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

HÀ NỘI - 2016

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, toàn vẹn và sẵn sàng, 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 được tổ chức thành 3 chương như sau:

Chương 1 Trình bày tổng quan về an toàn thông tin.

Chương 2 Trình bày tiểu chuẩn quốc tế ISO 27001.

Chương 3 Xây dựng hệ thống quản lý hệ thống an toàn thông tin 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 ISO17799 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 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.

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 ngưng 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 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.

1.3. Nhu cầu cấp thiết cần phải xây dựng một hệ thống an toàn thông tin đáp ứng tiêu chuẩn quốc tế

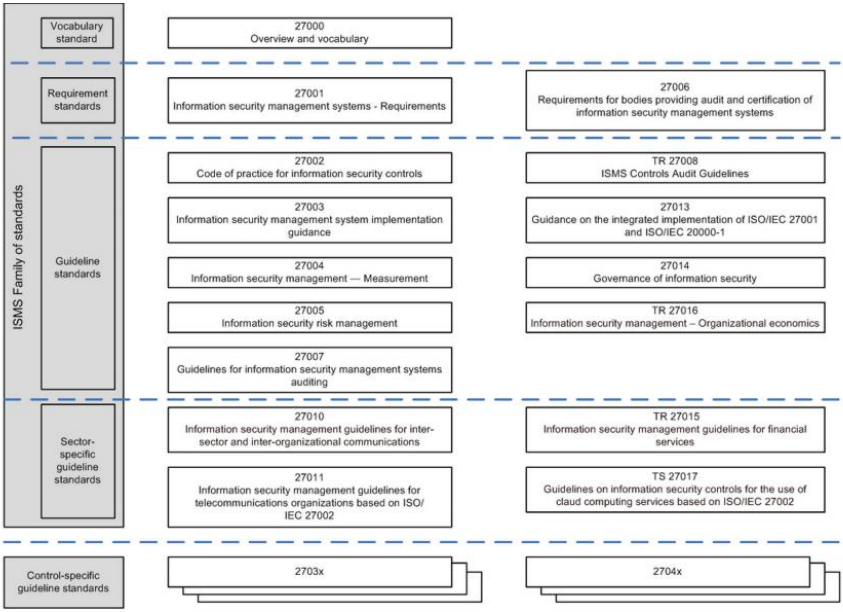
Từ những nguy cơ rủi ro mất an toàn thông tin như trên cho ta thấy, nhu cầu cần thiết phải thiết lập một chính sách an ninh thông tin dựa trên nền tảng một hệ thống quản lý an toàn thông tin (ISMS – Information Security Management System) chuẩn hóa là vô cùng cần thiết. ISO 27001 là một tiêu chuẩn quốc 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.



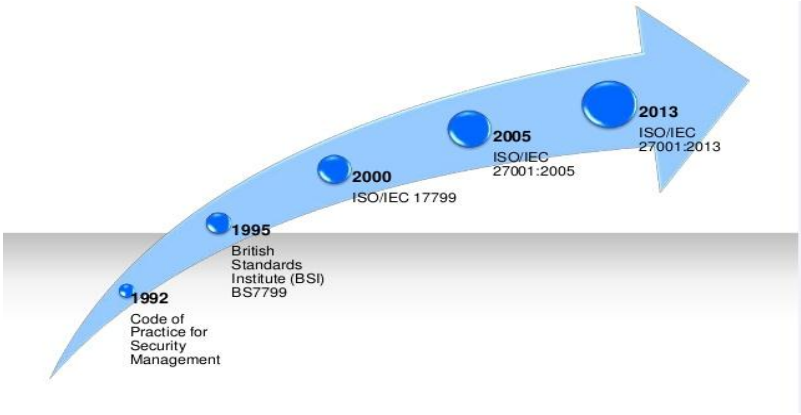
Hình 2.1: Họ tiêu chuẩn ISMS

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.

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.
- Tháng 10 năm 2013 tiêu chuẩn ISO/IEC 27001:2013 ra đời.

2.1.4. Tiếp cận 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.

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

2.1.5.1. Tổng quan

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

2.1.5.2. 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.

2.1.5.3. Đánh giá rủi ro an toàn thông tin

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.

2.1.5.4. Giải quyết rủi ro an toàn thông tin

Cho từng rủi ro được xác định sau khi đánh giá rủi ro thì một quyết định xử lý rủi ro cần phải được thực hiện.

2.1.5.5. Lựa chọn và thực hiện kiểm soát

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.

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

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.

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 sẵn sàng, tính toàn vẹn của thông tin. Doanh nghiệp, tổ chức nên thực hiện cải tiến liên tục.

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.

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.

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.

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

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.

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.

2.2.3.2. Chính sách

Lãnh đạo cao nhất phải thiết lập một chính sách an toàn thông tin phù hợp với một số mục đích, mục tiêu và cam kết. Chính sách an toàn thông tin phải sẵn có và được truyền đạt trong tổ chức.

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.

2.2.4. Hoạch định

2.2.4.1. Hành động và cơ hội giải quyết rủi ro

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.

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

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.

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 xác định được những người có năng lực cần thiết phù hợp với công việc và đưa ra những hành động để đạt được năng lực cần thiết.

2.2.5.3. Nhận thức

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

2.2.5.5. Thông tin dạng văn bản

Nêu khái quát hệ thống an toàn thông tin của tổ chức, tạo và cập nhật thông tin dạng văn bản. Thực hiện kiểm soát 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.

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).

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.

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.

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.

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.

2.2.8. Cải tiến

2.2.8.1. Sự không phù hợp và hành động khắc phục.

Khi xảy ra sự không phù hợp, tổ chức phải thực hiện đánh giá, giải quyết và xác định các nguyên nhân, xem xét tính hiệu lực của hành động khắc

phục được thực hiện. Các hành động phải thích hợp với tác động của sự không phù hợp gặp phải và phải lưu lại thông tin dưới dạng văn bản.

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 phụ lục A của tiêu chuẩn

Phụ lục A bao gồm 14 chương, 35 mục tiêu và 114 kiểm soát

2.3. Mười lý do để chứng nhận ISO 27001

10 lý do để chứng nhận ISO 27001 bao gồm: Thông tin đúng, thúc đẩy quan hệ đối tác, cắt giảm chi phí trong chuỗi cung ứng, không đơn thuần về an ninh thông tin, hoạt động trên quy trình và hệ thống nhất quán, áp dụng mở rộng và bao quát không chỉ riêng công nghệ thông tin, được đánh giá bởi tổ chức chứng nhận được công nhận Quốc tế.

2.4. Thực trạng và triển vọng phát triển ISO 27001

Từ năm 2006, nhiều tổ chức, cơ quan ở Việt Nam đã quan tâm đến ISO 27001 và có nhiều tổ chức lấy chứng nhận tiêu chuẩn này.

Theo đánh giá của một số chuyên gia, triển vọng áp dụng ISO 27001 tại Việt Nam là khá cao. 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 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.

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.

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.

Có 2 phương pháp để đánh giá rủi ro là đánh giá rủi ro định tính và định lượng[1]:

- Phương pháp đánh giá định lượng là việc gán một giá trị cụ thể tới các mất mát có thể xảy ra.

[1]https://dnasecurity.com.vn/truyen-thong/tin-tuc-trong-nganh/164-qun-ly-va-xac-nh-ri-ro-risk-identification-a-management-p2.html

- 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[2]

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[3]

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

[2]Công thức do chuẩn ISO ban hành
[3]Công thức do chuẩn ISO ban hành

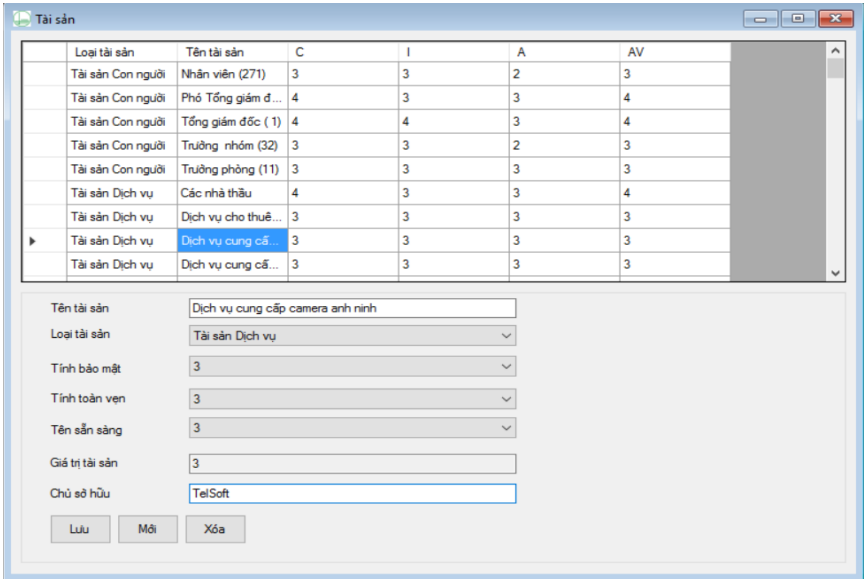
Bảng 3.1: Ma trận tính giá trị rủi ro

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

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 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.

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.

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 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 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.

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 băng
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.
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 virus 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 virus 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.

Chương trình cho phép quản lý danh sách và định nghĩa giá trị các tài sản, nguy cơ, điểm yếu. Đối với mỗi loại tài sản có nguy cơ, điểm yếu khác nhau. Phần mềm cho phép nhập liệu và tính được giá trị rủi ro. Từ đó cho nhập liệu được biện pháp kiểm soát và tính được giá trị rủi ro của tài sản đó khi áp dụng biện pháp kiểm soát.

Chương trình đưa ra được bản tuyên bố áp dụng, các biểu đồ và danh sách báo cáo về nguy cơ, tài sản, điểm yếu.

KẾT LUẬN

A. Những vấn đề giải quyết được trong luận văn này

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 8 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: 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 nghiên 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.