nội thất) và các thiết bị khác.
- Tài sản được thống kê theo phần cứng và thiết bị vật lý

Tài sản phần mềm:

- Tài sản phần mềm là loại hình tài sản của Công ty áp dụng đối với tất cả các phần mềm được sử dụng phục vụ sản xuất, kinh doanh và các hoạt động nghiệp vụ khác của Công ty.
- Bao gồm các phần mềm ứng dụng, hệ điều hành, công cụ phát triển, các tiện ích và các sản phẩm do công ty phát triển, tạo ra.
- Tài sản được thống kê theo: Phần mềm ứng dụng; Hệ điều hành; Công cụ phát triển; Các tiện ích; Các hệ thống thông tin của công ty; Sản phẩm của công ty.

Tài sản con người:

- Bao gồm nhân viên công ty (trình độ, kỹ năng, kinh nghiệm), khách hàng của công ty và các nhà cung cấp dịch vụ của công ty.
- Tài sản được thống kê theo lãnh đạo, trưởng phòng ban và nhân viên

Tài sản dịch vụ:

- Tài sản dịch vụ bao gồm các dịch vụ đang được sử dụng để phục vụ các hoạt động của Công ty.
- Tài sản dịch vụ bao gồm dịch vụ truyền thông, các tiện ích chung như điện, chiếu sáng, điều hòa nhiệt độ, cơ sở hạ tầng.
- Tài sản dịch vụ được thống kê theo các dịch vụ truyền thông, các tiện ích chung (điện, chiếu sáng, điều hòa nhiệt độ, cơ sở hạ tầng)

Tài sản vô hình: Tài sản vô hình bao gồm hình ảnh và danh tiếng của Công ty.

Giá trị tài sản thể hiện qua các thuộc tính bảo mật (C), toàn vẹn (I), sẵn sàng (A) của tài sản. Tính bảo mật của tài sản nhận giá trị từ 1-5. Tính toàn vẹn của tài sản nhận giá trị từ 1-5. Tính sẵn sàng của tài sản nhận giá trị từ 1-5.

Bảng 3.2: Đánh giá tài sản về độ bảo mật

Giá trị	**Mô tả**
1	Không nhạy cảm, sẵn sàng công bố.
2	Không nhạy cảm, hạn chế chỉ sử dụng trong nội bộ.
3	Hạn chế sử dụng trong tổ chức.
4	Chỉ có thể sử dụng được ở nơi cần thiết.
5	Chỉ sử dụng ở nơi cần thiết bởi cấp quản lý cao nhất.

Bảng 3.3: Đánh giá tài sản về độ toàn vẹn

Giá trị	Mô tả
1	Ảnh hưởng tới kinh doanh là không đáng kể.
2	Ảnh hưởng tới kinh doanh thấp.
3	Ảnh hưởng quan trọng tới kinh doanh.
4	Ảnh hưởng chủ yếu tới kinh doanh.
5	Tác động có thể làm sụp đổ quá trình kinh doanh.

Bảng 3.4: Đánh giá tài sản về độ sẵn sàng

Giá trị	Mô tả
1	Sẵn sàng đáp ứng trong vòng 25% số giờ làm việc.
2	Sẵn sàng đáp ứng trong vòng 50-60 % số giờ làm việc
3	Sẵn sàng đáp ứng trong vòng 75-80 % số giờ làm việc
4	Sẵn sàng đáp ứng trong vòng 95 % số giờ làm việc.
5	Sẵn sàng đáp ứng trong vòng 99.5 % số giờ làm việc.

Giá trị lớn nhất trong các tính chất C, I, A của tài sản sẽ được lấy làm giá trị của tài sản, đây là cơ sở để tính giá trị rủi ro.

Ví dụ: Một tài sản của giá trị của C = 2, I=3, A=3 thì giá trị của tài sản này mang giá trị là 3. Giá trị của tài sản và độ quan trọng của tài sản tỷ lệ thuận với nhau.

3.2.3. Xác định các nguy cơ và điểm yếu của hệ thống

Mối nguy cơ (T): Các nguy cơ được coi là nguyên nhân tiềm tàng gây ra các sự cố không mong muốn, chúng có khả năng gây ra thiệt hại cho các hệ thống, công ty và các tài sản của các hệ thống, công ty. Nguy cơ có thể xuất phát từ những lý do như con người, môi trường hoặc công nghệ/ kỹ thuật; nguy cơ có thể phát sinh từ nội bộ hoặc bên ngoài tổ chức. Ví dụ: Bị mất file do lỗi người dùng, bị mất hoặc hỏng phần mềm quan trọng.

Đầu vào cho việc nhận biết nguy cơ và ước lượng các khả năng xảy ra có thể thu thập được từ việc soát xét sự cố, người quản lý tài sản, người sử dụng tài sản và các nguồn thông tin khác, kể cả danh mục về các nguy cơ từ bên ngoài.

Đầu ra cho việc nhận biết về các nguy cơ là một danh sách các nguy cơ cùng với những thông tin nhận biết về kiểu và nguồn gốc của các. Đầu vào cho việc nhận biết nguy cơ và ước lượng các khả năng xảy ra có thể thu thập được từ việc soát xét sự cố, người quản lý tài sản, người sử dụng tài sản và các nguồn thông tin khác, kể cả danh mục về các nguy cơ từ bên ngoài.

Đầu ra cho việc nhận biết về các nguy cơ là một danh sách các nguy cơ cùng với những thông tin nhận biết về kiểu và nguồn gốc của các nguy cơ.

Bảng 3.5: Danh sách nguy cơ

STT	**Tên nguy cơ**
1	Bão lụt
2	Bị đột nhập, trộm cắp tài sản
3	Bị khóa password cá nhân, không truy cập được
4	Bị mất file do lỗi của người dùng
5	Bị mất hoặc hỏng phần mềm quan trọng
6	Bụi, ăn mòn, đóng bang
7	Cài đặt hoặc thay đổi phần mềm trái phép
8	Can thiệp từ bên ngoài, bị nghe lén hoặc cài đặt các thông tin trả lời tự động trái phép
9	Cháy nổ cáp điện, đứt cáp điện thoại
10	Cháy, nổ
11	Công tác bảo hành, bảo trì kèm
12	Dễ bị hack
13	Dễ bị virus
14	Động đất

15	Gây nhầm lẫn trong việc sử dụng cho người dùng
16	Giả mạo danh tính người dùng
17	Lạm dụng quyền sử dụng tài sản
18	Lỗi kỹ thuật
19	Lỗi phần cứng
20	Lỗi phần mềm
21	Lỗi trong sử dụng
22	Lý do sức khỏe
23	Mất ATTT
24	Mất C, I, A của thông tin
25	Mất điện
26	Mất dữ liệu
27	Nhân viên làm việc dễ truy cập trái phép hoặc làm rò rỉ thông tin một cách thiếu ý thức
28	Nhiệt độ và độ ẩm không bảo đảm đối với máy tính và server
29	Những người đã nghỉ việc vẫn có thể truy cập văn phòng và hệ thống thông tin
30	Phá hoại, trộm cắp, gian lận
31	Phá hủy, trộm cắp tài sản thông tin
32	Quá tải mạng
33	Rách, mủn, mờ do môi trường
34	Rò rỉ thông tin
35	Sang làm việc cho đối thủ canh tranh

36	Sử dụng thiết bị trái phép
37	Sự sẵn sàng hoặc tính toàn vẹn của hệ thống sản xuất có thể bị ảnh hưởng, gây lỗi, hỏng nếu phần mềm chưa được kiểm tra đã đưa vào sử dụng
38	Thất lạc, không lưu trữ đúng quy định
39	Thiệt hại có chủ ý do con người
40	Thiếu cơ chế giám sát
41	Thời gian chờ đợi dài
42	Tính sẵn sàng của nguồn lực
43	Tính toàn vẹn của dữ liệu bị ảnh hưởng, bị trộm cắp các dữ liệu
44	Trộm cắp dữ liệu
45	Trộm cắp dữ liệu thông tin
46	Trộm cắp phương tiện hoặc tài liệu
47	Trộm cắp, gây rối, làm gián điệp, phá hoại Công ty
48	Truy cập trái phép
49	Truy cập trái phép thông tin
50	Truy cập trái phép tới máy chủ
51	Truy cập trái phép tới máy tính cá nhân
52	Truy cập trái phép và sử dụng trái phép tài nguyên
53	Truy cập trái phép và sửa đổi thông tin hệ thống
54	Từ chối dịch vụ
55	Vận hành hệ thống bị gián đoạn
56	Vi phạm bản quyền hoặc các điều khoản và điều kiện của thỏa thuận với nhà cung cấp phần mềm, có thể gây tranh chấp về pháp lý

57	Vi phạm bảo trì hệ thống, gây lỗi khi sử dụng

Điểm yếu (V): Các điểm yếu không tự gây ra thiệt hại mà chúng cần phải có một nguy cơ khai thác. Một tài sản có thể có nhiều điểm yếu và nguyên nhân là do con người, môi trường hoặc công nghệ/ kỹ thuật. Ví dụ: Bảo trì thiết bị không đầy đủ; Bảo vệ truy cập vật lý kém.

Đầu vào của việc nhận biết về điểm yếu là một danh sách các nguy cơ đã biết, danh sách các tài sản và các biện pháp hiện có.

Các hướng dẫn nhận biết điểm yếu:

- Cần phải nhận biết các điểm yếu có thể bị khai thác các nguy cơ về an toàn thông tin và là nguyên nhân gây thiệt hại cho các tài sản, cho tổ chức.
- Điểm yếu được nhận biết trong các vấn đề sau:
    - Tổ chức
    - Quy trình, thủ tục
    - Thủ tục quản lý
    - Nhân sự
    - Môi trường vật lý
    - Cấu hình hệ thống thông tin
    - Phần cứng, phần mềm, thiết bị truyền thông
    - Sự phụ thuộc vào các thành phần bên ngoài

Một điểm yếu mà không có nguy cơ tương ứng thì có thể không cần thiết phải triển khai một biện pháp nào nhưng các thay đổi cần được phát hiện và giám sát chặt chẽ. Ngược lại, một nguy cơ mà không có điểm yếu tương ứng thì có thể không gây ra bất kỳ một rủi ro nào. Trong khi đó, một biện pháp được thực hiện không đúng cách, quy trình hoặc sau chức năng hoặc áp dụng không đúng cũng có thể là một điểm yếu. Biện pháp có hiệu quả hay không còn phụ thuộc vào môi trường vận hành hệ thống.

Một điểm yếu có thể liên quan đến các thuộc tính của tài sản bị sử dụng khác với mục đích và cách thức khi được mua sắm hoặc sản xuất, cần phải xem xét các điểm yếu phát sinh từ nhiều nguồn khác nhau.

Đầu ra của việc nhận biết về điểm yếu là một danh sách các điểm yếu liên quan đến các tài sản, các mối đe dọa và các biện pháp xử lý. Một danh sách các điểm yếu không liên quan đến bất kỳ nguy cơ nào đã được nhận biết để soát xét.

Bảng 3.6: Danh sách điểm yếu

STT	Tên điểm yếu
1	Bảo trì thiết bị không đầy đủ
2	Bảo trì, bảo dưỡng điều hòa kém
3	Bảo vệ truy cập vật lý kém
4	Các mã độc hại có thể lây nhiễm sang các máy tính
5	Có nhiều người trong nội bộ cùng có quyền truy cập
6	Con người
7	Công tác PCCC kém
8	Đào tạo về an toàn thông tin không đầy đủ
9	Dịch vụ bảo vệ Tòa nhà kém
10	File mềm
11	Giao dịch qua mạng truyền thông, Đường cáp mạng không được bảo vệ
12	Giấy, bảo vệ vật lý yếu
13	Giấy, dễ bị ảnh hưởng bởi độ ẩm, bụi
14	Khi bàn giao người quản lý cũ quên ko bàn giao password cá nhân
15	Không tắt máy khi rời khỏi máy trạm
16	Không bảo mật file bằng password
17	Không cập nhật thường xuyên phần mềm chống virus
18	Không có nguồn điện dự phòng
19	Không có phụ tùng thay thế khi hỏng
20	Không được bảo vệ và kiểm soát đầy đủ
21	Không kiểm soát việc sao lưu hay nhân bản tài liệu

22	Kiểm soát vật lý không đầy đủ sự ra vào Công ty
24	Lỗi hoặc bị virut Trojan trong phần mềm cài đặt
25	Lỗi trong hệ điều hành và phần mềm ứng dụng
26	Mức độ cung cấp dịch vụ không rõ ràng
27	Nguồn điện không ổn định
28	Password bảo vệ yếu
29	Phần mềm chưa được cập nhật
30	Quy trình kiểm thử phần mềm thiếu hoặc không có
31	Rời bỏ Công ty
32	Sao chép không được kiểm soát
35	Sự vắng mặt
36	Tấn công bởi virut và hacker
37	Thiếu biện pháp kiểm soát việc mang máy tính cá nhân (được cấp phép truy cập mạng Công ty) ra, vào hàng ngày
38	Thiếu biện pháp thay đổi cấu hình hiệu quả
39	Thiếu các thủ tục quản lý sự thay đổi
40	Thiếu cẩn thận khi hủy bỏ
42	Thiếu chính sách sử dụng email và internet
43	Thiếu chính sách sử dụng tài sản
44	Thiếu cơ chế giám sát
45	Thiếu đường dự phòng
46	Thiếu giám sát công việc của cấp dưới
47	Thiếu giám sát hệ thống

48	Thiếu hoặc không có đầy đủ các quy định (liên quan đến ATTT) trong các hợp đồng với khách hàng hoặc/ và bên thứ ba
49	Thiếu kiểm soát phương tiện phần mềm
50	Thiếu kiểm soát truy cập
51	Thiếu nhận thức bảo mật thông tin
53	Thiếu phân loại đầy đủ
54	Thiếu phòng cháy chữa cháy
55	Thiếu quá trình backup dữ liệu
56	Thiếu quy định cho việc sử dụng đúng phương tiện thông tin
57	Thiếu sự bảo vệ vật lý
58	Thiếu sự nhận diện các rủi ro liên quan đến các đối tác bên ngoài
59	Thiếu thủ tục để xem xét, giám sát quyền truy cập
60	Thông tin trao đổi giữa bộ phận HRD và các bên liên quan không kịp thời
61	Thủ tục tuyển dụng không đầy đủ (thiếu sàng lọc)
62	Việc sử dụng phần mềm và phần cứng không đúng cách

3.2.4. Lựa chọn các mục tiêu kiểm soát

Mục đích của việc quản lý an ninh thông tin khi áp dụng ISO 27001:2013 là để đảm bảo rằng toàn bộ nhân viên, nhà thầu và bên thứ ba hiểu được được trách nhiệm của bản thân tương ứng với vai trò được giao, giảm thiểu các nguy cơ gây tổn hại tới an ninh thông tin như trộm cắp, lừa đảo hoặc lạm dụng cơ sở vật chất.

Thứ hai là, nhận thức được các mối nguy cơ và các vấn đề liên quan đến an toàn thông tin, trách nhiệm và nghĩa vụ pháp lý của họ; được đào tạo và trang bị kiến thức, điều kiện cần thiết nhằm hỗ trợ chính sách an toàn thông tin của công ty trong quá trình làm việc giảm thiểu các rủi ro do lỗi của con người gây ra.

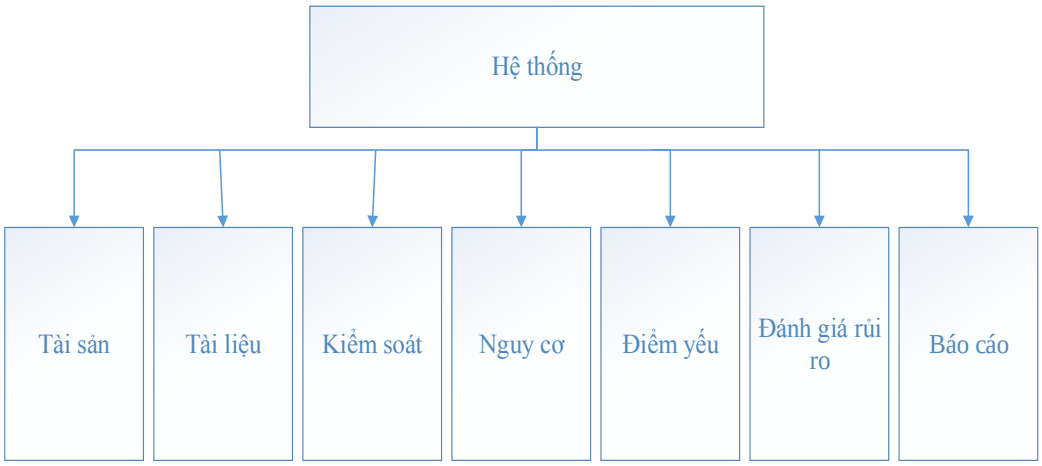
Thứ ba là, rời khỏi tổ chức hoặc thay đổi việc làm một cách tổ chức, đảm bảo an toàn thông tin.

Quản lý an ninh thông tin nhân sự bao gồm sẽ được áp dụng trong cả ba giai đoạn trước khi tuyển dụng, trong thời gian làm việc và chấm dứt hoặc thay đổi vị trí công việc.

3.2.5. Chương trình thử nghiệm

Chương trình được xây dựng bằng ngôn ngữ C# sử dụng công cụ Visual Studio 2012. Hệ quản trị cơ sở dữ liệu SQL Server 2008 R2.

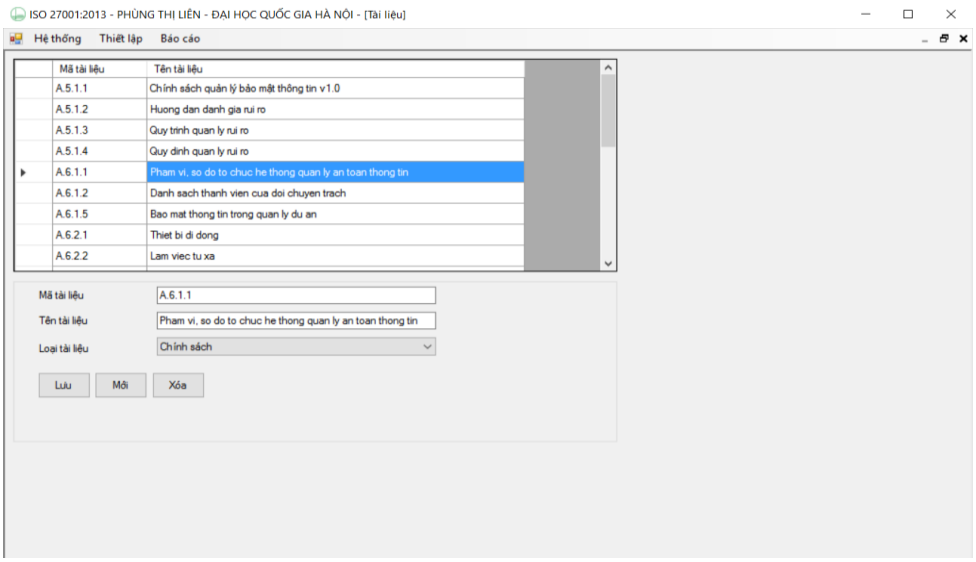
Chương trình thử nghiệm được cài đặt trên laptop có cấu hình: Intel core i3 2.13Hz, ram 4Gb. Máy tính sử dụng hệ điều hành Microsoft Win 7 32 bit.



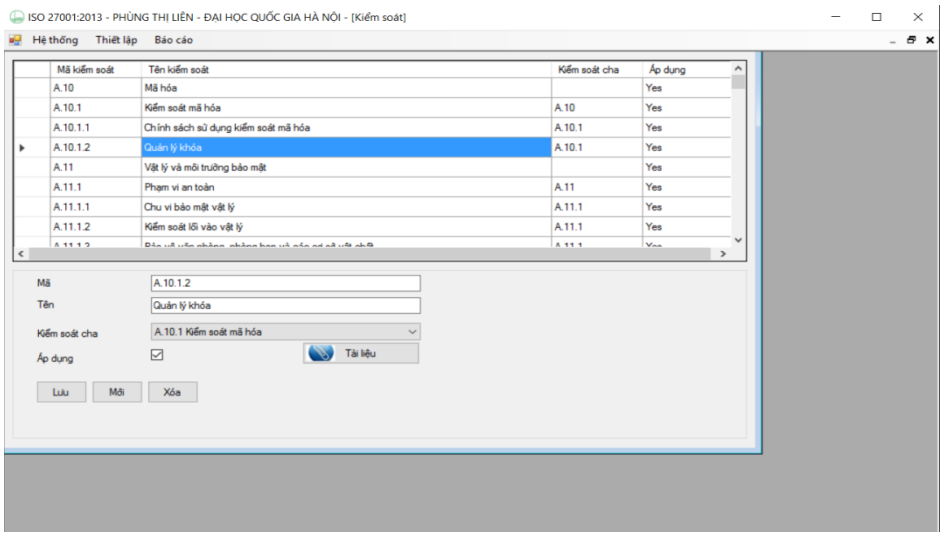
Hình 3.2: Các module của hệ thống

Chương trình được xây dựng cho phép định nghĩa thông tin tài sản của công ty, xác định giá trị tài sản dựa trên các thuộc tính C, I, A. Định nghĩa các nguy cơ, điểm yếu và xây dựng các kiểm soát. Từ đó cho phép quản lý rủi ro dựa trên các ảnh hưởng của nguy cơ và điểm yếu đối với tài sản. Với những rủi ro có giá trị lớn hơn 16 chương trình sẽ đưa ra cảnh báo để người dùng biết được cần phải đưa ra biện pháp kiểm soát để giảm rủi ro. Các báo cáo tuyên bố áp dụng (SoA) là những kiểm soát công ty áp dụng để giảm thiểu rủi ro. Ngoài ra, chương trình còn có biểu đồ trực quan so sánh giá trị rủi ro trước và sau khi áp dụng các biện pháp kiểm soát.

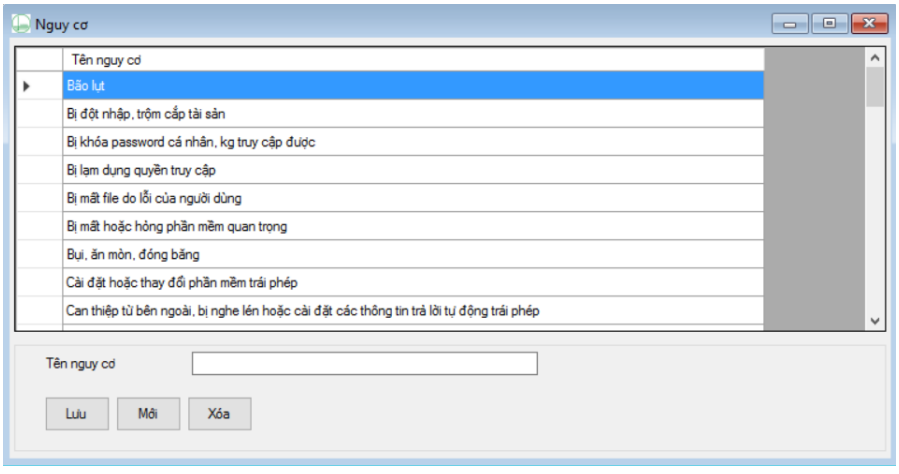
Một số hình ảnh của chương trình:



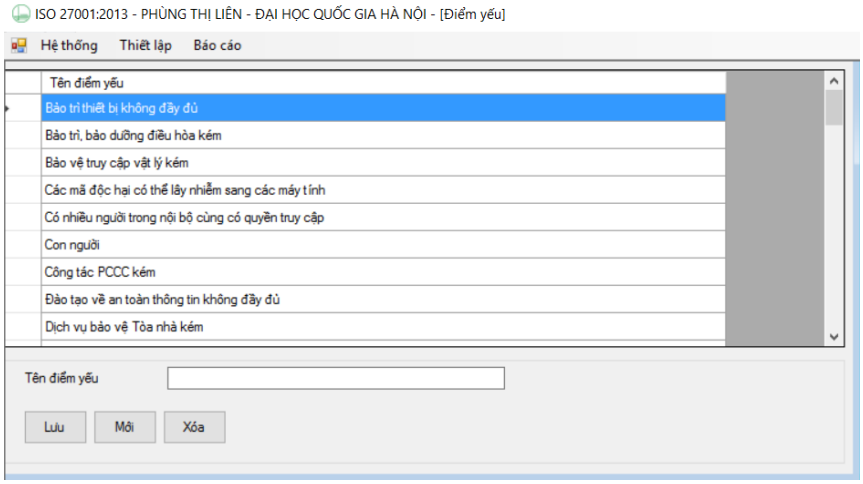
Hình 3.3: Tài liệu



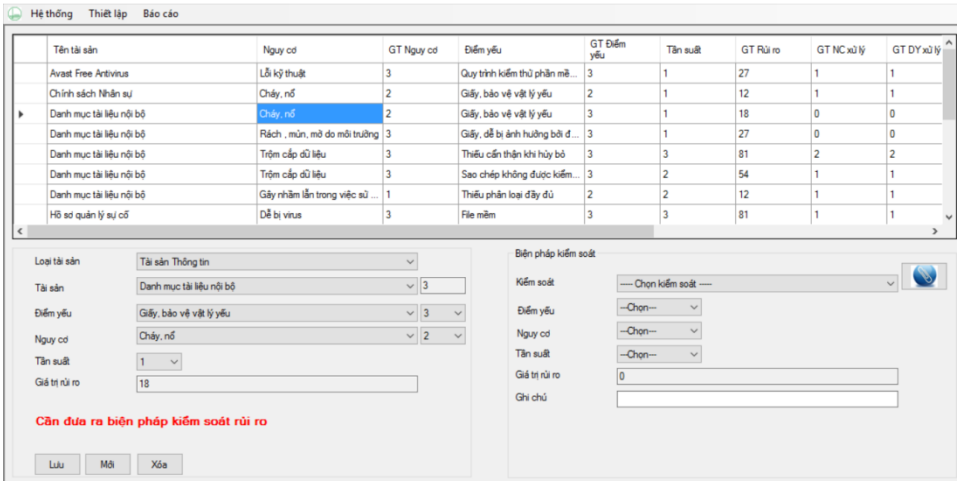
Hình 3.4: Kiểm soát



Hình 3.5: Nguy cơ



Hình 3.6: Điểm yếu



Hình 3.7: Đánh giá rủi ro

BẢNG TUYÊN BỐ ÁP DỤNG

Mã	Tên kiểm soát	Áp dụng	Mã tài liệu
A.5	Chính sách an ninh thông tin	Có	
A.5.1	Chỉ dẫn quản lý bảo mật thông tin	Có	
A.5.1.1	Chính sách bảo mật thông tin	Có	A.5.1.1
A.5.1.2	Xem xét chính sách bảo mật thông tin	Có	
A.6	Tổ chức của bảo mật thông tin	Có	
A.6.1	Tổ chức nội bộ	Có	
A.6.1.1	Vai trò và trách nhiệm bảo mật thông tin	Có	
A.6.1.2	Phân chia nhiệm vụ	Có	
A.6.1.3	Liên hệ với người có thẩm quyền	Có	
A.6.1.4	Liên hệ với các nhóm chuyên gia	Có	
A.6.1.5	Bảo mật thông tin trong quản lý dự án	Có	

Hình 3.8: Tuyên bố áp dụng

KẾT LUẬN

A. NHỮNG VẤN ĐỀ GIẢI QUYẾT ĐƯỢC TRONG LUẬN VĂN NÀY

Đảm bảo an toàn thông tin cần được thực hiện định kỳ một cách thường xuyên, nhằm đảm bảo cho hệ thống thông tin được an toàn. Tránh được các rủi ro đáng tiếc xảy ra, gây ảnh hưởng tới hoạt động sản xuất, kinh doanh của công ty. Luận văn đã đạt được 2 kết quả quan trọng trong quá trình xây dựng hệ thống ISMS theo tiêu chuẩn ISO 27001.

1/ Về nghiên cứu, tìm hiểu hệ thống quản lý theo chuẩn ISO 27001: Luận văn đã đưa ra được đầy đủ lý thuyết từ lịch sử phát triển, phạm vi, bộ tiêu chuẩn liên quan và các kiểm soát, mục tiêu kiểm soát và phụ luc A trong tiêu chuẩn. Lập một hệ thống quản lý ATTT theo chuẩn ISO 27001 là cách tiếp cận mang tính hệ thống để quản lý thông tin nhạy cảm của tổ chức nhằm duy trì và đảm bảo ba thuộc tính an toàn thông tin: Tính tin cậy, Tính toàn vẹn, Tính sẵn sàng. Với các yêu cầu cụ thể gồm Tiêu chuẩn ISO 27001:2013 có 7 nội dung chính:

- Bối cảnh của tổ chức
- Lãnh đạo
- Hoạch định
- Hỗ trợ
- Điều hành
- Đánh giá kết quả
- Cải tiến

Và phụ lục A bao gồm 14 chương, 35 mục tiêu và 114 kiểm soát.

Như vậy ISO 27001 giúp cho tổ chức tạo được một hệ thống quản lý an toàn thông tin chặt chẽ nhờ luôn được cải tiến nhằm đảm bảo an ninh và khai thác thông tin một cách hợp lý và hiệu quả nhất.

2/ Về thử nghiệm xây dựng hệ thống an toàn thông tin cho doanh nghiệp: Từ cơ sở lý thuyết đã nghiên cứu được, chương này đã đưa ra các phương pháp xác định rủi ro, định nghĩa các tài sản, các nguy cơ và điểm yếu. Từ các tài sản, nguy cơ, điểm yếu đó lựa chọn các mục tiêu kiểm soát phù hợp để nhằm mục đích giảm bớt rủi ro xảy ra đối với doanh nghiệp. Qua quá trình nghiên cứu và quá trình làm việc thực tiễn của một công ty, tôi cũng đã định nghĩa ra một số tài liệu về chính sách, quy trình, quy định liên quan đến hệ thống quản lý an toàn thông tin, và xây dựng được chương trình demo thử nghiệm về các thông tin quản lý hệ thống an toàn thông tin đưa ra được tuyên bố áp dụng đối với mỗi tổ chức.

B. KIẾN NGHỊ VÀ HƯỚNG NGHIÊM CỨU TRONG TƯƠNG LAI

Việc một tổ chức hay doanh nghiệp tuân thủ và đạt được chứng chỉ ISO 27001 là sự thừa nhận quốc tế trong việc đảm bảo an toàn thông tin của tổ chức. Tuy nhiên, việc tuân thủ hay đạt được được chứng chỉ ISO 27001 không khẳng định là tổ chức được an toàn tuyệt đối. Do vậy, cần liên tục kiểm soát, đánh giá rủi ro, xác định các mối đe dọa và điểm yếu của hệ thống để có những hiểu biết tốt hơn về hệ thống thông tin, từ đó đưa được các giải pháp để giảm thiểu rủi ro. Nên đánh giá hệ thống định kỳ 6 tháng/1 lần để có những cải tiến phù hợp với hệ thống quản lý an toàn thông tin. Đảm bảo tài sản thông tin luôn đáp ứng được ba thuộc tính là tính bảo mật, tính toàn vẹn và tính sẵn sàng.

Hệ thống quản lý an toàn thông tin cũng đang được khá nhiều tổ chức đang quan tâm và đón nhận và áp dụng. Trong tương lai, tôi muốn nghiên cứu thêm về phương pháp đánh giá rủi ro theo định lượng có nghĩa là việc đánh giá rủi ro gây thiệt hại về tiền mặt, để nhằm giúp cho các tổ chức, doanh nghiệp sẽ có một hình dung cụ thể về những thiệt hại, mất mát do các rủi ro gây ra. Đồng thời tôi sẽ nghiên cứu phương pháp đánh giá và công nhận chứng chỉ ISO 27001 cho một tổ chức, doanh nghiệp.

TÀI LIỆU THAM KHẢO

Tiếng việt

1. Trịnh Nhật Tiến (2008), *Giáo trình an toàn dữ liệu*, Trường Đại học công nghệ, đại học Quốc gia Hà Nội.
2. Nghị định 64/2007/NĐ-CP, ngày 10/04/2007 của Chính phủ về Ứng dụng công nghệ thông tin trong hoạt động của cơ quan Nhà nước.

Tiếng anh

3. Alan Calder & Steve Watkins, *IT Governance A manager's Guide to Data Security and ISO 27001/ISO 27002.*
4. Barry L. Williams (2010), *Information Security Policy Development for Compliance*, New York.
5. Gary Stoneburner, Alice Goguen, and Alexis Feringa (2002), *Risk Management Guide for Information Technology Systems.*
6. Val Thiagarajan B.E., M.Comp, CCSE, MCSE, SFS, ITS 2319, IT Security Specialist (2006), *BS ISO/IEC 17799:2005 SANS Audit Check List*.
7. ISO/IEC 27000 – Information technology – Security techniques – Information security management systems – Overview and vocabulary (2014).
8. ISO/IEC 27001 – Information technology – Security techniques – Information security management systems – Overview and vocabulary (2005, 2013).
9. ISO/IEC 27003 – Information technology – Security techniques – Information security management system implementation guidance.
10. ISO/IEC 27005 - Information technology – Security techniques – Information security management systems – Information security risk management (2008, 2013).
11. ISO 31000: Risk management – A practical guide for SMEs.