CHƯƠNG I

TẠI SAO PHẢI QUẢN LÝ AN TOÀN THÔNG TIN

1.1 An toàn thông tin là gì?

Thông tin là một trong những tài sản có giá trị nhất của tổ chức. Theo tiêu chuẩn ISO/IEC 27001:2005 thì An toàn thông tin là bảo vệ thông tin trước nguy cơ mất an toàn nhằm đảm bảo tính liên tục trong hoạt động kinh doanh của doanh nghiệp, giảm thiểu sự phá hoại doanh nghiệp, gia tăng tới mức tối đa các cơ hội kinh doanh và đầu tư phát triển. Thông tin có thể tồn tại dưới nhiều dạng. Thông tin có thể được in hoặc được viết trên giấy, được lưu trữ dưới dạng điện tử, được truyền đi qua bưu điện hoặc dùng thư điện tử, được trình diễn trên các bộ phim, hoặc được nói trên các cuộc đàm thoại. Nhưng cho dù thông tin tồn tại dưới dạng nào đi chăng nữa, thì nó cũng được đưa ra với hai mục đích chính là chia sẻ và lưu trữ, vì vậy nó luôn luôn cần sự bảo vệ thích hợp. Việc đảm bảo an toàn thông tin là phải đảm bảo tính bí mật, tính toàn vẹn, tính sẵn sàng của thông tin. Vậy tính bí mật, tính toàn vẹn, tính sẵn sàng của thông tin là gì? Tiêu chuẩn ISO/IEC 27001:2005 đã định nghĩa như sau:

- Tính bí mật (**confidentiality**): Tài sản là thông tin không được cung cấp hoặc tiết lộ cho các cá nhân không có thẩm quyền.
- Tính toàn vẹn (**integrity**): Tài sản được truy cập và được sử dụng theo nhu cầu của một tổ chức có thẩm quyền.
- Tính sẵn sàng (**availability**): Đảm bảo tính chính xác và đầy đủ của tài sản.

Việc đảm bảo an toàn cho thông tin sẽ là trách nhiệm của tất cả các nhà quản lý, chủ sở hữu hệ thống thông tin, người nắm giữ hệ thống thông tin, người sử dụng.

1.2 Tầm quan trọng của việc quản lý an toàn thông tin

Hiện nay các hoạt động tin tặc liên tục gia tăng. Những hoạt động này ngày càng đa dạng về kiểu tấn công, mức độ nguy hiểm ngày càng tăng và có tính tự

động cao. Đích nhắm tới của những cuộc tấn công này là vào các tổ chức tài chính, chính phủ, các doanh nghiệp……Mục đích của các cuộc tấn công có thể là vì lợi nhuận, vì tò mò, vì vấn đề chính trị, hoặc vì sự ghen ghét nhau…..nhưng mục tiêu chung của các cuộc tấn công là chúng thường tấn công vào các hệ thống thông tin chứa các tài nguyên quan trọng như: số thẻ ATM của khách hàng, số hợp đồng, thông tin kinh doanh quan trọng….Nếu mất những thông tin này các doanh nghiệp sẽ phải đối mặt với việc mất lòng tin của khách hàng và của đối tác, mất một lượng tiền lớn nếu kẻ tấn công truy cập được vào hệ thống ngân hàng, đánh cắp những thông tin kinh doanh quan trọng và làm cho hoạt động kinh doanh của công ty bị gián đoạn. Vì vậy đảm bảo an toàn cho thông tin là một việc quan trọng hàng đầu trong doanh nghiệp, nếu các tổ chức hay các doanh nghiệp làm tốt việc bảo mật cho thông tin thì doanh nghiệp đó sẽ chống lại được các nguy cơ sau:

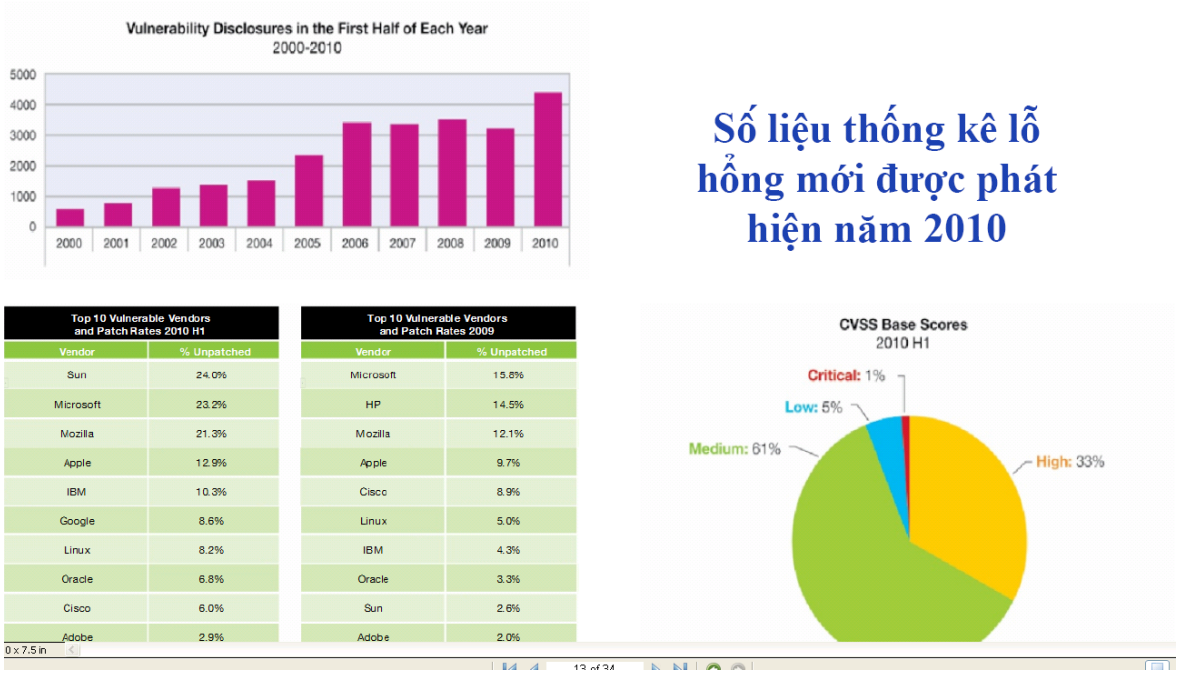
- Các thông tin nhạy cảm hoặc các thông tin bí mật bị mất, bị rò rỉ hoặc bị tiết lộ một cách vô tình hay cố ý.
- Việc cố ý hay vô tình sửa chữa thông tin mà không có sự cho phép của người sở hữu thông tin
- Bất cứ một thông tin kinh doanh quan trọng nào bị mất mà không để lại dấu vết hoặc không thể hồi phục lại.
- Bất cứ một thông tin kinh doanh quan trọng không có khả năng đáp trả những khi người dùng cần tới chúng.

Với việc quản lý tốt an toàn thông tin thì các doanh nghiệp sẽ bảo vệ tốt được tài sản của mình. Tuy nhiên việc đảm bảo an toàn thông tin không chỉ đơn giản liên quan đến vấn đề máy móc, kỹ thuật và hệ thống thông tin như nhiều người lầm tưởng mà nó còn phải tính đến việc quản lý con người, các thủ tục, hành lang pháp lý….

1.3 Hiện trạng an toàn thông tin ở Việt Nam

Tại Việt Nam an toàn thông tin hiện nay vẫn là một vấn đề khá mới mẻ tuy vậy nhà nước và các doanh nghiệp đã có những quan tâm đáng kể tới việc này. Năm 2010 là năm thực sự nóng bỏng của an toàn thông tin trên thế giới nói chung

và ở Việt Nam nói riêng. Tại Việt Nam số thuê bao sử dụng Internet tính đến 2/2011 là 27559006 chiếm 31,9% dân số. Đa số các tổ chức và các doanh nghiệp có hệ thống mạng website để quảng bá thương hiệu là 191667 tên miền .vn và hàng triệu tên miền thương mại. Có rất nhiều doanh nghiệp đã ứng dụng thanh toán trực tuyến vào công việc kinh doanh, giao dịch trong khi đó mạng Internet Việt Nam còn tiềm ẩn rất nhiều những nguy cơ về mặt an ninh an toàn thông tin. Hàng loạt các Website lớn bị tấn công với mức độ phức tạp ngày càng gia tăng. Các cuộc tấn công nhằm vào hệ thống thông tin, trang thông tin điện tử Chính phủ một số nước để đánh cắp dữ liệu, làm ngưng hệ thống mạng ngày càng nhiều. Ở nước ta theo đánh giá của một số chuyên gia về an ninh mạng các tên miền .vn hiện đang đứng hàng thứ 3 trong bảng xếp hạng các tên miền có nguy cơ bị tấn công (khoảng 15.000 Website). Đặc biệt đã có nhiều trang Web có tên miền .vn bị hacker tấn công ví dụ như: ngày 22/11/2010 là ngày đầu tiên hacker tấn công vào hệ thống Website của báo Vietnamnet, đây là cuộc tấn công có quy mô lớn, kéo dài và liên tục, nó đã phá hủy hầu như gần hết cơ sở dữ liệu được lưu trữ 10 năm của báo VietNamnet. Dưới đây là thống kê lỗ hổng an toàn thông tin của một số Website ở Việt Nam.



Hình 1: Thống kê lỗ hổng ATTT của một số Website ở Việt Nam

Các cuộc tấn công trên mạng chủ yếu có tính chất vụ lợi, có tổ chức và mang tính quốc tế đang nở rộ với quy mô lớn. Hacker – thủ phạm các cuộc tấn công nhằm vào các Website có trình độ rất cao. Họ sử dụng hệ thống Bootnet rất tinh vi, hình thức tấn công cực kì chuyên nghiệp và rất khó chống đỡ. Hình thức tấn công rất đa dạng từ thay đổi giao diện cho đến đánh cắp các dữ liệu nhạy cảm ở trong website và tấn công làm tê liệt hệ thống website đó. Mục tiêu tấn công của hacker không chỉ là các tổ chức, doanh nghiệp tài chính, ngân hàng mà là tất cả hệ thống. Các cuộc tấn công trên là một lời cảnh báo về an toàn thông tin đối với các báo điện tử và những website quan trọng của Việt Nam.

Thực trạng tấn công vào các website của các hacker không mới so với những năm trước tuy nhiên các website tại Việt Nam vẫn chưa được đầu tư về nhân lực, kinh phí để được bảo vệ một cách tốt nhất. Nguyên nhân chủ yếu là sự yếu kém trong quản trị Website và không thường xuyên kiểm soát lỗ hổng, khoán trắng vấn đề bảo đảm ATTT cho nơi đặt website, ít quan tâm đến cảnh báo an ninh của các cơ quan, tổ chức có chức năng đảm bảo an ninh an toàn thông tin quốc gia. Rất nhiều website trong nước tồn tại các lỗ hổng an toàn an ninh thông tin ở mức độ cao. Đa số các website lớn ở Việt Nam đều có lỗ hổng bảo mật và có thể bị chiếm quyền điều khiển. Hiện nay trên mạng Internet ở Việt Nam có đến 90% các website được xây dựng trên công nghệ ASP.Net và sử dụng dịch vụ IIS 6.0, đây là lỗ hổng lớn nhất và vẫn chưa khắc phục được. Trong năm 2010 đã ghi nhận hơn 1000 Website ở nước ta bị tấn công từ các lỗ hổng đang tồn tại trên các website và các lỗ hổng trên máy chủ hệ thống. Các Website của tổ chức tài chính, ngân hàng, chứng khoán vẫn tồn tại rất nhiều lỗ hổng. Lỗ hổng an ninh hệ thống ngày càng được phát hiện nhiều hơn. Số lượng các điểm yếu an ninh trong năm 2010 là 4300 (năm 2009 là 3500) có tới 30% lỗ hổng có mức độ nguy hiểm cao. Gần một nửa (49%) số lỗ hổng an ninh vẫn chưa có các bản vá do nhà cung cấp dịch vụ phát hành. Lỗ hổng liên quan đến phần mềm Adobe Acrobat PDF được phát hiện nhiều nhất. Ở nước ta vấn đề lỗ hổng của hệ thống, ứng dụng vẫn chưa được các quản trị hệ thống cập nhật các bản vá kịp thời. Tội phạm mạng tại Việt Nam đang diễn ra với tốc độ nhanh hơn, quy mô hơn, tính chuyên nghiệp, trình độ kỹ thuật ngày

càng cao và khả năng để lại dấu vết ngày càng ít hơn. Tội phạm mạng hiện nay thường tập trung hoạt động vào các dịch vụ thanh toán trực tuyến, các tháng khuyến mãi của các hãng lớn. Mới đây theo các chuyên gia an ninh mạng thì tội phạm đang lợi dụng thảm họa động đất sóng thần vừa xảy ra ở Nhật Bản để thực hiện những hành vi lừa đảo, phá hoại.

Hiện tại mạng xã hội ở Việt Nam đang phát triển mạnh mẽ, ở đó là nơi hội tụ của tất cả người dùng trong đó có người dùng với ý đồ xấu, dùng mạng xã hội để thực hiện mục đích xấu. Virus máy tính, phần mềm mã độc có tốc độ lây lan rất nhanh, sự phá hoại của virus giờ đây không đơn giản chỉ là phá hoại máy tính và đánh cắp thông tin cá nhân hay thẻ tín dụng của người dùng, mà đã chuyển hướng sang các hạ tầng công nghiệp của các quốc gia. Năm 2010 đã có gần 60 triệu máy tính bị nhiễm virus. Trung bình một ngày có hơn 160.000 máy tính bị nhiễm virus. Đây là con số đáng báo động về tình hình máy tính bị nhiễm virus tại Việt Nam. Đã có hơn 57.000 dòng virus mới xuất hiện. Virus lây lan nhiều nhất qua các máy tính vẫn là virus Conficker. Trong năm 2010 đã có tới 6,5 triệu lượt máy tính bị nhiễm loại virus này. Có hơn 1,4 triệu lượt máy tính đã bị nhiễm dòng virus giả mạo thư mục, giả mạo file ảnh, file word, excel….Virus siêu đa hình vẫn là một thách đố đối với các phần mềm diệt virus. Các virus siêu đa hình tiếp tục đứng trong top 3 với những virus lây nhiễm nhiều nhất trong năm và là nỗi ám ảnh với người sử dụng máy tính tại Việt Nam. Với khả năng "thay hình đổi dạng" để lẩn trốn, 2 dòng virus Vetor và Sality đã lan truyền trên 5,9 triệu lượt máy tính. Năm 2010 đã đánh dấu sự quay trở lại của virus phá hủy dữ liệu, đây sẽ là mối đe dọa lớn đối với dữ liệu của người sử dụng trong thời gian tới. Trong năm đã phát hiện những đợt virus phá hủy dữ liệu với các hình thức tấn công đơn giản như xóa, ghi đè dữ liệu. Các dòng virus phá hủy dữ liệu mới được trang bị các kỹ thuật lây lan nhanh qua Internet, nên tốc độ phát tán nhanh những virus phá hủy dữ liệu trước đây. Do vậy, mức độ nguy hiểm sẽ cao hơn rất nhiều. Với xu hướng tập trung nhiều dữ liệu quan trọng trên máy tính như hiện nay, virus phá dữ liệu quay trở lại với tốc độ lây lan nhanh chóng, sẽ gây ra những hậu quả khôn lường khi lây lan trên diện rộng. Trong năm 2010 đã bùng nổ nhiều phần mềm diệt virus giả mạo.

Đã có 2,2 triệu phần mềm xuất hiện trong năm 2010, gấp 8.5 lần so với con số 258.000 của năm 2009. Các phần mềm virus giả mạo này được mời chào rất nhiều trên các trang quảng cáo, có giao diện tương tự như các phần mềm có bản quyền. Tất cả các phần mềm diệt virus giả mạo này đều là những phần mềm mã độc, khi tải về, cài đặt trên máy nó sẽ tạo ra các lỗ hổng để hacker điều khiển máy tính. Đã phát hiện được một số nhóm hacker xâm nhập vào các hệ thống mạng tại nước ta sau đó cài cắm virus, các phần mềm mã độc, xây dựng, mở rộng mạng bootnet. Trong năm 2010 đã đánh dấu sự phát triển nở rộ của các mạng bootnet, việc công khai rao bán, sử dụng các hệ thống mạng bootnet diễn ra công khai trên mạng. Đây là tình trạng đáng báo động đối với các hệ thống lớn vì chúng có thể bị tấn công bất cứ lúc nào. Hiện nay tại nước ta đã có hàng chục nghìn máy tính bị nhiễm phần mềm mã độc và đã trở thành agent của các mạng bootnet bị hacker điều khiển.

Điện thoại không chỉ có chức năng nghe gọi mà nó còn được sử dụng như một máy tính chuyên dụng vì vậy virus trên điện thoại di động không còn là một định nghĩa mới mẻ nữa, mặt khác nó còn phát triển, lây lan ngày càng nhiều. Hiện nay việc đánh cắp tài khoản, thông tin cá nhân của người trên điện thoại di động, được hacker tận dụng và khả năng thành công rất cao thông qua tin nhắn hoặc thực hiện các cuộc gọi. Cùng với sự phát triển của 3G, người sử dụng sẽ dễ dàng truy cập Internet chỉ bằng một vài phím bấm trên điện thoại di động. Điều này cũng gia tăng các nguy cơ tấn công của virus đối với điện thoại di động. Sau máy vi tính, điện thoại di động ngày nay đã trở thành "con mồi" mới cho giới tội phạm công nghệ cao. Hàng loạt mẫu virus đã tấn công trực tiếp vào điện thoại di động, nhằm làm tê liệt phần mềm hệ thống, thay đổi mật khẩu, từ đó dễ dàng đánh cắp toàn bộ dữ liệu bên trong máy và tự phát tán qua những máy điện thoại di động khác thông qua danh bạ hoặc sóng wifi. Xét về mức độ nguy hiểm thì bị virus tấn công qua điện thoại di động nguy hiểm gấp nhiều lần so với bị tấn công qua máy tính và mạng Internet, bởi vì hầu như tất cả máy điện thoại di động đều không được cài đặt phần mềm ngăn chặn hoặc diệt virus.

Việt Nam vẫn thuộc các nước có tỷ lệ phát tán Spam mail cao nhất thế giới. Năm 2009 đứng trong top 10, năm 2010 đứng trong top 5 chỉ sau Mỹ, Brazil, Ấn

Độ, Nga. Tại Việt Nam bắt đầu xuất hiện các email lừa đảo bằng tiếng Việt, loại email này trước đây chỉ tồn tại dưới dạng tiếng Anh. Đã xuất hiện dịch vụ trao đổi, mua bán các thông tin cá nhân của khách hàng như số điện thoại di động, địa chỉ thư điện tử,….đây là tác nhân thúc đẩy số lượng spam mail phát tán từ nước ta tăng nhanh.

Với hiện trạng an toàn thông tin ở Việt Nam như vậy, chính phủ đã đưa ra các văn bản pháp lý định hướng, các sự kiện an toàn thông tin liên tục diễn ra đã góp phần nâng cao nhận thức về an toàn thông tin cho các cá nhân, tổ chức. Vào năm 2010 thủ tướng đã ký ban hành Quy hoạch An toàn thông tin quốc gia từ năm 2010 tới năm 2020, đây là văn bản chính thức đầu tiên của Việt Nam đề cập toàn diện, sâu sắc đến lĩnh vực An toàn thông tin, đóng vai trò "lịch sử" đối với ngành ATTT Việt Nam. Bộ Thông tin và Truyền thông công bố thông điệp về an toàn thông tin tại Ngày an toàn thông tin năm 2010, đây là hành động có ý nghĩa nhằm kêu gọi các cá nhân, tầng lớp, các ngành liên quan cùng chung tay vì lĩnh vực ATTT tại Việt Nam.

Tại Việt Nam đã có những hệ thống CA công cộng được hình thành, các chuyên gia Việt Nam phát hiện các lỗi an ninh trong ASP.net của Microsoft và cuộc thi sinh viên với an toàn thông tin từ việc chỉ có phạm vi ở toàn Miền Bắc nhưng vào năm 2010 đã được mở rộng phạm vi trên toàn quốc tế. Cũng vào năm 2010 thì Việt Nam liên tục có tên trong nhiều danh sách của quốc tế về các vấn đề liên quan tới công nghệ thông tin.

Như vậy việc bảo vệ người dùng đầu cuối trong mạng thông tin và viễn thông dần trở thành những vấn đề nóng. Phần lớn các ngân hàng, doanh nghiệp đã có website cung cấp thông tin, dịch vụ nhưng chưa xây dựng giải pháp tổng thể về bảo mật nên thường họ không phát hiện được các hacker xâm nhập bất hợp pháp, lấy cắp các dữ liệu. Sự phổ biến của web 2.0: các mạng xã hội như facebook, twitter, blog, podcast và wiki làm nảy sinh hàng loạt các thách thức đảm bảo an toàn thông tin và giao dịch trực tuyến. Vậy hiện trạng ATTT ở Việt Nam đang rất cấp bách đòi hỏi sự quan tâm hơn nữa của các doanh nghiệp và nhà nước nhằm bảo vệ tài sản thông tin khỏi sự "nhòm ngó" của các hacker mũ đen.

CHƯƠNG II

TỔNG QUAN VỀ ISO/IEC 27001:2005

2.1 Giới thiệu bộ tiêu chuẩn ISO/IEC 27000.

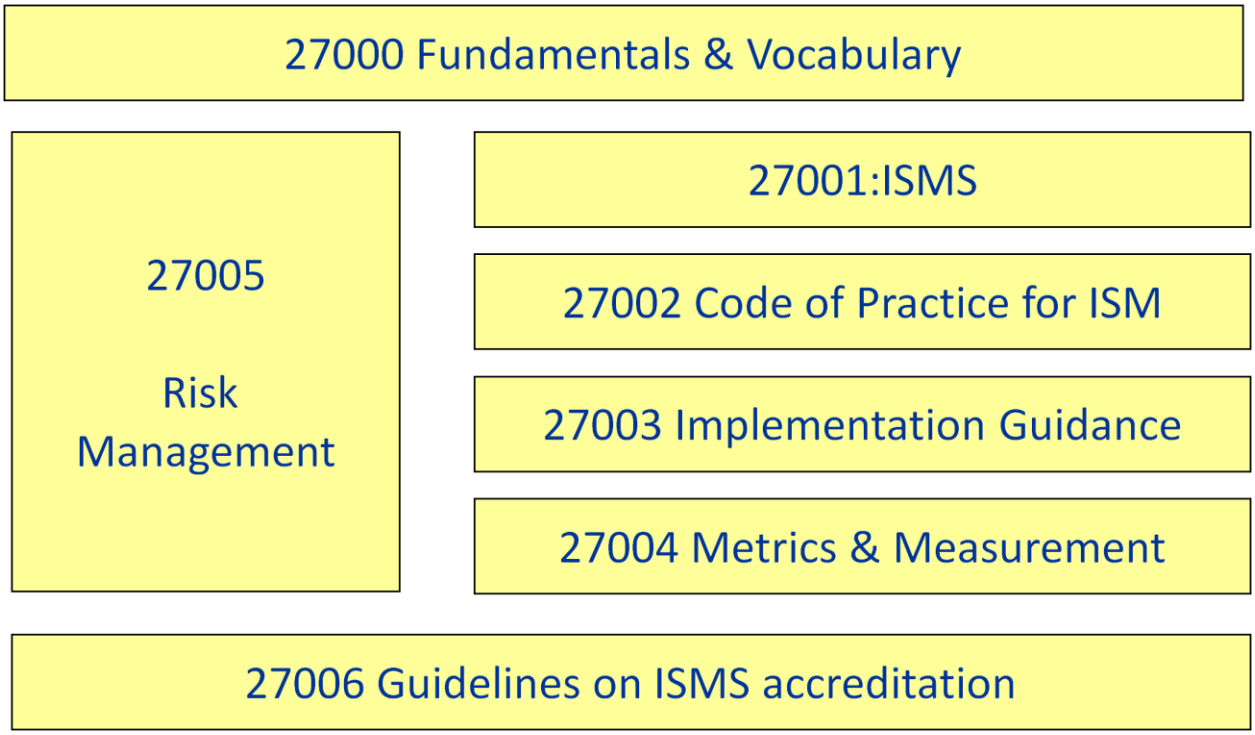
Trong bối cảnh có sự phát triển như vũ bão của công nghệ thông tin, ngày càng nhiều các tổ chức, đơn vị, doanh nghiệp hoạt động lệ thuộc gần như hoàn toàn vào hệ thống mạng máy tính, máy tính, và cơ sở dữ liệu. Nói cách khác, khi hệ thống công nghệ thông tin hoặc cơ sở dữ liệu gặp các sự cố thì hoạt động của các đơn vị này bị ảnh hưởng nghiêm trọng và thậm chí có thể bị tê liệt hoàn toàn. Một trong các biện pháp phòng ngừa được nhắc đến trong thời gian qua chính là triển khai áp dụng Hệ thống Quản lý An toàn Thông tin (ISMS: Information Security Management System) theo các nguyên tắc của bộ tiêu chuẩn quốc tế ISO 27000. ISO (the International Organation for Standardization - Tổ chức tiêu chuẩn quốc tế) và IEC (the International Electrotechnical Commission - Hội đồng kỹ thuật quốc tế) là tổ chức thiết lập các hệ thống tiêu chuẩn trên toàn cầu. Các quốc gia là các thành viên của ISO và IEC tham gia vào sự phát triển chung của các chuẩn quốc tế thông qua các ủy ban được thiết lập bởi các tổ chức tương ứng nhằm giải quyết các lĩnh vực cụ thể về kỹ thuật. ISO và IEC phối hợp trong các lĩnh vực liên quan đến lợi ích của nhau. Có thể nói rằng, ISO 27000 là một phần của hệ thông quản lý chung trong tổ chức, được thực hiện dựa trên nguyên tắc tiếp cận các rủi ro trong hoạt động, để thiết lập, áp dụng, thực hiện, theo dõi, xem xét, duy trì và cải tiến đảm bảo an toàn thông tin của tổ chức.

Cho tới nay, việc áp dụng hệ thống quản lý an toàn thông tin phù hợp ISO 27000 đã được triển khai rộng khắp ở hầu hết các quốc gia trên thế giới đặc biệt là

trong lĩnh vực tài chính ngân hàng. Tại Việt Nam, một số ngân hàng cũng đang triển khai áp dụng hệ thống này và bước đầu đã có được những kết quả nhất định.

Xét về lịch sự hình thành của bộ tiêu chuẩn, ISO 27000 cũng có nguồn gốc từ Anh quốc. Bắt đầu vào năm 1992, Phòng Thương mại và Công nghiệp Anh (UK Department Trade and Industrial) ban hành ra qui phạm thực hành về hệ thống an toàn thông tin dựa trên các hệ thống đảm bảo an toàn thông tin nội bộ của các công ty dầu khí. Tài liệu này sau đó được Viện tiêu chuẩn hoá Anh chính thức ban hành thành tiêu chuẩn quốc gia với mã hiệu BS 7799-1 vào năm 1995. Năm 2000, tiêu chuẩn này được Tổ chức Tiêu chuẩn hoá Quốc tế (ISO) chính thức chấp nhận và ban hành với mã hiệu ISO/IEC 17799:2000 - tiền thân của bộ tiêu chuẩn ISO 27000 ngày nay.

Hình dưới đây sẽ mô tả cấu trúc của bộ tiêu chuẩn ISO 27000:



Hình 2: Cấu trúc bộ tiêu chuẩn ISO 27000

Bộ tiêu chuẩn ISO 27000 đã và sẽ bao gồm những tiêu chuẩn cụ thể sau:

- ISO 27000 quy định các vấn đề về từ vựng và định nghĩa (thuật ngữ)

- ISO 27001:2005 xác định các yêu cầu đối với hệ thống quản lý an toàn thông tin
- ISO 27002:2007 đưa ra qui phạm thực hành mô tả mục tiêu kiểm soát an toàn thông tin một các toàn diện và bảng lựa chọn kiểm soát thực hành an toàn tốt nhất
- ISO 27003:2007 đưa ra các hướng dẫn áp dụng
- ISO 27004:2007 đưa ra các tiêu chuẩn về đo lường và định lượng hệ thống quản lý an toàn thông tin để giúp cho việc đo lường hiệu lực của việc áp dụng ISMS
- ISO 27005:2007 tiêu chuẩn về quản lý rủi ro an toàn thông tin
- ISO 27006 tiêu chuẩn về hướng dẫn cho dịch vụ khôi phục thông tin sau thảm hoạ của công nghệ thông tin và viễn thông

Theo con số thống kê chưa đầy đủ thì hiện nay số lượng các tổ chức đã áp dụng ISMS và đã được chứng nhận trên toàn thế giới là 2063 trong đó đứng đầu là Nhật Bản với số chứng chỉ được cấp ra là 1190 sau đó là Anh 219, Đài loan 69...

Tiêu chuẩn ISO/IEC 27001:2005 mang tính tổng quát và để áp dụng cho mọi tổ chức không phân biệt loại hình, quy mô và bản chất hoạt động của tổ chức. ISO 27001 là tiêu chuẩn cho Hệ thống quản lý An toàn thông tin (Information Security Management Systems - ISMS) nhằm cung cấp một framework cho việc khởi tạo, triển khai, duy trì và văn bản hoá các vấn đề về an toàn thông tin trong một cơ quan tổ chức. Các lĩnh vực áp dụng đối với ISMS cũng chiếm các tỉ lệ khác nhau. Ví dụ lĩnh vực viễn thông được áp dụng nhiều nhất với 27% tổng số lượng chứng chỉ cấp ra, Lĩnh vực tài chính ngân hàng chiếm 20%, Lĩnh vực công nghệ thông tin chiếm 15%,.. các tổ chức áp dụng ISMS để có thể giảm thiểu các rủi ro liên quan tới an toàn thông tin, đảm bảo cho sự phát triển bền vững.

2.2 Giới thiệu về ISO/IEC 27001:2005

ISO (the International Organation for Standardization - Tổ chức tiêu chuẩn quốc tế) và IEC (the International Electrotechnical Commission - Hội đồng kỹ

thuật quốc tế) là tổ chức thiết lập các hệ thống tiêu chuẩn trên toàn cầu. Các quốc gia là các thành viên của ISO và IEC tham gia vào sự phát triển chung của các chuẩn quốc tế thông qua các ủy ban được thiết lập bởi các tổ chức tương ứng nhằm giải quyết các lĩnh vực cụ thể về kỹ thuật. ISO và IEC phối hợp trong các lĩnh vực liên quan đến lợi ích của nhau. Các tổ chức quốc tế khác trong mối quan hệ với ISO, IEC, thuộc chính phủ cũng như phi chính phủ đều tham gia vào công việc chung của ISO và IEC.

Các chuẩn quốc tế được dự thảo nhằm phù hợp với các quy tắc đã đưa ra trong ISO/IEC. Trong lĩnh vực công nghệ thông tin, ISO và IEC đã thiết lập một hội đồng kỹ thuật chung ISO/IEC JTC 1. Bản dự thảo chuẩn quốc tế ISO/IEC đã được chấp nhận bởi hội đồng kỹ thuật chung được đưa đến các quốc gia để bầu cử. Sự xuất bản như một chuẩn quốc tế yêu cầu sự chấp thuận chung của ít nhất là 75% các quốc gia.

ISO và IEC sẽ không được nắm giữ các trách nhiệm cho việc phát triển và các quyền sáng chế. Chuẩn quốc tế ISO/IEC 27001:2005 được chuẩn bị bởi hội đồng kĩ thuật chung ISO/IEC JTC 1, Công nghệ thông tin, tiểu ban SC 27, kĩ thuật bảo mật thông tin.

2.3 Lịch sử phát triển của ISO/IEC 27001:2005

ISO 27001:2005 ban đầu được phát triển trên chuẩn BS7799 của Viện các chuẩn Anh quốc (British Standards Institution BSI). BS7799 bắt đầu phát triển từ những năm 1990 nhằm đáp ứng các yêu cầu cho doanh nghiệp, chính phủ và công nghiệp về việc thiết lập cấu trúc an ninh thông tin chung. Năm 1995, chuẩn BS7799 đã được chính thức công nhận.

Tháng 5 năm 1999 phiên bản chính thứ 2 của chuẩn BS7799 được phát hành với nhiều cải tiến chặt chẽ. Trong thời gian này Tổ chức thế giới về chuẩn (ISO) đã bắt đầu quan tâm đến chuẩn này. Tháng 12 năm 2000, ISO đã tiếp quản phần đầu của BS7799, đổi tên thành ISO 17799 và như vậy chuẩn an toàn thông tin này bao gồm ISO 17799 (mô tả Qui tắc thực tế cho hệ thống quản lý an ninh thông tin) và BS7799 (đặc tính kỹ thuật cho hệ thống an ninh thông tin. Trong tháng 9 năm

2002, soát xét phần 2 của chuẩn BS7799 được thực hiện để tạo sự nhất quán với các chuẩn quản lý khác như ISO 9001:2000 và ISO 14001:1996 cũng như với các nguyên tắc chính của Tổ chức Hợp tác và phát triển kinh tế (OECD).

Ngày 15 Tháng 10 năm 2005 ISO phát triển ISO 17799 và BS7799 thành ISO 27001:2005 và chú trọng vào công tác đánh giá và chứng nhận. ISO 27001 thay thế một cách trực tiếp cho BS7799-2:2002, nó định nghĩa hệ thống ISMS và hướng đến cung cấp một mô hình cho việc thiết lập, thi hành, điều hành, kiểm soát, xem xét, duy trì và cải tiến ISMS. Chuyển tiếp BS7799 (BS7799 Transition) dành cho các tổ chức đã được chứng nhận BS7799 sẽ được ghi nhận giai đoạn chuyển tiếp cho việc chuyển đổi sang chuẩn mới ISO 27001. Sự thu hút của chuẩn phát triển một cách mạnh mẽ trong 10 năm qua, đặc biệt là trong vài năm gần đây. Theo ISMS International User Group, trong năm 2002, khoảng 200 tổ chức trên thế giới đã đạt được chứng chỉ BS7799. Hôm nay con số này tăng lên 1.870. Theo kết quả khảo sát của Ernst & Young's Global Information Security Survey, sự quan tâm đến chuẩn đang tăng lên, trong số 1,300 tổ chức toàn cầu được khảo sát, ¼ trong số đó đã thừa nhận chuẩn an ninh và nhiều hơn 30% đang có kế hoạch để triển khai.

Chuẩn quốc tế này được chuẩn bị để cung cấp một mô hình cho việc thiết lập, thực thi, điều hành, theo dõi, xem xét, duy trì và cải tiến một hệ thống quản lý an toàn thông tin (ISMS). Việc thực hiện một ISMS nên là một quyết định chiến lược cho một tổ chức. Thiết kế và thực thi ISMS của tổ chức phụ thuộc vào các nhu cầu, các mục tiêu, các yêu cầu bảo mật, các quy trình làm việc, kích cỡ và cấu trúc của tổ chức. Và hệ thống hỗ trợ của họ phải được dự kiến để thay đổi theo thời gian. Điều này được dự định là thực thi một ISMS sẽ được thực hiện theo nhu cầu của tổ chức. Ví dụ như một tình huống đơn giản đòi hỏi một giải pháp ISMS đơn giản. Chuẩn ISO/IEC 27001:2005 có thể được sử dụng để đánh giá sự phù hợp với các thành phần quan tâm ở bên trong và các thành phần quan tâm ở bên ngoài.

2.4 Các phương pháp tiếp cận.

Chuẩn quốc tế ISO/IEC 27001:2005 áp dụng một số các phương pháp tiếp cận việc thiết lập, thực thi, điều hành, theo dõi, xem xét, duy trì và cải tiến ISMS của một tổ chức. Một tổ chức cần phải xác định và quản lý nhiều hoạt động để các

chức năng đó có hiệu quả. Bất kì một hành động nào sử dụng tài nguyên và việc quản lý để cho phép việc chuyển đổi đầu vào thành đầu ra đều được coi là một quá trình. Thường thì đầu ra từ một quá trình trực tiếp hình thành đầu vào của quá trình tiếp theo.

Việc áp dụng một hệ thống các quá trình đối với một tổ chức, cùng với sự nhận biết và sự tương tác của các quá trình đó và việc quản lý của họ có thể được gọi là một "phương pháp tiếp cận". Các phương pháp tiếp cận cho một hệ thống quản lý an toàn thông tin được trình bày trong tiêu chuẩn quốc tế này khuyến khích người sử dụng nó nhấn mạnh tầm quan trọng của những điều sau:

- Hiểu rõ được các yêu cầu bảo mật an toàn thông tin của tổ chức, các chính sách cần thiết lập và các mục tiêu của việc bảo mật thông tin.
- Thực thi và điều hành kiểm soát để quản lý các rủi ro an toàn thông tin của tổ chức trong bối cảnh rủi ro kinh doanh của toàn bộ tổ chức.
- Theo dõi và xem xét việc thực thi và tính hiệu quả của ISMS
- Tiếp tục cải tiến ISMS dựa trên việc đo lường một cách khách quan.

Chuẩn này tuân theo mô hình PDCA (Plan - Do - Check - Act) cái mà được áp dụng với tất cả các tiến trình ISMS. PDCA minh họa việc làm thế nào để một ISMS đưa ra như các đầu vào yêu cầu an toàn thông tin, sự mong đợi của các bên quan tâm, thông qua các hành động cần thiết và đưa ra các sản phẩm an toàn thông tin đáp ứng được những yêu cầu và sự mong đợi.

Việc áp dụng mô hình PDCA sẽ phản ánh những nguyên tắc được quy định trong hướng dẫn OECD (2002) về việc điều chỉnh bảo mật hệ thống thông tin và mạng. Chuẩn quốc tế này cung cấp một mô hình mạnh mẽ để thực thi các quy định trong những hướng dẫn về việc điều chỉnh đánh giá rủi ro, thiết kế bảo mật, thực thi, bảo đảm việc quản lý và đánh giá lại.

Ví dụ:

Một yêu cầu có thể là vi phạm an toàn hệ thống sẽ không gây ra thiệt hại nghiêm trọng về mặt tài chính cho tổ chức và/hoặc sẽ gây bối rối cho tổ chức. Một

mong đợi có thể hiểu được rằng nếu một sự cố nghiêm trọng xảy ra - có thể trang thương mại điện tử của tổ chức bị hack - và phải có người được đào tạo đầy đủ trong một chương trình đào tạo phù hợp để giảm thiểu tác động đó.

2.5 Khả năng tương thích với các hệ thống khác

Tiêu chuẩn ISO/IEC 27001:2005 phù hợp với các chuẩn ISO 9001:2000 và ISO 14001:2004 để chắc chắn hỗ trợ và tích hợp việc thực thi, hoạt động với các tiêu chuẩn quản lý liên quan. Một hệ thống quản lý được thiết kế phù hợp có thể đáp ứng yêu cầu của tất cả các chuẩn. Các chuẩn quốc tế này được thiết kế để cho phép một tổ chức sắp xếp hoặc tích hợp ISMS của chúng với các yêu cầu quản lý hệ thống liên quan.

2.6 Lợi ích của việc sử dụng ISO/IEC 27001:2005

Việc tuân theo hoặc đạt được chứng chỉ chuẩn ISO 27001:2005 không thể chứng minh tổ chức được đảm bảo an toàn 100%. Không có điều gì là an ninh hoàn toàn ngoại trừ không làm gì cả. Tuy nhiên, sự thừa nhận chuẩn quốc tế này đưa ra những lợi ích chắc chắn mà người quản lý cần phải xem xét.

a. Cấp độ tổ chức

Sự cam kết: Chứng chỉ như là một cam kết hiệu quả của nỗ lực đưa an ninh của tổ chức đạt tại các cấp độ và chứng minh sự cần cù thích đáng của chính những người quản trị.

b. Cấp độ pháp luật

Tuân thủ: chứng minh cho nhà chức trách rằng tổ chức đã tuân theo tất cả các luật và các qui định áp dụng ngoài ra nó cũng giúp cho tổ chức "hoàn vốn đầu tư" nhanh nhất - nếu một tổ chức phải tuân thủ các quy định khác nhau liên quan tới bảo vệ dữ liệu, bảo mật và quản trị CNTT thì ISO 27001 có thể mang lại các phương pháp cho phép tổ chức làm những điều đó một cách có hiệu quả nhất. Điều quan trọng là chuẩn đã bổ sung những gì mà chuẩn và luật đã tồn tại khác chưa đề cập tới.

c. Cấp độ điều hành

Quản lý rủi ro: Mang lại những hiểu biết tốt hơn về các hệ thống thông tin, điểm yếu của chúng và làm thế nào để bảo vệ chúng. Tương tự, nó đảm bảo khả năng sẵn sàng ở cả phần cứng và phần mềm.

d. Cấp độ thương mại

Sự tín nhiệm và tin cậy: Các thành viên, cổ đông, và khách hàng vững tin khi thấy khả năng và sự chuyên nghiệp của tổ chức trong việc bảo vệ thông tin. Chứng chỉ có thể giúp nhìn nhận riêng từ các đối thủ cạnh tranh trong thị trường.

e. Cấp độ tài chính

Thông tin bảo mật thường được coi là một chi phí không được tính rõ ràng. Tuy nhiên bạn vẫn có thể tính được tài chính nếu bạn giảm các phí tổn do các sự cố gây ra. Có thể không gây ra việc gián đoạn các dịch vụ hoặc bị rò rỉ dữ liệu hoặc nhận được sự bất mãn của nhân viên. ISO/IEC 27001:2005 sẽ giúp cho tổ chức tiết kiệm chi phí khắc phục các lỗ hổng an ninh và có khả năng giảm chi phí bảo hiểm.

f. Cấp độ con người

Cải tiến nhận thức của nhân viên về các vấn đề an ninh và trách nhiệm của họ trong tổ chức. Chuẩn này giúp các tổ chức xác định được tính chịu trách nhiệm của con người đối với một tài sản nhất định, xác định được người đã cho phép những người nào đã truy cập vào hệ thống thông tin….do đó người trong tổ chức sẽ ý thức được trách nhiệm, quyền lợi và nghĩa vụ của mình trong tổ chức đó hơn.

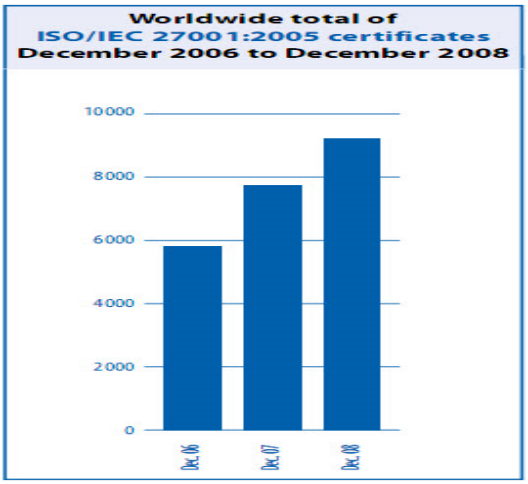
2.7 Tình hình áp dụng ISO/IEC 27001:2005

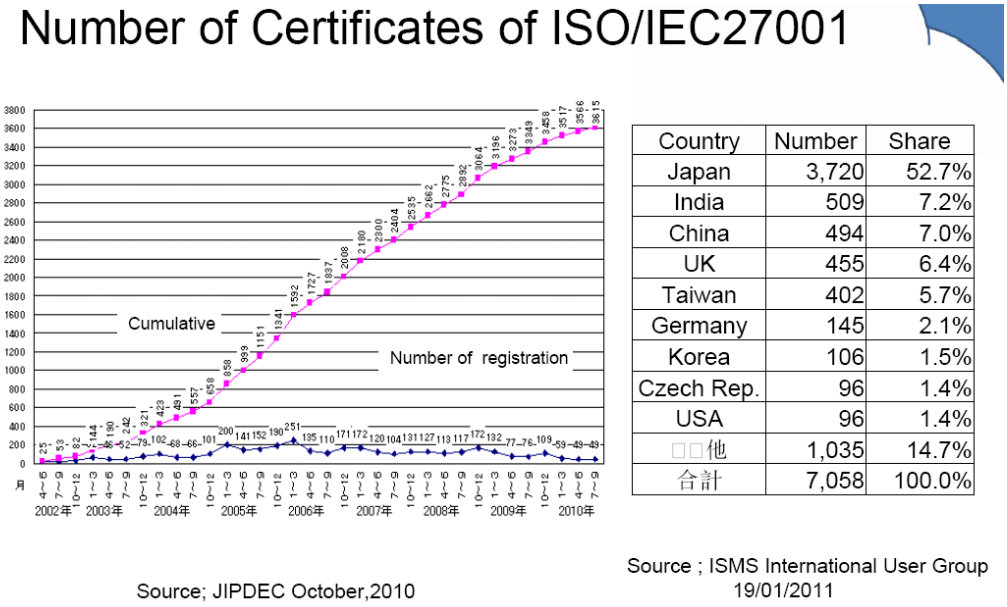
2.7.1 Tình hình áp dụng ISO/IEC 27001:2005 trên thế giới

Theo Tổ chức Tiêu chuẩn hóa Thế giới (ISO), tính đến thời điểm khảo sát gần đây nhất (năm 2008) các hệ thống về an toàn thực phẩm và bảo mật thông tin đang tăng mạnh. Trên thế giới đã có khoảng 25.000 đơn vị áp dụng tiêu chuẩn ISO/IEC 27001:2005 về hệ thống quản lý an toàn thông tin.

ISO / IEC 27001:2005 là tiêu chuẩn đưa ra các yêu cầu cho hệ thống quản lý an toàn thông tin. Vào cuối năm 2008, có ít nhất 9246 ISO / IEC 27001:2005 được

cấp giấy chứng nhận ở 82 quốc gia và nền kinh tế. Như vậy năm 2008 tiêu chuẩn ISO / IEC 27001 tăng là 1514 chứng chỉ so với năm 2007 trên tổng số là 7732 tại 70 quốc gia. Tỉ lệ tăng trưởng là 94% so với năm 2007 là 90%.





Country	Number	Share
Japan	3,720	52.7%
India	509	7.2%
China	494	7.0%
UK	455	6.4%
Taiwan	402	5.7%
Germany	145	2.1%
Korea	106	1.5%
Czech Rep.	96	1.4%
USA	96	1.4%
□□他	1,035	14.7%
合計	7,058	100.0%

Source; JIPDEC October,2010

Source ; ISMS International User Group
19/01/2011

Hình 3: Tình hình áp dụng ISO/IEC 27001:2005 trên thế giới

2.7.2 Tình hình áp dụng chuẩn ISO/IEC 27001:2005 tại Việt Nam

Tại Việt Nam, tiêu chuẩn quốc tế ISO/IEC 27001 đã được nhiều cơ quan và đơn vị có ứng dụng các hệ thống thông tin nghiên cứu và quan tâm áp dụng. Tuy nhiên do việc chuẩn hóa công tác quản lý nói chung và quản lý công nghệ thông tin nói riêng là chưa tốt nên phát sinh khá nhiều vướng mắc. Mặc dù vậy hiện nay đã có một số công ty mạnh dạn áp dụng và được công nhận phù hợp tiêu chuẩn.

Tháng 1/2007 công ty đầu tiên của Việt Nam là FCG Việt Nam đã được chứng nhận phù hợp ISO/ IEC 27001: 2005

Tháng 3/2007 Công ty Hệ thống thông tin FPT thông báo đã được công nhận phù hợp tiêu chuẩn này sau 8 tháng triển khai. Tiêu chuẩn này đã giúp các công ty giảm thiểu rủi ro an toàn thông tin có thể xảy ra cũng như nâng cao uy tín của công ty đặc biệt đối với các khách hàng nước ngoài.

Đến tháng 8/2008, tại Việt Nam đã có gần 20 tổ chức được cấp chứng chỉ phù hợp ISO/ IEC 27001: 2005 và có gần 50 tổ chức sẽ được cấp chứng chỉ ISO/ IEC 27001: 2005 trong thời gian tới nhất là đối với các tổ chức tài chính, ngân hàng, các tổ chức sản xuất, gia công phần mềm. Tháng 4/ 2009, Sở Khoa học Công nghệ Đồng Nai là đơn vị Hành chính công đầu tiên của Việt Nam đã được Tổ chức Chứng nhận DAScertification (Vương Quốc Anh) cấp chứng chỉ ISMS nhằm nâng cao hiệu lực công tác Quản lý Nhà nước và ứng dụng Công nghệ Thông tin thông qua việc sử dụng hệ thống văn phòng điện tử với cổng cách ly phi chuẩn. Tương lai của chứng chỉ ISO 27001 sẽ thu hút mối quan tâm mạnh mẽ như tiêu chuẩn chất lượng ISO 9000 của những năm 90.

Far East	Dec. 2006	Dec. 2007	Dec. 2008
Philippines	10	24	27
Singapore	7	17	36
Thailand	7	9	16
Viet Nam	1	2	7

Hình 4: Tình hình áp dụng ISO/IEC 27001:2005 tại Châu Á

CHƯƠNG III
TRIỂN KHAI ISO/IEC 27001:2005 TRONG THỰC TẾ

3.1 Thuật ngữ và định nghĩa

3.1.1 Tài sản

Bất kì những thứ gì có giá trị đối với tổ chức [ISO/IEC 13335 - 1:2004]

3.1.2 Sẵn sàng

Tài sản được truy cập và được sử dụng theo nhu cầu của một tổ chức có thẩm quyền [ISO/IEC 13335 - 1:2004]

3.1.3 Bí mật

Tài sản là thông tin không được cung cấp hoặc tiết lộ cho các cá nhân không có thẩm quyền [ISO/IEC 13335 - 1: 2004]

3.1.4 Bảo mật thông tin

Bảo đảm tính bí mật, tính toàn vẹn và tính sẵn sàng của thông tin, thêm vào đó còn có một số tính chất khác như tính xác thực, tính chịu trách nhiệm, tính không chối bỏ, độ tin cậy cũng có thể kể đến. [ISO/IEC 17799:2005]

3.1.5 Sự kiện an toàn thông tin

Một sự xuất hiện được xác định của một hệ thống, một dịch vụ hoặc một mạng trong tình trạng cho thấy có thể có một sự vi phạm vào chính sách an toàn thông tin hay làm thất bại các biện pháp bảo vệ hoặc một tình thế chưa biết có thể sẽ liên quan đến bảo mật [ISO/IEC TR 18044:2004]

3.1.6 Các sự cố an toàn thông tin

Một loạt hoặc một sự kiện bảo mật thông tin không mong muốn hoặc không được kể đến có một xác suất lớn ảnh hưởng đến các hoạt động kinh doanh và đe dọa an toàn thông tin [ISO/IEC TR 18044:2004]

3.1.7 Hệ thống quản lý an toàn thông tin ISMS

Là một phần của toàn bộ hệ thống quản lý, dựa trên các phương pháp tiếp cận rủi ro kinh doanh, để thiết lập, thực thi, điều hành, theo dõi, xem xét, duy trì và cải tiến an toàn thông tin.

Chú ý: Hệ thống quản lý bao gồm cấu trúc, chính sách, kế hoạch hoạt động, việc chịu trách nhiệm, việc thực hành, các thủ tục, các quy trình và các tài nguyên của tổ chức.

3.1.8 Toàn vẹn

Đảm bảo tính chính xác và đầy đủ của tài sản [ISO/IEC 13335 - 1:2004]

3.1.9 Các rủi ro còn lại

Các nguy cơ rủi ro còn lại sau khi rủi ro đã được khắc phục [hướng dẫn ISO/IEC 73:2002]

3.1.10 Chấp nhận rủi ro

Quyết định chấp nhận một rủi ro [hướng dẫn ISO/IEC 73:2002]

3.1.11 Phân tích rủi ro.

Có hệ thống sử dụng thông tin để xác định các nguồn và để ước tính các rủi ro. [Hướng dẫn ISO/IEC 73:2002]

3.1.12 Đánh giá rủi ro

Toàn bộ quá trình phân tích rủi ro và định giá rủi ro [Hướng dẫn ISO/IEC 73:2002]

3.1.13 Định giá rủi ro

Quá trình so sánh các ước tính nguy cơ rủi ro đối với các tiêu chí nhất định để xác định tầm quan trọng của các rủi ro đó. [Hướng dẫn ISO/IEC 73:2002]

3.1.14 Quản lý rủi ro

Các hoạt động phối với việc hướng dẫn và kiểm sóat một tổ chức về vấn đề rủi ro [Hướng dẫn ISO/IEC 73:2002]

3.1.15 Khắc phục rủi ro

Quá trình lựa chọn và thực hiện đo lường để sửa đổi rủi ro [hướng dẫn ISO/IEC 73:2002]

Chú ý: Trong chuẩn này thuật ngữ "kiểm soát" là được sử dụng như một từ đồng nghĩa với từ "đo lường"

3.1.16 Các tuyên bố được áp dụng(SOA)

Các tài liệu tuyên bố miêu tả các mục tiêu kiểm soát và các kiểm soát có liên quan và được áp dụng cho ISMS của tổ chức.

Chú ý: Các mục tiêu kiểm soát và các kiểm soát dựa trên các kết quả hay kết luận của việc đánh giá rủi ro và quy trình khắc phục rủi ro, các quy phạm pháp luật hoặc các quy định được yêu cầu, các nghĩa vụ hợp đồng và các yêu cầu kinh doanh cho việc bảo mật thông tin của tổ chức.

3.2 Cốt lõi của việc triển khai ISO/IEC 27001:2005

Hệ thống quản lý an toàn thông tin (ISMS) là trái tim của ISO/IEC 27001:2005 và là điều kiện tiên quyết cho việc thi hành và lấy chứng chỉ một cách toàn diện. Hệ thống quản lý thông tin (ISMS) là một phần của toàn bộ hệ thống quản lý, dựa trên các phương pháp tiếp cận rủi ro kinh doanh, để thiết lập, thực thi, điều hành, theo dõi, xem xét, duy trì và cải tiến an toàn thông tin. Một hệ thống ISMS phải quản lý tất cả các mặt của an toàn thông tin bao gồm con người, các quy trình và các hệ thống công nghệ thông tin. Điều cốt lõi để có hệ thống ISMS thành công là dựa trên đánh giá phản hồi để cung cấp sự cải tiến liên tục và lấy cách tiếp cận có cấu trúc để quản lý tài sản và rủi ro. ISMS phải được thiết kế để đảm bảo lựa chọn thích hợp và các kiểm soát bảo mật cân xứng để bảo vệ tài sản thông tin, cung cấp sự tin tưởng cho các bên quan tâm.

3.2.1 Khái niệm ISMS

Ý tưởng cơ bản đằng sau ISMS ở tiêu chuẩn ISO/IEC 27001:2005 là sự thiết lập, thực thi và duy trì một tập hợp các hệ thống quy trình quản lý nhằm đạt được an toàn thông tin một cách có hiệu quả. ISMS nên được xem như là một phần không thể thiếu của các tổ chức điều hành và văn hóa kinh doanh, dựa trên việc tiếp cận các rủi ro kinh doanh của tổ chức, gồm có tổ chức, cơ cấu, chính sách, lập kế hoạch hoạt động, trách nhiệm thi hành, các thủ tục, các quy trình và nguồn lực để cung cấp bảo mật thông tin hiệu quả.

3.2.2 Cung cấp bảo mật thông tin hiệu quả.

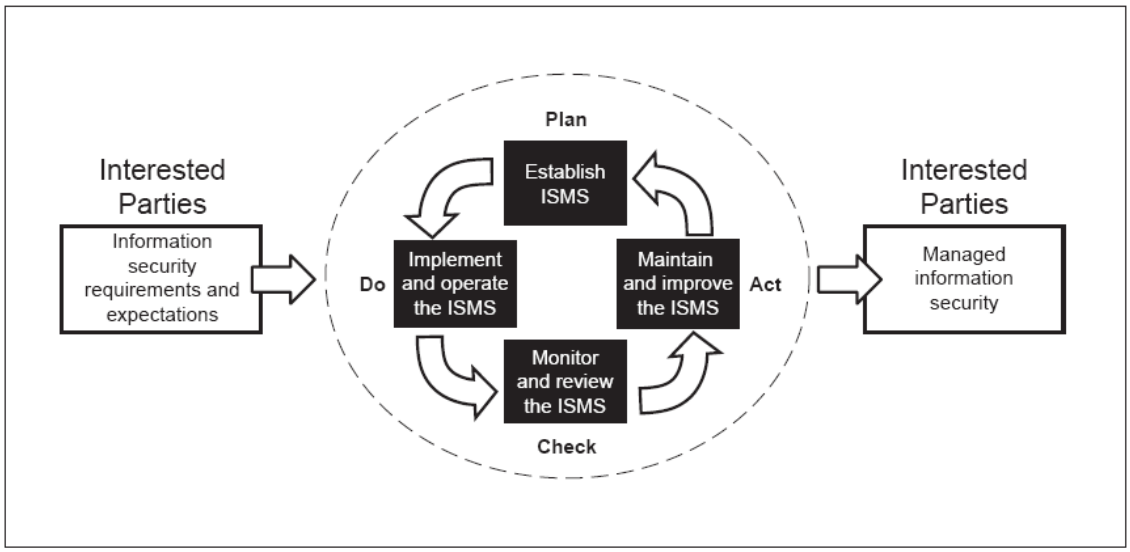
Không một tổ chức nào có thể hoạt động một cách thành công trong thế giới ngày nay mà thiếu bảo mật thông tin. ISMS nên được thiết kế để đảm bảo việc quản lý an toàn thông tin là đầy đủ và tương xứng, việc này được đặt ra nhằm bảo vệ tài sản thông tin của tổ chức và để cho các bên quan tâm có sự tin tưởng và sự đảm bảo. ISMS phải có khả năng thực hiện được thành công an toàn thông tin nếu điều này có ích và góp phần tích cực cho thành công của tổ chức. An toàn thông tin chủ yếu được đưa ra như một vấn đề quản lý thay vì đưa ra như một vấn đề về kỹ thuật hoặc về CNTT. Tuy nhiên ta không nên bỏ qua các vấn đề kỹ thuật, đặc biệt là sự phụ thuộc vào tính phổ biến của việc sử dụng CNTT.

3.2.3 Quá trình thực hiện

Quản lí an toàn thông tin không phải chỉ được làm một lần mà nó cần được liên tục cải tiến hoạt động (dựa trên mô hình PDCA) được thông qua bởi tiêu chuẩn ISO/IEC 27001:2005, cũng như các tiêu chuẩn hệ thống quản lý khác (ví dụ: ISO 9001 QMS requirement). Doanh nghiệp nào quản lý được tốt an toàn thông tin thì doanh nghiệp đó là một doanh nghiệp có tiềm năng. Hỗ trợ quản lý và cam kết hoạt động của ISMS là một trong những yếu tố trọng điểm để đạt được sự thành công và tính hiệu quả trong việc thực thi ISMS.

3.2.4 Mô hình PDCA

Mô hình PDCA được gọi là mô hình"Plan - Do - Check - Act", được sử dụng trong ISO/IEC 27001:2005. Mô hình này được sử dụng làm cơ sở cho việc thiết lập, thực thi, điều hành, theo dõi, rà soát, duy trì và cải tiến một ISMS.



Hình 5: Mô hình PDCA được áp dụng cho quy trình ISMS

- **Plan (Thiết lập ISMS)**: Thiết lập chính sách ISMS, đối tượng, tiến trình, thủ tục liên quan tới quản lý rủi ro và cải thiện vấn đề an toàn thông tin để cung cấp kết quả phù hợp với chính sách, đối tượng của tổ chức.
- **Do (Thực thi và điều hành ISMS)**: Thực thi và điều hành chính sách ISMS, kiểm soát, xử lý và thủ tục.
- **Check (theo dõi và rà sóat ISMS)**: Đánh giá, nơi được áp dụng, đo lường quá trình thực hiện đối với các chính sách ISMS, đối tượng và những kinh nghiệm trong thực thế, báo cáo kết quả để người quản lý xem xét.
- **Act (Duy trì và cải tiến ISMS)**: Tiến hành sửa chữa và ngăn ngừa các hành động, dựa trên kết quả của kiểm toán nội bộ ISMS và quản lý xem xét hoặc những thông tin khác có liên quan để có thể liên tục cải tiến ISMS.

3.3 Cốt lõi của việc quản lý rủi ro (Risk Management).

3.3.1 Quản lý rủi ro thỏa mãn nhu cầu của ai?

Việc quản lý rủi ro thường dành cho những người không phải là kĩ sư mà chỉ hỗ trợ hoặc sử dụng quy trình quản lý rủi ro cho hệ thống thông tin của họ. Những người đó bao gồm:

- Quản lý cấp cao, những người có nhiệm vụ sở hữu, những người đưa ra quyết định về bảo mật ngân sách CNTT.
- Giám đốc phụ trách kĩ thuật, người mà đảm bảo thực thi quản lý rủi ro cho hệ thống an toàn thông tin và cung cấp bảo mật cho hệ thống thông tin.
- Các DAA người mà có trách nhiệm cho những quyết định cuối cùng cho phép hệ thống an toàn thông tin hoạt động.
- Người quản lý các chương trình bảo mật thông tin, những người thực hiện chương trình bảo mật.
- Văn phòng bảo mật hệ thống thông tin là những người mà chịu trách nhiệm về bảo mật.
- Chủ hệ thống thông tin của các phần mềm hệ thống và/hoặc phần cứng sử dụng để hỗ trợ các chức năng thông tin.
- Người chủ sỡ hữu thông tin của dữ liệu được lưu trữ, xử lý và truyền qua các hệ thống thông tin.
- Các kĩ sư hỗ trợ (ví dụ: mạng, hệ thống, ứng dụng và quản trị cơ sở dữ liệu, các chuyên gia máy tính, các nhà phân tích bảo mật) người mà quản lý và quản trị bảo mật cho hệ thống thông tin.
- Hệ thống CNTT và lập trình viên ứng dụng người mà phát triển và duy trì code có gây ảnh hưởng tới hệ thống và toàn vẹn dữ liệu.
- Người chịu trách nhiệm đảm bảo chất lượng nhân sự, người mà kiểm tra, đảm bảo tính toàn vẹn của hệ thống thông tin và các dữ liệu.
- Kiểm toán viên hệ thống thông tin, người mà kiểm toán hệ thống thông tin.
- Chuyên gia tư vấn an toàn thông tin, những người hỗ trợ khách hàng trong việc quản lý rủi ro

3.3.2 Tầm quan trọng của quản lý rủi ro

Quản lý rủi ro bao gồm 3 quá trình: đánh giá rủi ro, giảm thiểu rủi ro, ước lượng và định giá rủi ro. Đánh giá rủi ro bao gồm việc xác định, ước lượng các rủi

ro và tác động của các rủi ro đó, khuyến cáo các biện pháp giảm thiểu nguy cơ rủi ro. Giảm thiểu rủi ro trong đó đề cập đến việc ưu tiên , thực thi và duy trì các biện pháp được khuyến cáo từ quá trình đánh giá rủi ro nhằm giảm thiểu rủi ro. DAA hoặc hệ thống ủy quyền chính thức có trách nhiệm cho việc xác định những rủi ro còn lại ở một mức độ chấp nhận được hoặc các kiểm soát bảo mật bổ sung được thực hiện nhằm giảm thiểu hoặc loại bỏ các rủi ro đó trước khi ủy quyền hoặc (chấp nhận) cho việc hoạt động của hệ thống quản lý an toàn thông tin.

Quản lý rủi ro là quá trình cho phép người quản trị công nghệ thông tin cân bằng các chi phí hoạt động để bảo vệ hệ thống an toàn thông tin và dữ liệu. Quá trình này không phải là duy nhất cho môi trường trong hệ thống an toàn thông tin, thực sự nó bao trùm tất cả các quyết định trong mọi lĩnh vực của cuộc sống hàng ngày. Lấy trường hợp của bảo mật gia đình. Có rất nhiều người quyết định cài đặt một hệ thống bảo mật gia đình và trả một khoản phí hàng tháng cho một nhà cung cấp dịch vụ để có hệ thống giám sát tốt hơn để bảo vệ tài sản của họ. Có lẽ các chủ nhà đã cân đo chi phí của hệ thống cài đặt, giá trị tài sản và sự an toàn của gia đình họ. Đây là một nhiệm vụ cơ bản cần phải hoàn thành. Những người đứng đầu một đơn vị phải đảm bảo rằng tổ chức đó có các khả năng cần thiết để hoàn thành nhiệm vụ của mình. Những nhiệm vụ mà chủ sở hữu phải xác định khả năng bảo mật mà hệ thống an toàn thông tin của họ phải cung cấp đến một mức mong muốn cho nhiệm vụ hỗ trợ khi đối mặt với các mối đe dọa trên thực tế. Hầu hết các tổ chức có ngân sách rất eo hẹp cho CNTT do vậy chi tiêu dành cho bảo mật cần phải được xem xét ở mức độ quản lý. Một cấu trúc tốt của phương pháp quản lý rủi ro sử dụng có hiệu quả sẽ giúp quản lý xác định các kiểm soát phù hợp cho việc cung cấp các khả năng bảo mật cho các nhiệm vụ cần thiết.

3.3.3 Chức năng chính của người quản lý rủi ro.

Quản lý rủi ro là quản lý tính chịu trách nhiệm. Lựa chọn này miêu tả các chức năng chính của người sẽ hỗ trợ và thực thi quá trình quản lý rủi ro.

- Senior Management: Senior management, dựa trên các chuẩn và sau cùng là tính chịu trách nhiệm việc hoàn thành nhiệm vụ, phải đảm bảo rằng các tài nguyên cần thiết đều được áp dụng hiệu quả để phát triển các năng lực nhằm

hoàn thành các nhiệm vụ đó. Họ cũng phải đánh giá và kết hợp với các kết quả của việc đánh giá rủi ro trong quá trình đưa ra các quyết định. Một chương trình đánh giá rủi ro có hiệu quả đó là phải đánh giá và giảm thiểu được các rủi ro đòi hỏi phải hỗ trợ và có sự tham gia của senior management.

- Chief Information Officer (CIO): CIO có trách nhiệm trong việc lập kế hoạch, ngân sách cho các bộ phận của bảo mật thông tin và thực hiện tất cả các thành phần bảo mật thông tin bao gồm trong đó. Các quyết định được thực hiện trong những khu vực này phải dựa trên các chương trình quản lý rủi ro có hiệu quả.
- Hệ thống và chủ sỡ hữu thông tin: Hệ thống và chủ sở hữu thông tin phải có trách nhiệm đảm bảo rằng các kiểm soát thích hợp được đặt ra để giải quyết tính toàn vẹn, bí mật và sẵn sàng cho hệ thống an toàn thông tin và dữ liệu của chúng. Các kiểu hệ thống và các chủ sỡ hữu thông tin phải có trách nhiệm thay đổi hệ thống an toàn thông tin của họ. Vì vậy họ thường phải phê duyệt và ký tắt cho những thay đổi hệ thống an toàn thông tin đó (ví dụ việc tăng cường hệ thống, thay đổi các phần mềm và phần cứng). Các hệ thống và chủ sỡ hữu thông tin phải hiểu được vai trò của quy trình quản lý rủi ro.
- Kinh doanh và các chức năng quản lý: Người quản lý có trách nhiệm điều hành kinh doanh và quá trình mua bán phải có một vai trò tích cực trong quá trình quản lý rủi ro. Những nhà quản lý là các cá nhân có thẩm quyền và có trách nhiệm cho việc thực hiện các quyết định thương mại cần thiết để hoàn thành nhiệm vụ. Sự tham gia của họ trong quá trình quản lý an toàn thông tin cho phép họ thu được một hệ thống bảo mật phù hợp và nếu được quản lý đúng cách nó sẽ đảm bảo nhiệm vụ một cách có hiệu quả chỉ với các chi phí tối thiểu về mặt tài nguyên.
- ISSO: Quản lý chương trình bảo mật thông tin và cán bộ quản lý bảo mật máy tính phải có trách nhiệm cho chương trình bảo mật của tổ chức, bao gồm việc quản lý rủi ro. Do đó họ đóng vai trò hàng đầu trong việc giới thiệu sự thích hợp, các cấu trúc phương pháp để xác định sự giúp đỡ, tính

toán và thu nhỏ rủi ro tới hệ thống CNTT nhằm hỗ trợ các nhiệm vụ của tổ chức họ. ISSO cũng hoạt động như nhà tư vấn chính trong sự hỗ trợ của các quản lý cấp cao để đảm bảo rằng hành động này diễn ra liên tục.

- IT Security Practitioners: Các thành phần bảo mật CNTT (ví dụ: mạng, hệ thống, ứng dụng và các quản trị cơ sở dữ liệu, các chuyên gia máy tính, các nhà phân tích bảo mật, các chuyên gia tư vấn bảo mật) phải có trách nhiệm thực hiện đúng về các yêu cầu an ninh cho hệ thống CNTT. Khi thay đổi xảy ra trong môi trường hệ thống CNTT đã tồn tại (ví dụ: mở rộng kết nối mạng, thay đổi các cơ sở hạ tầng đang tồn tại và chính sách của tổ chức, giới thiệu các công nghệ mới) các thành phần bảo mật CNTT phải hỗ trợ hoặc sử dụng quá trình quản lý rủi ro để xác định và đánh giá các rủi ro tiềm năng, thực thi kiểm soát bảo mật mới là cần thiết để bảo vệ hệ thống CNTT của họ.
- Đào tạo nâng cao nhận thức bảo mật (bảo mật/chuyên gia vấn đề bảo mật): Cá nhân của tổ chức là những người sử dụng hệ thống an toàn thông tin. Hành vi sử dụng các hệ thống an toàn thông tin và dữ liệu theo các chính sách, hướng dẫn, quy tắc của tổ chức nhằm giảm thiểu các yếu tố rủi ro và bảo vệ các tài nguyên của tổ chức. Để giảm thiểu rủi ro của hệ thống CNTT, điều quan trọng là người sử dụng hệ thống và ứng dụng phải được cung cấp các chương trình nâng cao nhận thức bảo mật. Vì vậy tất cả các giảng viên bảo mật hoặc chuyên gia vấn đề bảo mật phải hiểu các quá trình quản lý rủi ro để họ có thể xây dựng tài liệu đào tạo phù hợp và kết hợp với việc đánh giá rủi ro trong chương trình đào tạo cho người sử dụng đầu cuối.

3.3.4 Đánh giá rủi ro (Risk Assestment)

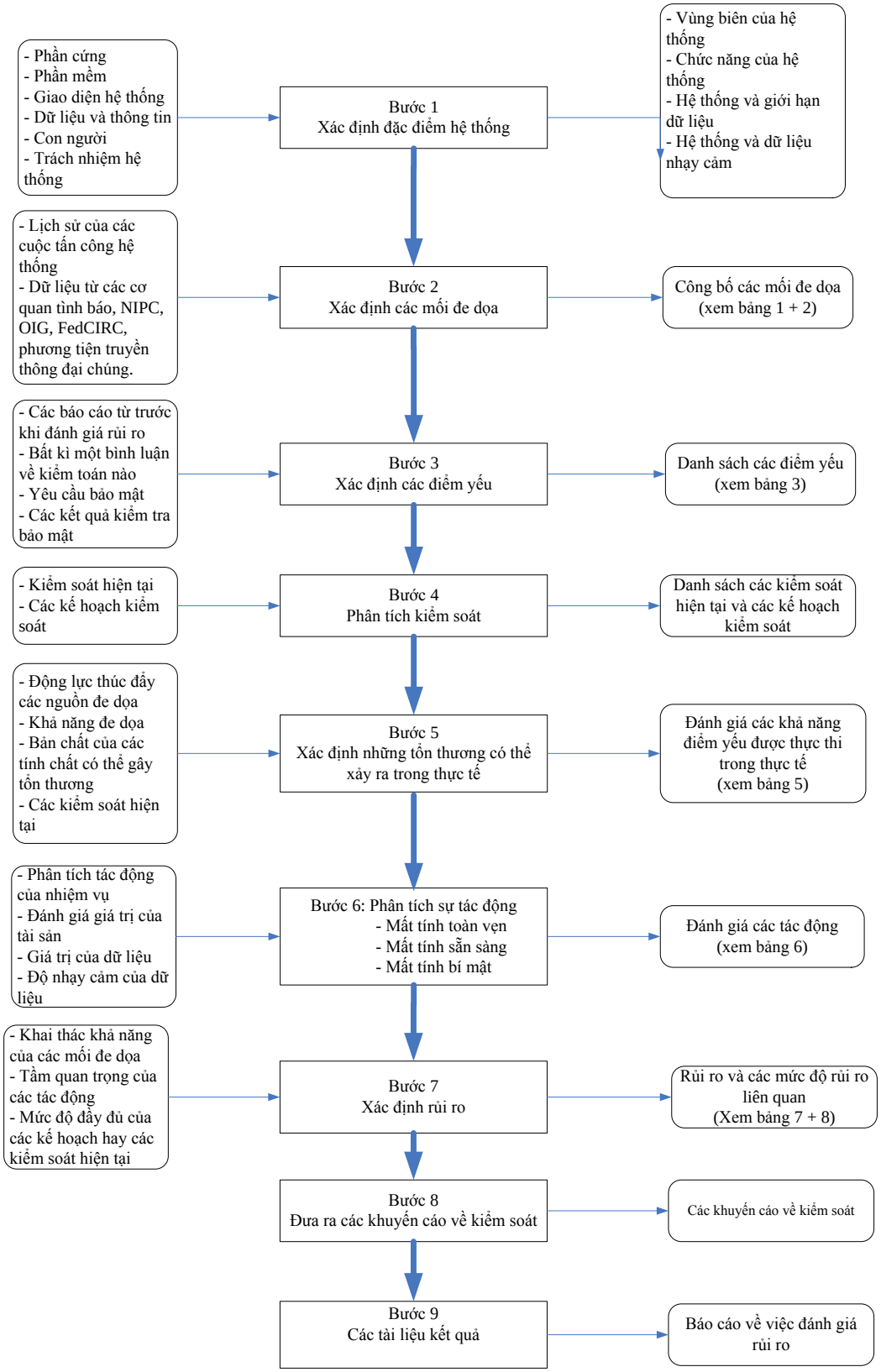
Đánh giá rủi ro là quá trình đầu tiên trong phương pháp quản lý rủi ro. Các tổ chức sử dụng đánh giá rủi ro để xác định mức độ của các mối đe dọa tiềm năng và rủi ro kết hợp với một hệ thống CNTT. Kết quả của quá trình này giúp để xác định các kiểm soát thích hợp cho việc giảm thiểu hoặc loại bỏ rủi ro trong suốt quá trình giảm thiểu rủi ro. Rủi ro là nguồn cung cấp các mối đe dọa gây ra các điểm yếu và là kết quả tác động của những sự kiện gây hại cho tổ chức. Để xác định những sự kiện có thể gây hại, các mối đe dọa tới một hệ thống an toàn thông tin thì

các mối đe dọa, các sự kiện đó phải được phân tích kết hợp với các mối đe dọa và các kiểm soát ngay tại chỗ của hệ thống an toàn thông tin. Các tác động đề cập đến tầm quan trọng của sự thiệt hại có thể được gây ra bởi một mối đe dọa của điểm yếu. Mức độ tác động được quy định bởi khả năng thực thi các tác động đó và lần lượt tạo ra các giá trị tin tưởng cho tài sản thông tin và các tài nguyên bị ảnh hưởng (ví dụ: Các yếu tốc, độ nhạy cảm của thành phần hệ thống thông tin và dữ liệu). Đánh giá rủi ro bao gồm chín bước chính dưới đây:

- Bước 1: Mô tả đặc điểm của hệ thống
- Bước 2: Xác định các mối đe dọa
- Bước 3: Xác định các điểm yếu
- Bước 4: Phân tích các kiểm soát
- Bước 5: Xác định khả năng thực thi của điểm yếu
- Bước 6: Phân tích các tác động
- Bước 7: Xác định rủi ro
- Bước 8: Các kiểm soát được khuyến cáo.
- Bước 9: Tài liệu các kết quả

Bước 2,3,4 và 6 có thể được tiến hành song song sau khi bước 1 đã được hoàn thành. Hình dưới sẽ mô tả các bước này và các đầu vào, đầu ra từ mỗi bước.

Input	Risk Assessment Activities	Output


- Phần cứng
- Phần mềm
- Giao diện hệ thống
- Dữ liệu và thông tin
- Con người
- Trách nhiệm hệ thống
Bước 1
Xác định đặc điểm hệ thống
- Vùng biên của hệ thống
- Chức năng của hệ thống
- Hệ thống và giới hạn dữ liệu
- Hệ thống và dữ liệu nhạy cảm
- Lịch sử của các cuộc tấn công hệ thống
- Dữ liệu từ các cơ quan tình báo, NIPC, OIG, FedCIRC, phương tiện truyền thông đại chúng.
Bước 2
Xác định các mối đe dọa
Công bố các mối đe dọa (xem bảng 1 + 2)
- Các báo cáo từ trước khi đánh giá rủi ro
- Bất kì một bình luận về kiểm toán nào
- Yêu cầu bảo mật
- Các kết quả kiểm tra bảo mật
Bước 3
Xác định các điểm yếu
Danh sách các điểm yếu (xem bảng 3)
- Kiểm soát hiện tại
- Các kế hoạch kiểm soát
Bước 4
Phân tích kiểm soát
Danh sách các kiểm soát hiện tại và các kế hoạch kiểm soát
- Động lực thúc đẩy các nguồn đe dọa
- Khả năng đe dọa
- Bản chất của các tính chất có thể gây tổn thương
- Các kiểm soát hiện tại
Bước 5
Xác định những tổn thương có thể xảy ra trong thực tế
Đánh giá các khả năng điểm yếu được thực thi trong thực tế (xem bảng 5)
- Phân tích tác động của nhiệm vụ
- Đánh giá giá trị của tài sản
- Giá trị của dữ liệu
- Độ nhạy cảm của dữ liệu
Bước 6: Phân tích sự tác động
- Mất tính toàn vẹn
- Mất tính sẵn sàng
- Mất tính bí mật
Đánh giá các tác động (xem bảng 6)
- Khai thác khả năng của các mối đe dọa
- Tầm quan trọng của các tác động
- Mức độ đầy đủ của các kế hoạch hay các kiểm soát hiện tại
Bước 7
Xác định rủi ro
Rủi ro và các mức độ rủi ro liên quan (Xem bảng 7 + 8)
Bước 8
Đưa ra các khuyến cáo về kiểm soát
Các khuyến cáo về kiểm soát
Bước 9
Các tài liệu kết quả
Báo cáo về việc đánh giá rủi ro

Hình 5: Biểu đồ phương pháp đánh giá rủi ro

3.3.4.1 Bước 1: Đặc điểm hệ thống

Khi đánh giá rủi ro cho hệ thống an toàn thông tin, bước đầu tiên là phải xác định phạm vi để đánh giá rủi ro. Trong bước này, đường biên của hệ thống an toàn thông tin phải được xác định cùng với các tài nguyên, thông tin xác lập lên hệ thống. Đặc điểm của một hệ thống an toàn thông tin là phải thiết lập phạm vi của việc nỗ lực đánh giá rủi ro, mô tả ranh giới của việc ủy quyền hoạt động (hoặc ủy nhiệm), và cung cấp thông tin (ví dụ: phần cứng, phần mềm, kết nối hệ thống và phân chia trách nhiệm hay người hỗ trợ) cần thiết để xác định rủi ro.

a. Thông tin liên quan đến hệ thống

Xác định rủi ro cho một hệ thống an toàn thông tin yêu cầu một sự hiểu biết thật rõ ràng về môi trường xử lý của hệ thống. Người hoặc những người thực hiện việc đánh giá rủi ro trước hết phải thu thập các thông tin liên quan đến hệ thống, những thông tin mà thường được phân loại như sau:

- Phần cứng
- Phần mềm
- Giao diện hệ thống (ví dụ: Kết nối Internal và External)
- Dữ liệu và thông tin
- Những người hỗ trợ và sử dụng hệ thống an toàn thông tin
- Nhiệm vụ của hệ thống (ví dụ: Quá trình thực hiện bởi hệ thống an toàn thông tin)
- Giá trị của hệ thống và dữ liệu (ví dụ: giá trị hoặc tầm quan trọng với tổ chức)
- Tính nhạy cảm của hệ thống và dữ liệu

Các thông tin liên quan được thêm vào với môi trường hoạt động của hệ thống an toàn thông tin, bao gồm cả dữ liệu của nó nhưng không được hạn chế những điều dưới đây:

- Các yêu cầu chức năng của hệ thống an toàn thông tin.
- Người sử dụng hệ thống (ví dụ: người sử dụng hệ thống, là người mà cung cấp hỗ trợ kỹ thuật tới hệ thống an toàn thông tin, người sử dụng ứng dụng, là người mà sử dụng hệ thống CNTT để tiến hành các chức năng kinh doanh)
- Các chính sách bảo mật của hệ thống quản lý hệ thống an toàn thông tin (chính sách của tổ chức, quy phạm pháp luật, ngành công nghiệp)
- Cấu trúc hệ thống bảo mật.
- Mô hình mạng hiện tại (ví dụ: Biểu đồ mạng)
- Bảo vệ thông tin lưu trữ đó là bảo vệ hệ thống và tính sẵn sàng, tính toàn vẹn và tính bí mật của dữ liệu.
- Luồng thông tin liên quan đến hệ thống thông tin (ví dụ: Giao diện hệ thống, hệ thống đầu vào và sơ đồ đầu ra)
- Kỹ thuật kiểm soát sử dụng cho hệ thống thông tin (ví dụ: Xây dựng hoặc các tiện ích từ các sản phẩm bảo mật cái mà hỗ trợ việc nhận dạng và xác thực, kiểm soát truy cập bắt buộc hoặc truy cập tùy ý, kiểm toán, bảo vệ thông tin còn sót lại, các phương pháp mã hóa).
- Quản lý kiểm soát sử dụng cho hệ thống thông tin (ví dụ: các quy tắc hành động, các kế hoạch bảo mật)
- Kiểm soát hoạt động sử dụng cho hệ thống thông tin (ví dụ: an ninh nhân sự, sao lưu, dự phòng, khôi phục hệ thống, lưu trữ off-site, thiết lập tài khoản người sử dụng và xóa bỏ các thủ tục, các kiểm soát phân chia chức năng người sử dụng, ví dụ như quyền người sử dụng truy cập so với các tiêu chuẩn truy cập người sử dụng.
- Môi trường bảo mật vật lý của hệ thống thông tin (ví dụ: xử lý bảo mật, chính sách dữ liệu trung tâm).
- Môi trường thực thi bảo mật cho môi trường xử lý hệ thống thông tin (ví dụ: các kiểm soát cho độ ẩm, nước, nguồn, nhiệt độ, hóa chất, ô nhiễm).

Đối với một hệ thống trong pha khởi tạo hoặc thiết kế, hệ thống thông tin có thể được bắt nguồn từ việc thiết kế hoặc các yêu cầu văn bản. Đối với một hệ thống thông tin điều này là cần thiết để xác định chìa khóa quy tắc bảo mật thông tin và các kế hoạch cho hệ thống thông tin trong tương lai. Tài liệu thiết kế hệ thống và kế hoạch bảo mật hệ thống có thể cung cấp những thông tin hữu ích về bảo mật hệ thống thông tin đang trong sự phát triển.

Đối với một hệ thống thông tin, dữ liệu được thu thập về hệ thống thông tin trong môi trường xử lý của nó, bao gồm các dữ liệu cài đặt hệ thống, các kết nối, các văn bản hoặc các thủ tục phi văn bản. Do đó, mô tả hệ thống có thể dựa trên việc cung cấp bảo mật bởi cơ sở hạ tầng hoặc các kế hoạch bảo mật trong tương lai cho hệ thống thông tin.

b. Kỹ thuật thu thập thông tin

Bất kỳ hoặc một sự kết hợp trong những kỹ thuật sau đây có thể được sử dụng trong việc thu thập thông tin liên quan tới hệ thống thông tin trong vùng biên hoạt động của nó.

- Bảng câu hỏi: Để thu thập thông tin liên quan, người đánh giá rủi ro có thể phá triển một bảng câu hỏi có liên quan đến việc quản lý và kế hoạch hoạt động kiểm soát được sử dụng cho hệ thống thông tin. Bảng câu hỏi này nên được phân phối bởi các nhân viên kĩ thuật và người quản lý không thuộc lĩnh vực kĩ thuật, là những người mà thiết kế hoặc hỗ trợ hệ thống thông tin. Bảng câu hỏi có thể được sử dụng trong quá trình on-site và trong các cuộc phỏng vấn.
- On-site Interview: Với sự hỗ trợ của quản lý nhân sự, điều này có thể cho phép nhân viên đánh giá rủi ro thu thập thông tin về hệ thống thông tin(ví dụ: làm thế nào để hệ thống được vận hành và quản lý). Ghé thăm trên site cũng cho phép người đánh giá rủi ro quan sát và thu thập thông tin về vật lý, môi trường và các hoạt động bảo mật của hệ thống thông tin. Đối với hệ thống vẫn còn trong giai đoạn thiết kế, ghé thăm trên site sẽ trực tiếp thu

được dữ liệu và có thể cung cấp các cơ hội để đánh giá môi trường vật lý mà hệ thống CNTT sẽ hoạt động.

- Document Review: Các chính sách tài liệu (ví dụ: tài liệu lập pháp, các chỉ thị), hệ thống tài liệu (ví dụ: hệ thống hướng dẫn người sử dụng, hệ thống quản trị bằng tay, hệ thống thiết kế, các yêu cầu tài liệu, mua lại tài liệu) và các tài liệu liên quan tới bảo mật (ví dụ: các báo cáo kiểm toán trước đây, báo cáo đánh giá rủi ro, kết quả kiểm tra hệ thống, kế hoạch bảo mật hệ thống, chính sách bảo mật) có thể cung cấp nhiều thông tin quý giá về kiểm soát bảo mật được sử dụng cho việc quy hoạch hệ thống thông tin. Trách nhiệm của tổ chức là tác động vào việc phân tích hoặc đánh giá giá trị của tài sản cung cấp thông tin về hệ thống, giá trị cũng như độ nhạy cảm của dữ liệu.
- Sử dụng các công cụ quét tự động: Phương pháp kĩ thuật đầu tiên có thể được sử dụng để thu thập hệ thống thông tin có hiệu quả. Ví dụ: sơ đồ mạng có thể xác định các dịch vụ chạy trên một nhóm host lớn và cung cấp một cách nhanh nhất để xây dựng một profile riêng cho mỗi hệ thống đích.

Thu thập thông tin có thể tiến hành thông qua quá trình quản lý rủi ro từ bước 1 (xác định đặc điểm hệ thống) tới bước 9 (các tài liệu kết quả). Đầu ra từ bước 1 - Đặc điểm của việc đánh giá hệ thống thông tin, một bức tranh đẹp về môi trường hệ thống thông tin và xác định ranh giới hệ thống.

3.3.4.2 Bước 2: Xác định mối đe dọa

Một mối đe dọa tiềm năng của một nguồn đe dọa để thực hiện thành công một điểm yếu cụ thể. Một điểm yếu có thể là do vô tình gây ra hoặc bị khai thác một cách cố ý. Một nguồn đe dọa không phải là một rủi ro khi không có tổn thương nào được thực hiện. Khi xác định khả năng của một mối đe dọa phải xem xét được nguồn của mối đe dọa đó và các tiềm năng gây ra sự thương tổn và các kiểm soát hiện tại.

Threat: Tiềm năng để nguồn đe dọa để thực hiện (Vô tình thực thi hoặc khai thác một cách cố ý) một điểm yếu cụ thể.

a. Xác định nguồn đe dọa

Mục tiêu của bước này là xác định tiềm năng của các nguồn đe dọa và đưa một danh sách các nguồn đe dọa tiềm năng đó là cái được áp dụng cho việc đánh giá hệ thống thông tin.

Nguồn đe dọa:

1) Ý định và mục đích của phương pháp là nhắm tới việc cố ý khai thác điểm yếu hoặc

2) Điểm nút của phương pháp này có thể thực thi một cách cố ý các điểm yếu.

Một nguồn đe dọa được xác định cũng có thể là một sự kiện bất kì nào có khả năng gây hại cho một hệ thống thông tin. Các nguồn đe dọa phổ biến có thể là tự nhiên, là con người hay là môi trường.

Khi đánh giá một nguồn đe dọa điều quan trọng nhất là phải xem tất cả các tiềm năng mà các nguồn đó có thể gây hại tới cho hệ thống thông tin và môi trường thực hiện chúng. Ví dụ: Mặc dù tuyên cáo đe dọa cho hệ thống thông tin ở miền sa mạc không thể bao gồm cả lũ lụt bởi vì khả năng xảy ra của mối đe dọa này là rất thấp, các đe dọa môi trường như một ngòi nổ có thể làm ngập các phòng máy tính và gây hại tới các tài sản của tổ chức và các nguồn tài nguyên. Con người cũng có thể là một mối hiểm họa thông qua những hành động cố ý chẳng hạn như các cuộc tấn công có mục đích bởi những người gây hại hoặc của những nhân viên bất mãn hay là các hành vi vô ý ví dụ như sự sơ xuất hay sai sót của nhân viên trong công ty. Một cuộc tấn công có chủ đích có thể được ví dụ như sau: Một mã độc hại cố gắng truy cập trái phép vào một hệ thống CNTT (ví dụ: thông qua việc đoán mật khẩu) nhằm thỏa hiệp với hệ thống và tính toàn vẹn dữ liệu, tính sẵn sàng hay tính bí mật nhưng dù sao cũng là mục đích phá vỡ hệ thống bảo mật. Một trong những ví dụ về loại tấn công có chủ ý là một người lập trình viên viết ra một chương trình Trojan horse để vượt qua hệ thống bảo mật nhằm thực hiện những công việc mà họ muốn. Bảng 1 đưa ra các ví dụ về các nguồn đe dọa. Các mối đe dọa có thể là cố ý, vô tình hay từ môi trường tự nhiên.

Danh sách dưới đây đã xếp các loại đe dọa vào 3 loại sau:

D(cố ý),

A(vô ý),

E(do môi trường).

D được sử dụng cho tất cả các hành động có chủ ý nhằm vào tài sản thông tin, A được sử dụng cho tất cả các hành động vô ý của con người có thể làm thiệt hại tới tàn sản thông tin và E được sử dụng cho tất cả các sự cố xảy ra mà không phải do con người.

Kiểu	Các mối đe dọa	Nguyên nhân
Các mối đe dọa về mặt vật lý	Lửa	A, D, E
	Nước	A, D, E
	Ô nhiễm môi trường	A, D, E
	Bụi, ăn mòn hóa chất, nhiệt độ…	A, D, E
Các hiện tượng tự nhiên	Khí hậu	E
	Động đất	E
	Núi lửa	E
	Lũ lụt	E
Các mối đe dọa về mặt dịch vụ	Điều hòa bị ngắt	A, D
	Nguồn điện bị mất	A, D, E
	Các thiết bị truyền bị lỗi	A, D
	Gián điệp	D
	Nghe trộm	D

Làm tổn thương thông tin.	Các hành vi trộm cắp văn bản hoặc phi văn bản	D
	Trộm cắp thiết bị	D
	Thu hồi, tái chế, hay phá hủy các thiết bị	D
	Sử dụng dữ liệu từ các nguồn không đáng tin cậy	A, D
	Can thiệp vào phần cứng	A, D
	Can thiệp vào phần mềm	A, D
Lỗi về mặt kỹ thuật	Thiết bị lỗi	A
	Hệ thống thông tin bị tấn công một cách dồn dập	A, D
	Phần mềm bị lỗi	A
	Các vi phạm làm hệ thống thông tin ngừng hoạt động	A, D
Các hành động trái phép	Sử dụng thiết bị một cách trái phép	D
	Sao chép phần mềm một cách trái phép	D
	Sử dụng những phần mềm không có bản quyền	A, D
	Ăn cắp dữ liệu	D
	Xử lý dữ liệu một cách bất hợp pháp	D
Gây ảnh hưởng tới hoạt động kinh doanh của tổ chức	Lỗi trong khi sử dụng	A
	Lạm dụng quyền hạn	A, D
	Giả mạo quyền hạn	D
	Các vi phạm của nhân viên	A, D, E

Bảng 1: Danh sách các nguồn đe dọa

b. Các động lực và các hành động đe dọa

Động lực và các nguồn lực để thực hiện một cuộc tấn công được thực hiện bởi các mối đe dọa từ con người. Bảng dưới hiển thị một cái nhìn tổng quan các mối đe dọa phổ biến từ con người, các động lực có thể và các phương pháp hay các hành động đe dọa mà họ có thể thực hiện từ các cuộc tấn công. Thông tin này sẽ rất hữu ích cho tổ chức nghiên cứu và tùy biến các tuyên cáo về mối đe dọa đó. Thêm vào đó việc xem xét lịch sử tấn công của hệ thống, báo cáo các vi phạm an ninh, báo cáo các sự cố và cuộc phỏng vấn người quản trị mạng, sự giúp đỡ người dùng và cộng đồng người sử dụng trong quá trình thu thập thông tin sẽ giúp việc xác định dễ dàng hơn các mối đe dọa, những người có khả năng gây hại cho hệ thống thông tin và nơi mà điểm yếu đang tồn tại.

Nguồn đe dọa	Động lực	Hành động đe dọa
Hacker, cracker	- Thách thức - Cái tôi - Là các cuộc nổi loạn	- Hacking - Social enigneering - Thăm dò và bẻ gãy hệ thống - Truy cập vào hệ thống một cách trái phép
Tội phạm máy tính	- Tiêu hủy thông tin - Công bố thông tin bất hợp pháp - Lợi ích về tiền bạc - Tự ý thay đổi dữ liệu	- Tội phạm máy tính (ví dụ: cyber stalking) - Các hành vi gian lận (ví dụ: Tấn công phát lại, mạo danh…) - Mua chuộc thông tin - Spoofing - Xâm nhập hệ thống
Kẻ khủng bố	- Blackmail	- Bom/Khủng bố

	- Phá hủy - Khai thác - Trả thù	- Thông tin chiến tranh - Tấn công hệ thống - Thâm nhập hệ thống - Giả mạo hệ thống
Gián điệp công nghiệp (các công ty, Chính phủ quốc tế, các chính phủ quan tâm khác)	- Cạnh tranh - Gián điệp kinh tế	- Khai thác kinh tế - Trộm cắp thông tin - Xâm phạm quyền riêng tư cá nhân - Social engineering - Xâm nhập và hệ thống - Truy cập vào hệ thống một cách trái phép (truy cập đến các vùng được phân loại, hoặc tài sản có chủ sở hữu, và/hoặc liên quan tới công nghệ liên quan tới thông tin)
Trong nội bộ (được đào tạo kém, do bất bình, do sự cẩu thả, do các mã độc hại, không trung thực hoặc chấm dứt hợp đồng lao động)	- Tò mò - Vì cái tôi của mình - Là gián điệp - Lợi ích về tiền bạc - Trả thù - Gây lỗi một cách vô ý (ví dụ: nhập dữ liệu bị lỗi, lập trình bị lỗi)	- Tấn công vào nhân viên - Tống tiền - Đưa ra các thông tin có chủ sở hữu - Lợi dụng máy tính - Gian lận và trộm cắp - Mua chuộc thông tin

		- Giả mạo đầu vào và làm hỏng dữ liệu - Bị chặn - Mã độc hại (ví dụ: virus, bom logic, trojan horse) - Bán thông tin cá nhân - Lỗi hệ thống - Xâm nhập hệ thống - Phá hoại hệ thống - Truy cập trái phép vào hệ thống.

Bảng 2: Nguồn, động lực và các hành động đe dọa

3.3.4.3 Bước 3: Xác định điểm yếu

Phân tích những đe dọa đến một hệ thống thông tin phải bao gồm việc phân tích những điểm yếu kết hợp với môi trường của hệ thống. Mục tiêu của bước này là phát triển danh sách điểm yếu có thể được khai thác bởi những nguồn đe dọa có tiềm năng

- Những nơi dễ bị tấn công: Một thiếu sót hoặc điểm yếu trong thủ tục bảo mật của hệ thống, thiết kế, thực thi hoặc kiểm soát bên trong có thể được thực hiện (vô tình gây ra hoặc cố ý khai thác) và kết quả của sự vi phạm bảo mật, vi phạm một trong những chính sách bảo mật của hệ thống.

Kiểu	Điểm yếu	Mối đe dọa
	Lỗi trong việc cài đặt thiết bị ngoại vi	Các vi phạm của nhân viên
	Không có kế hoạch thay thế thiết	Thu hồi, tái chế hoặc

Phần cứng	bị định kỳ	tiêu hủy các thiết bị
	Nhạy cảm với bụi, độ ẩm.	Bụi, ăn mòn hóa chất, nhiệt độ…
	Không có cấu hình một cách hiệu quả	Lỗi khi sử dụng
	Không có nguồn điện dự trữ	Nguồn điện bị ngắt
	Không bảo vệ các thiết bị lưu trữ thông tin	Các hành vi trộm cắp văn bản hoặc phi văn bản
	Không cẩn thận khi tiêu hủy văn bản.	Các hành vi trộm cắp văn bản hoặc phi văn bản
	Không kiểm soát khi sao chép văn bản.	Các hành vi trộm cắp văn bản hoặc phi văn bản
Phần mềm	Không có quy trình kiểm thử phần mềm hay kiểm thử phần mềm không đầy đủ.	Lạm dụng quyền hạn
	Các điểm yếu đã được biết đến trong các phần mềm	Lạm dụng quyền hạn
	Không Logout khi rời khỏi máy tính	Lạm dụng quyền hạn
	Phân bố phần mềm một cách rộng rãi	Ăn cắp dữ liệu
	Giao diện người dùng phức tạp	Lỗi trong khi sử dụng
	Không có tài liệu hướng dẫn sử dụng	Lỗi trong khi sử dụng

	Phần mềm mới	Sự cố về phần mềm
	Không có bản sao lưu dự phòng	Can thiệp vào phần mềm
Mạng	Không bảo vệ đường truyền	Nghe trộm
	Lỗi tại một điểm truyền	Lỗi của thiết bị truyền
	Truyền các mật khẩu không mã hóa	Gián điệp
	Không có nhân viên quản trị mạng	Tấn công mạng một cách dồn dập
	Không bảo vệ các mạng kết nối	Sử dụng thiết bị một cách trái phép
Con người	Thiếu nhân lực	Các vi phạm của nhân viên
	Không có sự đào tạo về lĩnh vực bảo mật	Lỗi trong khi sử dụng
	Sử dụng phần mềm hay phần cứng bị sai	Lỗi trong khi sử dụng
	Không có cơ chế giám sát	Xử lý dữ liệu một cách trái phép
	Không có cơ chế giám sát ID của nhân viên thôi việc	Các hành vi trộm cắp văn bản hoặc phi văn bản
	Không có các chính sách về việc sử dụng đúng mục đích của thiết bị truyền thông	Sử dụng thiết bị một cách trái phép
	Quản lý bất cẩn việc ra vào tòa nhà	Thu hồi, tái chế hoặc tiêu hủy các thiết bị
	Tòa nhà nằm trong vị trí dễ bị lũ lụt	Lũ lụt

Tổ chức	Điện lưới không ổn định	Mất nguồn điện
	Không có bảo vệ cho tòa nhà	Ăn cắp thiết bị
	Không có thủ tục giám sát thông tin	Lạm dụng quyền hạn
	Không theo dõi và thay đổi các kiểm soát	Vi phạm của nhân viên
	Không có các thủ tục cho ISMS kiểm soát tài liệu	Mất dữ liệu
	Không có các thủ tục phân loại thông tin	Lỗi khi sử dụng
	Thiếu hoặc không đủ các quy định trong khi kí hợp đồng với nhân viên mới	Xử lý thông tin một cách trái phép
	Thiếu chính sách hoặc các chính sách của tổ chức không rõ ràng	Các hành vi ăn cắp văn bản hoặc phi văn bản

Bảng 3: Ví dụ về điểm yếu cùng các mối đe dọa

Các phương pháp khuyến cáo cho sự nhận biết điểm yếu trong hệ thống là sử dụng nguồn của các điểm yếu đó, thực hiện kiểm tra an ninh hệ thống và sự phát triển của danh sách các yêu cầu bảo mật. Nó nên được ghi chú lại các kiểu điểm yếu sẽ tồn tại, các phương pháp cần được xác định rõ nơi mà các điểm yếu đó xuất hiện, thông thường sẽ phụ thuộc vào bản chất của hệ thống thông tin.

- Nếu hệ thống thông tin vẫn chưa được thiết kế, việc tìm kiếm các điểm yếu nên đặt trọng tâm vào chính sách bảo mật của tổ chức, các kế hoạch thực thi bảo mật và xác định các yêu cầu hệ thống, phân tích các sản phẩm bảo mật của nhà sản xuất hoặc nhà phát triển.
- Nếu hệ thống đang được thực thi, việc xác định các điểm yếu cần phải được mở rộng nhằm bao gồm nhiều thông tin cụ thể hơn ví dụ như lên kế hoạch

các tính năng bảo mật được mô tả trong các tài liệu bảo mật và các kết quả của việc kiểm tra chứng chỉ hệ thống và đánh giá kết quả của chứng chỉ hệ thống.

- Nếu hệ thống đang hoạt động, quá trình xác định các điểm yếu nên bao gồm việc phân tích các đặc điểm hệ thống bảo mật và các kiểm soát bảo mật, công nghệ và sản phẩm bảo mật sử dụng bảo vệ hệ thống.

a. Các nguồn điểm yếu

Các điểm yếu liên quan tới kĩ thuật hoặc phi kĩ thuật kết hợp với một môi trường xử lý của hệ thống thông tin sẽ được xác định thông qua các công nghệ thu thập thông tin được miêu tả ở phần trên. Việc xem qua các nguồn công nghiệp khác (ví dụ: nhà sản xuất web đã xác định lỗi về kĩ thuật và các lỗ hổng của hệ thống) sẽ rất có ích trong việc chuẩn bị phỏng vấn và phát triển các câu hỏi một cách có hiệu quả để xác định điểm yếu ở các hệ thống thông tin cụ thể(ví dụ: phiên bản của một hệ điều hành cụ thể). Mạng Internet là một nguồn thông tin khác mà khi dựa vào đó ta có thể biết được những điểm yếu của hệ thống được đăng lên bởi các nhà sản xuất, các thợ sửa chữa và các bản vá hay các biện pháp khắc phục hậu quả có thể được áp dụng để loại bỏ hoặc giảm thiểu những điểm yếu đó. Nguồn các tài liệu về điểm yếu cần được phân tích một cách kĩ lưỡng nhưng không được hạn chế những điều dưới đây:

- Các tài liệu đánh giá rủi ro tài sản hệ thống
- Các bản báo cáo kiểm toán hệ thống, báo cáo, báo cáo sự dị thường của hệ thống, các bản báo cáo về bảo mật của hệ thống, bản báo cáo kiểm thử và đánh giá hệ thống.
- Danh sách các điểm yếu.
- Cố vấn bảo mật
- Các thông báo của nhà sản xuất.
- Các sự cố máy tính thương mại/ đội phản ứng khẩn cấp
- Cảnh báo thông tin về các điểm yếu.

- Phân tích phần mềm bảo mật hệ thống.

b. Kiểm tra hệ thống bảo mật

Các phương pháp chủ động, thực hiện việc kiểm thử hệ thống, có thể sử dụng để xác định điểm yếu cho hệ thống, độc lập các yếu tố của hệ thống thông tin và sẵn sàng các nguồn tài nguyên (ví dụ: vị trí của các kho, sẵn sàng các công nghệ, người có chuyên môn để tiến hành các thử nghiệm). Phương pháp thử bao gồm:

- Các công cụ quét điểm yếu tự động
- Kiểm tra và đánh giá bảo mật
- Kiểm tra tính thâm nhập.

Các công cụ quét lỗ hổng tự động để sử dụng để quét các nhóm máy chủ hoặc một mạng nhằm phát hiện ra những điểm yếu của các dịch vụ (ví dụ: hệ thống cho phép FPT chuyển tiếp sendmai). Tuy nhiên nó cần phải chú ý một vài điểm yếu có tiềm năng được xác định bởi các công cụ quét tự động có thể không phải là những lỗ hổng thực sự trong môi trường của hệ thống. Ví dụ: Một vài công cụ quét tự động các điểm yếu tiềm năng mà không xem xét tới môi trường và các yêu cầu của site. Một vài các điểm yếu được xác định bởi các phần mềm quét tự động có thể không phải là điểm yếu cho một site cụ thể nhưng lại được cài đặt vì môi trường của họ đòi hỏi điều đó. Vì vậy các phương pháp kiểm tra vẫn có thể xác định nhầm.

ST&E là một công nghệ khác có thể được sử dụng trong việc xác định điểm yếu của hệ thống thông tin trong suốt quá trình xác định rủi ro. Nó bao gồm việc phát triển và thực hiện các kế hoạch kiểm tra như (ví dụ: kiểm tra các script, kiểm tra các thủ tục và kiểm tra kết quả mong đợi). Mục đích của việc kiểm tra hệ thống bảo mật là để kiểm tra tính hiệu quả các kiểm soát bảo mật của hệ thống xem chúng như việc chúng được áp dụng vào trong môi trường hoạt động như thế nào. Mục tiêu là để đảm bảo rằng các kiểm soát được áp dụng đáp ứng được các đặc điểm kĩ thuật của phần mềm cũng như phần cứng và thực hiện được các chính sách bảo mật của tổ chức hoặc đáp ứng được các chuẩn công nghiệp.

Việc kiểm tra sự thâm nhập có thể được sử dụng để bổ sung cho việc xem xét các kiểm soát bảo mật và đảm bảo rằng các khía cạnh khác nhau của hệ thống thông tin phải được bảo mật. Việc kiểm tra sự thâm nhập khi làm việc trong quá trình đánh giá rủi ro, có thể được sử dụng để đánh giá khả năng chịu đựng của hệ thống thông tin khi chống lại sự cố gắng của kẻ tấn công nhằm phá hỏng hệ thống bảo mật. Mục tiêu của nó là để kiểm tra hệ thống thông tin nhìn dưới góc độ của kẻ tấn công và xác định các số phần trăm thất bại trong kế hoạch bảo vệ hệ thống thông tin. Kết quả của sự lựa chọn kiểu kiểm tra bảo mật sẽ giúp nhận biết các điểm yếu của hệ thống.

c. Phát triển các danh mục yêu cầu bảo mật.

Trong suốt quá trình này người đánh giá rủi ro phải xem xét các yêu cầu bảo mật theo các quy định của hệ thống thông tin và những thông tin thu thập về đặc điểm của hệ thống đang được đáp ứng bằng cách kiểm soát bảo mật hiện có hoặc kiểm soát bảo mật đã được lập kế hoạch. Thông thường các yêu cầu của hệ thống bảo mật có thể hiển thị trong một bảng, với mỗi yêu cầu kèm theo một lời giải thích về việc thiết kế hệ thống như thế nào hoặc thực thi hay không thực thi các yêu cầu kiểm soát an ninh ra sao?

Một danh sách yêu cầu bao gồm các tiêu chuẩn bảo mật cơ bản đó là có thể sử dụng hệ thống đánh giá và xác định những tổn thương của tài sản (ví dụ: con người, phần cứng, phần mềm, thông tin), hoặc các thủ tục không tự động, các quy trình và việc truyền thông tin kết hợp với một hệ thống thông tin trong các lĩnh vực bảo mật dưới đây:

- Quản lý
- Điều hành
- Kỹ thuật

Miền bảo mật	Yếu tố bảo mật
Quản lý bảo mật	- Phân công người chịu trách nhiệm - Hỗ trợ liên tục

	- Khả năng đáp ứng các sự cố - Xem xét các kiểm soát bảo mật định kì - Nhân viên phải thanh toán và giải phóng mặt bằng - Đánh giá rủi ro - Đào tạo về bảo mật và kĩ thuật - Phân chia nhiệm vụ - Hệ thống ủy quyền và tái ủy quyền - Hệ thống hoặc kế hoạch ứng dụng bảo mật
Hoạt động bảo mật	- Kiểm soát các chất gây ô nhiễm truyền qua không khí (khói, bụi, hóa chất) - Kiểm soát để đảm bảo chất lượng của các nguồn cung cấp năng lượng điện. - Các phương pháp truy cập dữ liệu và các phương tiện lưu trữ - Phân phối dữ liệu bên ngoài và ghi nhãn - Thiết bị bảo vệ (ví dụ: phòng máy, trung tâm dữ liệu, văn phòng) - Kiểm soát độ ẩm - Kiểm soát nhiệt độ - Máy trạm, laptop, các máy tính cá

	nhân.
Kỹ thuật bảo mật	- Các cách truyền (ví dụ: dial - in, siêu kết nối hệ thống, định tuyến routers) - Mật mã - Kiểm soát truy cập tùy ý - Xác định và xác thực - Phát hiện xâm nhập - Sử dụng lại đối tượng - Hệ thống kiểm toán

Bảng 4: Các yếu tố bảo mật được khuyến cáo sử dụng trong việc nhận biết các điểm yếu của hệ thống thông tin với mỗi miền bảo mật

Kết quả của quá trình này là danh sách các yêu cầu về bảo mật. Các mục tiêu kiểm soát được trừu tượng hóa trực tiếp từ các yêu cầu được tìm thấy trong các quy luật, các chính sách và các hướng dẫn về bảo mật hay tính riêng tư. Kết quả của danh sách kiểm tra (hoặc câu hỏi) có thể được sử dụng như là đầu vào cho việc tuân thủ hoặc không tuân thủ việc đánh giá. Quá trình này được xác định hệ thống, quy trình, các thủ tục và các điểm yếu thể hiện các lỗ hổng bảo mật tiềm năng.

3.3.4.4 Bước 4: Phân tích các kiểm soát

Mục tiêu của bước này là phân tích các kiểm soát được thực thi hoặc đã được lên kế hoạch để thực thi bởi các tổ chức nhằm giảm thiểu hoặc loại bỏ các mối đe dọa có khả năng tạo ra một điểm yếu trong hệ thống. Để đánh giá tổng thể xác suất một điểm yếu tiềm năng có thể được thực hiện trong các môi trường đe dọa có liên quan thì phải thực thi các kiểm soát hiện tại hoặc các kế hoạch kiểm soát phải được xem xét một cách kĩ lưỡng. Ví dụ: một điểm yếu không có khả năng thực hiện được hoặc khả năng tạo thành các nguồn đe dọa là thấp hay nếu có các kiểm soát bảo mật có hiệu quả thì nó có thể loại bỏ hoặc giảm thiểu mức độ của các tác hại.

a. Các phương pháp kiểm soát

Các kiểm soát bảo mật bao gồm việc sử dụng các phương pháp kỹ thuật hoặc các phương pháp phi kĩ thuật. Các kiểm soát kỹ thuật bảo vệ được tích hợp vào trong phần cứng của máy tính, phần mềm và phần sụn của máy (ví dụ: các cơ chế kiểm soát truy cập, nhận dạng và cơ chế xác thực, phương pháp mã hóa, phần mềm phát hiện xâm nhập). Các kiểm soát phi kĩ thuật được quản lý và thực thi ví dụ như: các chính sách bảo mật, các quy trình hoạt động, các cá nhân, về mặt vật lý, môi trường bảo mật.

b. Các loại kiểm soát

Các loại kiểm soát tính cả hai mặt kĩ thuật và phi kĩ thuật có thể đươc phân thành hai loại đó là ngăn chặn và dò tìm. Hai loại đó được giải thích như sau:

- Các kiểm soát ngăn chặn hạn chế việc cố gắng vi phạm các chính sách bảo mật và bao gồm các kiểm soát như việc tuân theo các kiểm soát truy cập, mã hóa và chứng thực.
- Các kiểm soát dò tìm cảnh báo các vi phạm hoặc sự cố gắng để vi phạm các chính sách an ninh và bao gồm các kiểm soát như vết kiểm toán, phương pháp phát hiện xâm nhập và checksum

Thực thi các kiểm soát như vậy trong suốt quá trình giảm thiểu rủi ro là kết quả trực tiếp của việc xác định các thiếu sót trong các kiểm soát hiện tại hoặc các kiểm soát đang lên kế hoạch ở quá trình đánh giá rủi ro (ví dụ: các kiểm soát không có tại chỗ hoặc các kiểm soát được thực hiện không đúng cách).

c. Kỹ thuật phân tích kiểm soát.

Danh sách các yêu cầu bảo mật có thể được sử dụng để xác nhận việc tuân thủ hoặc không tuân thủ các yêu cầu bảo mật. Vì vậy điều cần thiết là phải cập nhật bản danh sách thường xuyên để phản ánh những thay đổi trong môi trường kiểm soát của tổ chức (ví dụ: thay đổi các chính sách bảo mật, các phương pháp hay các yêu cầu) và đảm bảo rằng danh sách này vẫn còn có hiệu lực.

3.3.4.5 Bước 5: Xác định những điểm yếu có thể xảy ra trong thực tế.

Để đưa ra được một đánh giá tổng quát về xác xuất một điểm yếu có thể được thực thi trong môi trường đe dọa các yếu tố sau đây phải được xem xét:

- Động lực và khả năng của các nguồn đe dọa
- Bản chất của điểm yếu
- Tính hiệu quả của các kiểm soát hiện tại

Khả năng mà một điểm yếu tiềm năng có thể được thực thi bởi các nguồn đe dọa được miêu tả thành các cấp độ như sau: cao, thấp hoặc trung bình. Bảng dưới đây sẽ miêu tả 3 loại khả năng đó:

Cấp độ các khả năng xảy ra	Xác định các khả năng
Cao	Các nguồn đe dọa có nhiều động lực và có khả năng cao để thực hiện các kiểm soát nhằm ngăn chặn các điểm yếu thực thi không có hiệu quả.
Trung bình	Các nguồn đe dọa có động lực và có khả năng thực hiện nhưng các kiểm soát được đặt ra có thể thực thi thành công.
Thấp	Các nguồn đe dọa không có động lực hoặc không thể thực hiện được hoặc các kiểm soát đặt ra để ngăn chặn hoặc ít nhất là cản trở đáng kể các điểm yếu đó được thực thi.

Bảng 5: Khả năng thực thi điểm yếu

3.2.4.6 Bước 6: Phân tích các tác động

Những bước tiếp theo trong việc đo lường mức độ rủi ro để xác định các tác động bất lợi phát sinh từ việc thực thi thành công các rủi ro từ những điểm yếu. Trước khi bắt đầu phân tích các tác động điều bắt buộc là phải có những thông tin cần thiết như sau:

- Nhiệm vụ của hệ thống

- Giá trị của hệ thống hay dữ liệu (ví dụ: giá trị của hệ thống hoặc tầm quan trọng của tổ chức)
- Hệ thống nhạy cảm và dữ liệu nhạy cảm.

Thông tin này có thể bao gồm các tài liệu đang tồn tại trong tổ chức ví dụ như bản báo cáo đánh giá phân tích các tác động hoặc báo cáo giá trị của tài sản. Phân tích đánh giá tác động (còn gọi là phân tích các tác động về mặt kinh doanh ở một số tổ chức) ưu tiên các mức độ tác động liên quan tới việc làm tổn thương tới tài sản thông tin của tổ chức dựa trên việc đánh giá định tính hay định lượng giá trị và tính nhạy cảm của tài sản đó. Giá trị tài sản được đánh giá bằng độ ưu tiên và độ nhạy cảm của tài sản thông tin đó (ví dụ: phần cứng, phần mềm, hệ thống, dịch vụ và các công nghệ liên quan) điều này có thể hỗ trợ được các nhiệm vụ của tổ chức.

Nếu tài liệu này không tồn tại hoặc việc đánh giá các giá trị tài sản thông tin của tổ chức không được thực hiện thì độ nhạy cảm của hệ thống và dữ liệu có thể được xác định dựa trên mức độ bảo vệ cần thiết để duy trì tính sẵn sàng, toàn vẹn và bảo mật của hệ thống và dữ liệu. Bất cứ phương pháp nào được sử dụng để xác định độ nhạy cảm của hệ thống và dữ liệu đó như thế nào, hệ thống và chủ sở hữu thông tin phải có trách nhiệm nhất định đối với mức độ tác động tới hệ thống và thông tin của họ. Do đó trong việc phân tích các tác động, cách tiếp cận phù hợp đó là phải tìm hiểu về hệ thống và chủ sở hữu thông tin. Các tác động xấu của sự kiện bảo mật có thể được miêu tả trong các mục mất hoặc bị thiếu hoặc kết hợp cả hai, một trong ba mục tiêu của an toàn là : tính toàn vẹn, tính bí mật, tính sẵn sàng. Danh sách dưới đây cung cấp một mô tả ngắn gọn của mỗi mục tiêu bảo mật và hậu quả (hay tác động) của nó khi không được đáp ứng.

- Mất tính toàn vẹn: toàn vẹn hệ thống và dữ liệu được tham chiếu tới các yêu cầu bảo mật thông tin trước các hành động muốn sửa đổi thông tin một cách sai lệch. Tính toàn vẹn bị mất khi thông tin bị thay đổi trái phép bằng các hành động cố ý hay vô tình. Nếu sự mất mát của hệ thống hoặc tính toàn vẹn của dữ liệu không được sửa chữa mà tiếp tục sử dụng hệ thống đã bị sửa hoặc các dữ liệu bị hỏng có thể dẫn đến các kết quả không chính xác, gian lận, hoặc các quyết định sai lầm. Ngoài ra các vi phạm tính toàn vẹn có thể

là bước thành công đầu tiên của một cuộc tấn công vào tính sẵn sàng hoặc tính bảo mật của hệ thống. Đối với tất cả những lý do này mất tính toàn vẹn có thể làm giảm tính đảm bảo của hệ thống thông tin.

- Mất tính sẵn sàng: Nếu nhiệm vụ quan trọng của một hệ thống không sẵn sàng với người dùng thì nhiệm vụ của tổ chức có thể bị ảnh hưởng. Mất chức năng và hiệu suất hoạt động của hệ thống, ví dụ: về kết quả thời gian sản xuất, nó có thể cản trở hiệu suất của người dùng khi cần tới các chức năng của hệ thống trong việc hỗ trợ các nhiệm vụ của tổ chức.
- Mất tính bí mật: Tính bí mật của hệ thống và dữ liệu được xem là việc bảo vệ thông tin trước việc tiết lộ thông tin một cách trái phép. Các tác động của việc tiết lộ thông tin bí mật trái phép có thể tạo ra một chuỗi những nguy hiểm cho an ninh quốc gia. Tiết lộ một cách trái phép, bất ngờ hoặc không tự ý có thể làm mất tính bí mật, làm cho người khác xấu hổ hoặc các bằng chứng liên quan đến pháp lý chống lại tổ chức.

Một số các tác động hữu hình có thể được đo bằng cách tính toán số lượng doanh thu bị mất, các chi phí sửa chữa hệ thống, hoặc mức độ của việc cố gắng đưa ra các yêu cầu để sửa chữa các vấn đề gây ra bởi các hành động đe dọa thành công. Các tác động khác (ví dụ: mất tính bí mật, mất uy tín, thiệt hại về vấn đề tài sản của công ty) không thể được đo bằng đơn vị cụ thể nhưng nó lại có khả năng hoặc được miêu tả trong mục tác động cao, trung bình hoặc thấp

Tầm quan trọng của tác động	Định nghĩa các tác động
Cao	Thực hiện các tổn thương có thể dẫn tới sự mất nhiều chi phí hoặc các nguồn tài nguyên, nó có thể sẽ vi phạm này gây hại hoặc cản trở công việc của tổ chức, danh tiếng hoặc lãi suất hoặc có thể dẫn tới cái chết của con người hoặc gây tổn hại nghiêm trọng.
Trung bình	Thực thi các lỗ hổng này có thể dẫn tới việc mất nhiều chi phí hoặc các nguồn tài nguyên, có thể các vi phạm

	này sẽ gây hại hoặc cản trở công việc của tổ chức, gây tổn hại về mặt danh tiếng hoặc có thể dẫn tới tổn hại về mặt con người.
Thấp	Thực thi các lỗ hổng này có thể dẫn tới mất chi phí hoặc các nguồn tài nguyên hoặc ảnh hưởng tới công việc của tổ chức, về mặt danh tiếng hoặc tài sản.

Bảng 6: Xác định tầm quan trọng của các tác động

Định lượng chống lại các đánh giá định lượng

Khi tiến hành phân tích tác động cần xem xét đến những ưu điểm và khuyết điểm của việc định lượng chống lại các đánh giá định lượng. Ưu điểm chính của việc định lượng các phân tích tác động là nó ưu tiên những rủi ro, xác định các miền để cải thiện ngay lập tức trong việc giải quyết các tổn thương. Những khuyết điểm của việc đánh giá định tính là nó không cung cấp các phép đo định lượng cụ thể về độ lớn của các tác động, do đó làm việc phân tích lợi ích các chi phí của bất kì kiểm soát được khuyến cáo nào trở nên khó khăn.

Ưu điểm chính của phân tích định lượng các tác động đó là nó cung cấp một phép đo cường độ của các tác động cái mà có thể được sử dụng trong việc phân tích các phí lợi nhuận của các kiểm soát được khuyến cáo. Điểm bất lợi đó là điều này phụ thuộc vào phạm vi những dãy số được sử dụng để thể hiện các phép đo, các ý nghĩa của việc phân tích định lượng các tác động có thể không rõ ràng, đòi hỏi các kết quả cần phải được diễn giải một cách định tính. Các yếu tố thường phải được xem xét để xác định các mức độ tác động. Điều này có thể bao gồm nhưng không giới hạn tới

- Ước tính tần số của việc thực thi các nguồn đe dọa của các điểm yếu trong một thời gian quy định (ví dụ: 1 năm).
- Chi phí gần đúng cho mỗi lần xuất hiện của việc thực thi các điểm yếu.
- Một yếu tố quan trọng dựa trên sự phân tích chủ quan của các tác động mang tính tương đối của các mối đe dọa thực thi một điểm yếu cụ thể.

3.3.4.7 Xác định các rủi ro

Mục đích của bước này là đánh giá mức độ rủi ro đối với hệ thống . Xác định các rủi ro cho một mối đe dọa/điểm yếu riêng biệt có thể được thể hiện như là một chức năng của:

- Khả năng của việc cố gắng thực thi những điểm yếu.
- Các mức độ tác động sẽ là một nguồn đe dọa để thực thi thành công các điểm yếu.
- Các kế hoạch tương ứng hoặc các kiểm soát bảo mật tồn tại nhằm giảm thiểu hoặc loại bỏ các rủi ro.

Để đo lường các rủi ro, quy mô của các rủi ro và mức độ rủi ro phải được phát triển.

a. Ma trận mức độ rủi ro.

Việc cuối cùng là việc xác định các rủi ro được xác định bằng cách nhân các dãy số của các mối đe dọa có khả năng thực hiện và các tác động của các mối đe dọa đó. Bảng dưới đây sẽ cho thấy làm như thế nào để sắp xếp các thứ hạng rủi ro một cách tổng thể có thể được xác định dựa trên các yếu tố đầu vào từ các mối đe dọa và các loại đe dọa. Ma trận dưới đây là một ma trận 4x4 các khả năng của các mối đe dọa (cao, trung bình, thấp), khả năng khai thác các mối đe dọa (cao, trung bình, thấp), giá trị tài sản từ (0 -> 4). Tùy thuộc vào các yêu cầu của tổ chức và độ chi tiết của đánh giá rủi ro mà tổ chức có thể sử dụng ma trận 4x4 hoặc 5x5.. Mức độ rủi ro rất cao có thể yêu cầu tắt hệ thống hoặc ngừng tất cả các tích hợp hệ thống thống thông tin và những nỗ lực thử nghiệm.

Ma trận trong bảng dưới chỉ ra làm thế nào để tính các mức độ rủi ro ở mức cao, trung bình, thấp. Việc xác định các mức độ của rủi ro là các đánh giá chủ quan. Giá trị của tài sản và mức độ của mối đe dọa phù hợp với từng kiểu được chỉ ra trong ma trận nhằm chỉ ra chính xác các mức độ khi chúng kết hợp với nhau từ 0 đến 8. Các giá trị được đặt trong ma trận một cách có cấu trúc. Giả sử khả năng của các mối đe dọa là thấp, khả năng khai thác mối đe dọa đó là trung bình, mà giá trị

của tài sản ở mức độ là 2 thì thước đo rủi ro của rủi ro đó là 3. Nghĩa của các mức độ rủi ro từ 0 – 8 là:

- Rủi ro thấp: 0 – 2
- Rủi ro trung bình: 3 – 5
- Rủi ro cao: 6 - 8

Ma trận như sau:

	Khả năng của các mối đe dọa	Thấp (L)			Trung bình(M)			Cao(H)		
	Khả năng khai thác các mối đe dọa	L	M	H	L	M	H	L	M	H
Giá trị của tài sản	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Bảng 7: Ma trận mức độ rủi ro

b. Miêu tả mức độ rủi ro

Bảng 8 miêu tả mức độ rủi ro trong bảng 7. Thang đo rủi ro với các mức cao, trung bình, thấp, đại diện cho các mức độ hay cấp rủi ro mà một hệ thống thông tin, các thủ tục có liên quan khi một điểm yếu được thực hiện. Thang đo rủi ro

trình bày các hành động mà các quản lý cấp cao, các nhiệm vụ của người sở hữu phải thực hiện đối với mỗi mức độ rủi ro.

Mức độ rủi ro	Miêu tả rủi ro và các hành động cần thiết
Cao	Nếu việc quan sát hoặc tìm kiếm được đánh giá như một rủi ro ở mức độ cao và mạnh thì điều cần thiết là phải tìm được biện pháp khắc khục. Một hệ thống đang tồn tại có thể tiếp tục hoạt động nhưng một kế hoạch hành động đúng phải đưa ra càng sớm càng tốt.
Trung bình	Nếu việc quan sát được đánh giá là rủi ro ở mức độ trung bình hành động khắc phục là cần thiết và kế hoạch phải được phát triển để kết hợp với những hành động này trong một thời gian hợp lý.
Thấp	Nếu việc quan sát được mô tả là một mức độ rủi ro thấp, DDA của hệ thống phải xác định các hành động khắc phục khi vẫn còn yêu cầu hoặc quyết định chấp nhận rủi ro.

Bảng 8: Thang đo rủi ro và các hành động cần thiết

3.3.4.8 Bước 8: Các khuyến cáo kiểm soát

Trong bước này các kiểm soát phải được giảm thiểu hoặc loại bỏ những rủi ro đã được xác định và phải phù hợp với hoạt động của tổ chức. Mục tiêu của các kiểm soát là giảm thiểu mức độ rủi ro với hệ thống thông tin và các dữ liệu của nó nhằm đạt tới một mức độ có thể chấp nhận được. Các yếu tố sau đây có thể xem xét các kiểm soát được khuyến cáo và các giải pháp thay thế để giảm thiểu hoặc loại bỏ các rủi ro được xác định.

- Tính hiệu quả của các tùy chọn được khuyến cáo (ví dụ: Tính tương thích hệ thống)
- Các pháp luật và các quy định
- Chính sách của tổ chức
- Các ảnh hưởng của tác động

- An toàn và độ tin cậy

Các kiểm soát được để xuất là kết quả của quá trình đánh giá rủi ro và cung cấp đầu vào cho quá trình giảm thiểu rủi ro, trong các thủ tục khuyến cáo và công nghệ kiểm soát bảo mật là đều được đánh giá, đưa ra độ ưu tiên và thực thi. Cần lưu ý rằng không phải tất cả các kiểm soát có khả năng được khuyến cáo có thể thực hiện nhằm giảm thiểu các tổn thất. Để xác định những gì được yêu cầu và cần thiết cho một tổ chức thì cần phải phân tích các chi phí, nên thực thi các kiểm soát khuyến cáo có thể chứng minh rằng các chi phí thực thi kiểm soát có thể được minh chứng bằng việc giảm thiểu mức độ rủi ro. Ngoài ra ảnh hưởng của tác động (ví dụ : ảnh hưởng tới năng suất của hệ thống) và tính khả thi (ví dụ: các yêu cầu kĩ thuật, sự chấp nhận của người dùng) đều đưa ra các tùy chọn khuyến cáo cần tính toán cần thận trong suốt quá trình giảm thiểu rủi ro.

3.3.4.9 Bước 9: Tài liệu kết quả

Khi đánh giá rủi ro hoàn thành (xác định nguồn đe dọa và các điểm yếu được xác định và đưa ra đánh giá rủi ro, các kiểm soát khuyến cáo), các kết quả sẽ được ghi lại trong một báo cáo chính thức. Một báo cáo đánh giá rủi ro là một báo cáo quản lý nhằm giúp đỡ các quản lý cấp cao, chủ sở hữu thông tin đưa ra các quyết định về chính sách, ngân sách, thủ tục và sự thay đổi trong việc hoạt động hay quản lý. Không giống như các báo cáo về kiểm toán hoặc các báo cáo nghiên cứu tìm kiếm ra những việc làm sai trái, các báo cáo đánh giá rủi ro sẽ không được trình bày giống như kiểu buộc tội mà nó giống như một phương pháp tiếp cận có hệ thống và việc phân tích các rủi ro để đánh giá rủi ro nhằm cho người quản lý sẽ hiểu được các rủi ro đó, sau đó sẽ phân bổ nguồn lực để giảm bớt hay xác định đúng các thiệt hại. Vì lý do này một số người chỉ thích các mối đe dọa/điểm yếu đã được xác định trước hơn là phát hiện các điểm yếu đó trong báo cáo đánh giá rủi ro.

3.3.5 Giảm thiểu rủi ro

Giảm thiểu rủi ro là bước thứ 2 trong quá trình quản lý rủi ro, liên quan đến độ ưu tiên, tính toán và thực hiện một cách phù hợp các kiểm soát giảm thiểu rủi ro được khuyến nghị từ quá trình đánh giá rủi ro. Vì việc loại bỏ tất cả các rủi ro chắc

chắn là một việc không thể làm được, đây là trách nhiệm của người quản lý cấp cao và người quản lý các doanh nghiệp nhằm sử dụng các phương pháp với chi phí thấp nhất, thực thi các kiểm soát thích hợp nhất để giảm các rủi ro xuống một mức độ có thể chấp nhận được với các ảnh hưởng bất lợi với tài nguyên và chức năng của tổ chức là tối thiểu nhất.

3.3.5.1 Lựa chọn giảm thiểu rủi ro

Giảm thiểu rủi ro là một phương pháp sử dụng bởi các quản lý cấp cao nhằm giảm thiểu các nguy cơ rủi ro xảy ra. Giảm thiểu rủi ro có thể đạt được thông qua bất kì một lựa chọn giảm thiểu rủi ro nào dưới đây:

- Chấp nhận rủi ro: Chấp nhận các rủi ro có tiềm năng và tiếp tục điều hành hệ thống thông tin hoặc thực thi các kiểm soát để giảm các rủi ro xuống một mức độ có thể chấp nhận được.
- Tránh các rủi ro: Tránh các rủi ro bằng cách loại bỏ các nguyên nhân gây ra rủi ro và/hoặc các hậu quả (ví dụ: Từ bỏ một số chức năng của hệ thống hoặc tắt hệ thống khi rủi ro được xác định)
- Hạn chế rủi ro: Hạn chế rủi ro bằng cách thực thi các kiểm soát nhằm giảm thiểu các tác động bất lợi của việc thực thi các mối đe dọa thành một điểm yếu (ví dụ: sử dụng việc hỗ trợ, phòng ngừa, dò tìm các kiểm soát).
- Kế hoạch rủi ro: Quản lý các rủi ro bằng cách phát triển một kế hoạch giảm thiểu rủi ro, thực thi và duy trì các kiểm soát.
- Nghiên cứu và độ hiểu biết: Giảm thiểu rủi ro bằng cách hiểu biết về các điểm yếu hoặc các lỗi và nghiên cứu các kiểm soát để sửa chữa các điểm yếu đó.
- Chuyển đổi rủi ro: Chuyển đổi rủi ro bằng cách sử dụng các tùy chọn khác để bù đắp cho các mất mát ví dụ như mua bảo hiểm.

Các mục tiêu và nhiệm vụ của một tổ chức cần được xem xét trong việc lựa chọn bất kì cách giảm thiểu rủi ro nào. Đây chỉ là lý thuyết để xác định tất cả những rủi ro vì vậy độ ưu tiên nên được đặt ra đối với các mối đe dọa và các điểm yếu mà có khả năng gây tổn hại hoặc gây ảnh hưởng tới tổ chức.

3.3.5.2 Chiến lược giảm thiểu rủi ro

Các quản lý cấp cao, nhiệm vụ của các chủ sở hữu phải biết được những rủi ro tiềm năng và các kiểm soát khuyến cáo, họ có thể đặt ra câu hỏi "khi nào và trường hợp nào tôi cần đưa ra hành động gì? Khi nào tôi nên thực hiện những kiểm soát để giảm thiểu rủi ro và bảo vệ cho tổ chức của chúng tôi"?

Chiến lược này tiếp tục được nêu ra trong các quy định ở dưới đây, quy định này cung cấp các hướng dẫn hay các hành động để nhằm giảm thiểu rủi ro từ các mối đe dọa do chủ ý của con người:

- Khi điểm yếu tồn tại -> thực thi các kỹ thuật đảm bảo giảm khả năng các điểm yếu được thực thi.
- Khi một điểm yếu được thực thi -> áp dụng cách bảo vệ các lớp, thiết kế các kiến trúc và quản lý kiểm soát nhằm giảm thiểu các rủi ro hoặc ngăn ngừa để không cho chúng xuất hiện
- Khi giá phải trả của kẻ tấn công ít hơn số lợi kiếm được -> áp dụng việc bảo vệ để giảm động cơ của kẻ tấn công bằng cách gia tăng chi phí của kẻ tấn công (ví dụ: sử dụng hệ thống kiểm soát như hạn chế hệ thống người dùng truy cập và có thể làm giảm đáng kể sự tấn công của một attacker)
- Khi mất mát là quá lớn -> áp dụng các nguyên tắc thiết kế, thiết kế kiến trúc và các phương pháp bảo vệ kĩ thuật hoặc phi kĩ thuật để hạn chế mức nghiêm trọng của cuộc tấn công, từ đó làm hạn chế sự mất mát.

Các phương pháp nêu trên có các danh sách loại trừ (khi chi phí mà kẻ tấn công bỏ ra nhỏ hơn những gì đạt được) cũng có thể áp dụng để giảm thiểu rủi ro phát sinh từ môi trường hoặc sự vô ý của con người (ví dụ lỗi hệ thống hay lỗi do người dùng).

3.3.5.3 Cách tiếp cận để thực hiện các kiểm soát

Khi kiểm soát các hành động phải thực hiện những quy tắc dưới đây:

- Xác định chính xác những rủi ro lớn nhất và cố gắng giảm thiểu rủi ro làm sao cho chi phí trả cho rủi ro đó là thấp nhất, với việc giảm tối thiểu khả năng tác động tới các nhiệm vụ khác.

Các phương pháp giảm thiểu rủi ro miêu tả các phương pháp thực thi kiểm soát:

- Bước 1: Ưu tiên các hành động

Căn cứ vào mức độ rủi ro được trình bày trong báo cáo đánh giá rủi ro, thực thi những hành động được ưu tiên. Trong việc phân bổ nguồn lực, ưu tiên hàng đầu cần được thực hiện với các rủi ro đó là phải lập ra bảng xếp hạng các rủi ro mức cao (ví dụ: rủi ro rất cao hoặc mức rủi ro cao). Những điểm yếu/đe dọa này sẽ yêu cầu các hành động khắc phục ngay lập tức để bảo vệ quyền lợi và công việc kinh doanh của tổ chức.

- Bước 2: Đánh giá tùy chọn kiểm soát được khuyến cáo.

Các kiểm soát được khuyến cáo trong quá trình đánh giá rủi ro có thể không phải là sự lựa chọn thích hợp nhất và khả thi nhất cho một tổ chức và hệ thống thông tin cụ thể. Trong suốt bước này, tính khả thi (ví dụ: tính tương thích, sự chấp nhận của người dùng) và hiệu quả (ví dụ: Mức độ bảo vệ và mức giảm thiểu rủi ro) của các tùy chọn kiểm soát khuyến cáo đã được phân tích. Mục tiêu là để lựa chọn kiểm soát thích hợp nhất cho việc giảm thiểu rủi ro.

- Bước 3: Tiến hành phân tích chi phí – lợi ích.

Để hỗ trợ quản lý trong việc ra quyết định và xác định chi phí – lợi ích của các kiểm soát, việc phân tích chi phí-lợi ích cần phải được thực hiện.

- Bước 4: Dựa trên kết quả của việc phân tích chi phí – lợi ích, quản lý sẽ xác định chi phí – lợi ích của các kiểm soát được đưa ra nhằm mục đích giảm thiểu rủi ro cho tổ chức. Các kiểm soát được lựa chọn nên kết hợp kỹ thuật, hoạt động, các yếu tố quản lý kiểm soát để đảm bảo an ninh đầy đủ cho hệ thống thông tin và tổ chức.
- Bước 5: Phân bổ trách nhiệm

Những người thích hợp (ở trong tổ chức hoặc nhân viên ký hợp đồng ở ngoài) người mà có chuyên môn phù hợp và các kỹ năng để thực thi các kiểm soát được lựa chọn đã xác định sẵn và trách nhiệm phải được phân bổ cho từng người.

- Bước 6: Xây dựng các kế hoạch thực thi phương pháp bảo vệ

Trong bước này kế hoạch thực thi phương pháp bảo vệ (hoặc các kế hoạch hành động) được phát triển. Kế hoạch phải bao gồm những thông tin sau:

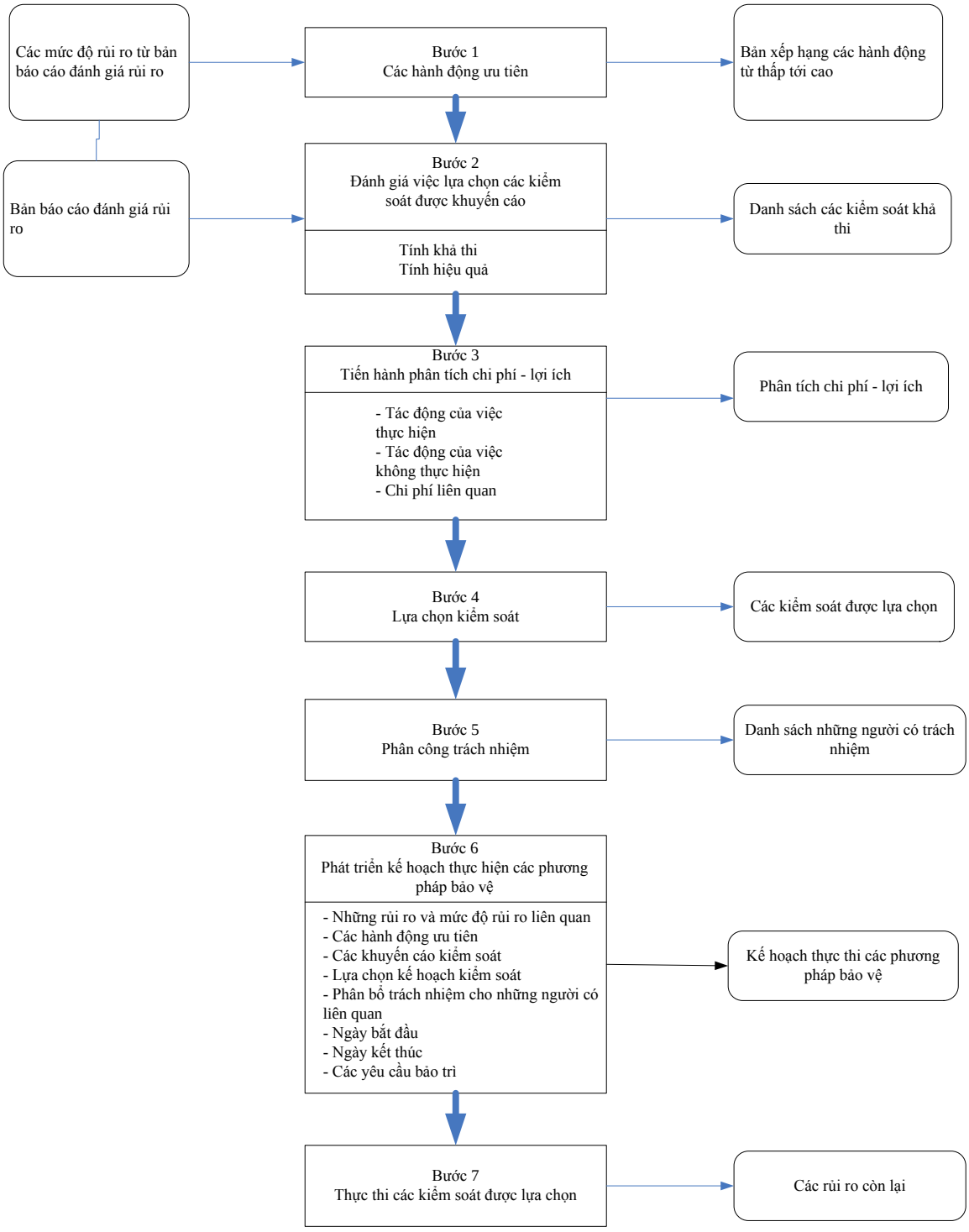
- Rủi ro (điểm yếu/đe dọa) và các mức rủi ro liên quan (Output từ các báo cáo đánh giá rủi ro)
- Các khuyến cáo về kiểm soát (Output từ báo cáo đánh giá rủi ro)
- Các hành động ưu tiên (Với độ ưu tiên cho mức rủi ro rất cao và cao)
- Lựa chọn các kế hoạch kiểm soát (Xác định dựa trên tính khả thi, tính hiệu quả, lợi ích đối với tổ chức và giá thành)
- Yêu cầu các nguồn lực cho việc thực thi để lên kế hoạch lựa chọn kiểm soát
- Danh sách các nhân viên và các đội phải có trách nhiệm với các công việc liên quan.
- Ngày bắt đầu thực hiện
- Ngày hoàn thành mục tiêu
- Các yêu cầu bảo trì

Ưu tiên về mặt thực thi và thời gian bắt đầu hay kết thúc dự án. Kế hoạch này sẽ được hỗ trợ và thực hiện quá trình giảm thiểu rủi ro.

- Bước 7: Thực hiện việc lựa chọn các kiểm soát

Tùy thuộc vào mỗi tình huống riêng mà việc thực thi các kiểm soát có thể giảm cấp độ rủi ro xuống thấp hơn nhưng không thể loại trừ rủi ro.

Input	Risk Mitigation Activities	Output



Hình 6: Biểu đồ phương pháp giảm thiểu rủi ro

3.3.5.4 Các loại kiểm soát

Trong việc thực thi các kiểm soát được khuyến cáo để giảm thiểu rủi ro, một tổ chức nên xem xét các kỹ thuật, quản lý và hoạt động kiểm soát bảo mật hoặc kết

hợp với các kiểm soát để nhằm tối đa hóa tính hiệu quả của kiểm soát đối với hệ thống thông tin và đối với tổ chức. Các kiểm soát bảo mật khi sử dụng một cách thích hợp có thể ngăn ngừa, hạn chế, hoặc ngăn chặn các mối đe dọa đối với tổ chức.

Quá trình khuyến cáo các kiểm soát sẽ bao gồm việc lựa chọn giữa sự kết hợp với kỹ thuật, quản lý và hoạt động kiểm soát nhằm cải thiện tình hình bảo mật của tổ chức. Sự thỏa hiệp phải được tổ chức xem xét một cách rõ ràng bằng cách xem lại các quyết định liên quan tới việc sử dụng mật khẩu người dùng một cách phức tạp để giảm thiểu việc dò tìm và phá vỡ mật khẩu. Trong trường hợp này một kiểm soát kĩ thuật cần phải yêu cầu các tiện ích bảo mật cần phức tạp hơn, đắt hơn những thủ tục kiểm soát nhưng các kiểm soát kĩ thuật cũng phải hiệu quả hơn bởi vì hệ thống hoạt động một cách tự động. Mặt khác một thủ tục kiểm soát có thể được thực thi một cách đơn giản bằng cách ghi nhớ tất cả các cá nhân liên quan và sửa đổi các hướng dẫn bảo mật cho tổ chức nhưng người dùng lại rất khó có thể ghi nhớ và thực hiện theo hướng dẫn đó và điều này có nghĩa là cần phải yêu cầu đào tạo nhằm nâng cao nhận thức và có được sự chấp nhận của người dùng.

a. Kĩ thuật kiểm soát bảo mật

Kĩ thuật kiểm soát nhằm giảm thiểu rủi ro có thể được cài đặt để bảo vệ chống lại các mối đe dọa. Những kiểm soát này có thể từ đơn giản tới phức tạp và nó thường liên quan tới cấu trúc hệ thống, các kĩ thuật, các gói bảo mật với việc pha trộn giữa phần cứng, phần mềm và phần sụn. Tất cả những biện pháp cần làm việc cùng với nhau để bảo vệ các dữ liệu quan trọng và nhạy cảm, chức năng của thông tin và chức năng của hệ thống thông tin. Kỹ thuật kiểm soát có thể được phân thành các loại chính sau đây, thông thường phân loại theo các mục đích chính:

- Hỗ trợ: Hỗ trợ các kiểm soát đều có đặc điểm chung và hầu hết đảm bảo chức năng bảo mật cho hệ thống thông tin. Những kiểm soát phải được đặt vào đúng chỗ để thực thi các kiểm soát khác.
- Ngăn ngừa: Các kiểm soát ngăn ngừa tập trung vào việc ngăn chặn các vi phạm bảo mật từ khi xảy ra ở nơi đầu tiên.

- Phát hiện và phục hồi: Những kiểm soát tập trung vào việc phát hiện và phục hồi từ những vi phạm bảo mật.

b. Hỗ trợ kĩ thuật kiểm soát

Các kiểm soát hỗ trợ đều quan hệ với những kiểm soát khác. Các kiểm soát hỗ trợ như sau:

- Nhận diện: Các kiểm soát cung cấp khả năng để nhận diện người sử dụng, các quy trình và thông tin tài nguyên. Thực thi các kiểm soát khác (ví dụ: Kiểm soát truy cập tùy ý (DAC), kiểm soát truy cập bắt buộc (MAC), kiểm toán) đó là các đối tượng cần thiết để nhận dạng.
- Quản lý khóa mã hóa: Các khóa mã hóa phải được quản lý an toàn khi chức năng mã hóa được thực hiện trong các kiểm soát khác nhau. Quản lý khóa mã hóa bao gồm các khóa chính, việc phân phối, lưu trữ và duy trì khóa.
- Quản trị bảo mật: Bảo mật các tính năng của hệ thống thông tin phải được cài đặt (ví dụ: enable hoặc disable) để đáp ứng nhu cầu cần thiết của một cài đặt cụ thể và để tính toán cho sự thay đổi trong môi trường hệ thống. Hệ thống bảo mật có thể được xây dựng thành hệ điều hành bảo mật hoặc các ứng dụng bảo mật. Các tiện ích bảo mật thương mại thì phải có sẵn.
- Bảo vệ hệ thống: Khả năng của các chức năng bảo mật khác nhau của hệ thống là cơ sở của bảo mật trong kĩ thuật thực thi. Điều này thể hiện chất lượng của việc thực thi từ tiến độ của cả quá trình thiết kế và của cách thức mà việc thực thi được hoàn thành. Một số ví dụ của việc bảo vệ hệ thống là bảo vệ thông tin còn sót lại (được biết như việc tái sử dụng đối tượng), các đặc quyền tối thiểu (hoặc ‘need to know), bóc tách quy trình, các module, các tầng và giảm thiểu những thứ cần được tin cậy.

c. Kỹ thuật kiểm soát dự phòng

Các kiểm soát này có thể ngăn cản các vi phạm chính sách an ninh bao gồm:

- Xác thực: Kiểm soát xác thực cung cấp các phương tiện để xác minh danh tính của đối tượng nhằm đảm bảo rằng các yêu cầu đã tuyên bố là hợp lệ.

Các cơ chế xác thực bao gồm: password, mã số cá nhân, mã PIN, và các công nghệ cung cấp xác thực mạnh như: token, smart card, digital certificate, kerberos).

- Ủy quyền: Kiểm soát ủy quyền cho phép các đặc điểm kỹ thuật và sau đó là quản lý các hành động cho phép đối với một hệ thống được đặt ra (ví dụ: chủ sở hữu thông tin hoặc người quản trị cơ sở giữ liệu, người có thể cập nhật việc truy cập các file được chia sẻ bởi một nhóm người dùng trực tuyến).
- Thực thi kiểm soát truy cập: Tính toàn vẹn dữ liệu và bảo mật dữ liệu được thực thi bởi việc kiểm soát truy cập. Khi một đối tượng yêu cầu được ủy quyền để truy cập vào một quy trình cụ thể, nó cần phải được thực thi các chính sách bảo mật đã được định nghĩa (ví dụ: MAC, DAC..). Các chính sách kiểm soát cơ bản này được thực thi thông qua các cơ chế kiểm soát (ví dụ: Nhãn nhạy cảm MAC, quyền cho phép truy cập vào tập tin DAC, Danh sách kiểm soát truy cập, vai trò, hồ sơ người dùng). Hiệu quả và sức mạnh của kiểm soát truy cập phụ thuộc vào sự đúng đắn của các quyết định kiểm soát truy cập (ví dụ: làm thế nào để các luật bảo mật được cài đặt) và sức mạnh của việc thực thi kiểm soát truy cập (ví dụ: Việc thiết kế bảo mật phần mềm hoặc bảo mật phần cứng).
- Chống chối bỏ: Hệ thống kiểm toán phụ thuộc vào khả năng đảm bảo việc người gửi không thể từ chối mọi thông tin mà họ đã gửi và người nhận không thể từ chối mọi thông tin mà họ đã nhận. Các kiểm soát này thường được áp dụng tại các điểm truyền hoặc, các điểm nhận.
- Bảo vệ đường truyền: Trong một hệ thống phân phối, Khả năng hoàn thành việc bảo mật đối tượng phải phụ thuộc vào sự tin cậy của đường truyền. Kiểm soát bảo vệ đường truyền đảm bảo tính toàn vẹn, sẵn sàng và bí mật của thông tin nhạy cảm và quan trọng hơn là việc truyền các thông tin này. Bảo vệ đường truyền sử dụng các phương pháp mã hóa (ví dụ: mạng riêng ảo, các giao thức bảo mật đường truyền như: IPSEC) và triển khai các công nghệ mã hóa như (DES, 3DES, RAS, MD4, MD5, các hàm băm, và các

thuật toán mã hóa như Clipper) để giảm thiểu các đe dọa trên mạng như: tấn công phát lại, packet sniffing, nghe lén……

- Bảo mật giao dịch: Cả hai hệ thống gồm hệ thống chính phủ và hệ thống riêng lẻ đều yêu cầu vấn đề về riêng tư cá nhân. Kiểm soát bảo mật giao dịch (ví dụ: SSL, secure shell) đều bảo vệ chống lại sự mất việc mất quyền riêng tư đối với các giao dịch cá nhân riêng lẻ.

d. Phát hiện và phục hồi các kiểm soát kỹ thuật

Dò tìm các kiểm soát cảnh báo vi phạm hoặc vi phạm các chính sách an ninh và bao gồm các kiểm soát như: vết kiểm toán, phương pháp phát hiện xâm nhập, checksum. Phục hồi các kiểm soát có thể được sử dụng để khôi phục lại các tài nguyên máy tính bị mất. Chúng thì cần thiết như việc bổ sung sự hỗ trợ và các biện pháp phòng ngừa bởi vì không ai trong số các phương án đó là tốt tuyệt đối. Phát hiện và phục hồi các kiểm soát bao gồm:

- Kiểm toán: Kiểm toán các sự kiện liên quan tới bảo mật và theo dõi, giám sát sự bất thường của hệ thống là yếu tố chính trong việc dò tìm, phục hồi từ các vi phạm bảo mật.
- Phát hiện ngăn chặn xâm nhập là điều cần thiết để dò tìm các vi phạm bảo mật (ví dụ: bẻ gãy mạng, các hành động đáng ngờ) vì vậy đó là một phản ứng xuất hiện được thông báo kịp thờ. Nó sử dụng để phát hiện vi phạm an ninh nếu không có phản ứng hiệu quả nào được khởi tạo. Kiểm soát Phát hiện và ngăn chặn xâm nhập cung cấp hai khả năng ngăn chặn và xâm nhập.
- Bằng chứng của sự đầy đủ. Các kiểm soát bằng chứng của sự đầy đủ (ví dụ: công cụ tính toàn vẹn của hệ thống) phân tích tính toàn vẹn hệ thống và xác định các mối đe dọa tiềm năng. Các kiểm soát này không ngăn chặn sự vi phạm chính sách bảo mật nhưng lại dò tìm các vi phạm đó và giúp đỡ việc xác định các hành động hỗ trợ cần thiết.

e. Các kiểm soát quản lý bảo mật.

Các kiểm soát quản lý bảo mật, kết hợp với các kiểm soát kỹ thuật, hoạt động được thực thi để quản lý và giảm thiểu rủi ro để bảo vệ nhiệm vụ của tổ chức. Các kiểm soát quản lý tập trung vào việc cung cấp các chính sách bảo vệ thông tin, hướng dẫn và các chuẩn được thực hiện thông qua các thủ tục để hoàn thành đầy đủ mục tiêu của tổ chức. Các kiểm soát quản lý bảo mật – Ngăn chặn, dò tìm và phục hồi cái mà được thực thi để giảm thiểu rủi ro. Các kiểm soát này bao gồm:

- Phân công trách nhiệm để đảm bảo rằng luôn bảo mật đầy đủ cho tổ chức.
- Phát triển và duy trì các kế hoạch bảo mật hệ thống với các tài liệu kiểm soát hiện tại và các kế hoạch kiểm soát cho hệ thống thông tin trong việc hỗ trợ cho tổ chức.
- Thực thi các kiểm soát bảo mật cá nhân, bao gồm việc phân chia nhiệm vụ, đặc quyền tối thiểu, người đăng nhập vào máy tính và các điểm đầu cuối.
- Thực hiện nâng cao nhận thức và đào tạo về kĩ thuật cho người sử dụng để đảm bảo rằng người dùng đầu cuối và người dùng trong hệ thống luôn nhận thức được các nguyên tắc đạo đức và trách nhiệm của họ trong việc bảo vệ quyền lợi của tổ chức.

f. Dò tìm các kiểm soát quản lý bảo mật

Dò tìm các kiểm soát bảo mật như sau:

- Thực thi các kiểm soát bảo mật cá nhân bao gồm các nhân viên đã thôi việc, chuyển giao nhiệm vụ.
- Thực hiện việc xem xét lại định kỳ các kiểm soát bảo mật để đảm bảo rằng các kiểm soát đó vẫn có hiệu quả.
- Thực hiện kiểm toán hệ thống định kỳ
- Thực hiện việc quản lý rủi ro một cách liên tục để đánh giá và giảm thiểu rủi ro.
- Cho phép hệ thống thông tin xác định và chấp nhận các rủi ro còn lại.

g. Phục hồi các kiểm soát quản lý bảo mật

Các kiểm soát đó là:

- Cung cấp việc hỗ trợ, phát triển, kiểm tra và duy trì tính liên tục của các kế hoạch hoạt động nhằm cung cấp cho tổ chức khi tổ chức rơi vào trường hợp khẩn cấp hoặc thảm họa.
- Thành lập khả năng ứng phó với các sự cố để chuẩn bị cho việc nhận biết, báo cáo và đáp ứng với các tai nạn và trả lại tình trạng hoạt động bình thường cho hệ thống thông tin.

3.3.5.5 Các kiểm soát thao tác bảo mật

Các chuẩn bảo mật cho tổ chức nên được thiết lập thành một tập các kiểm soát và các hướng dẫn để đảm bảo rằng các thủ tục bảo mật được điều chỉnh để sao cho việc sử dụng tài sản và tài nguyên của tổ chức được thực hiện đúng theo quy định, mục tiêu đã đề ra của tổ chức và quyền lợi của tổ chức. Quản lý đóng một vai trò quan trọng trong việc giám sát việc thực thi các chính sách và trong việc đảm bảo thiết lập các kiểm soát phù hợp với hoạt động.

Các kiểm soát được thực thi theo một tập các yêu cầu (ví dụ: kiểm soát kĩ thuật) và các kĩ năng thực thi được sử dụng để sửa chữa các thiếu sót trong việc ngăn ngừa các mối đe dọa. Để đảm bảo tính nhất quán trong các hoạt động bảo mật, từng bước các thủ tục và các phương pháp cho việc thực thi các kiểm soát phải được định nghĩa một cách rõ ràng, được viết thành các tài liệu và phải được duy trì. Các kiểm soát hoạt động bao gồm những điều dưới đây:

a. Kiểm soát các thao tác phòng ngừa

Kiểm soát các thao tác phòng ngừa như sau:

- Kiểm soát truy cập các thiết bị di động (ví dụ: kiểm soát truy cập vật lý…)
- Hạn chế phân phối dữ liệu ra bên ngoài (ví dụ: sử dụng nhãn)
- Kiểm soát các phần mềm diệt virus
- Bảo vệ các cơ sở máy tính (ví dụ: nhân viên bảo vệ, trang web dành cho client, các hệ thống điện tử, các kiểm soát truy cập bằng phương pháp sinh trắc học, quản lý và phân phối các lock và key, các rào cản)

- Bảo mật hệ thống dây và cable
- Cung cấp khả năng sao lưu dự phòng (ví dụ: thủ tục cho việc sao lưu dữ liệu và hệ thống, lưu giữ các log được lưu lại tất cả các thay đổi cơ sở dữ liệu đã sử dụng trong các kịch bản phục hồi khác nhau)
- Thiết lập các off-site để lưu trữ các thủ tục và bảo mật
- Bảo vệ laptop, PC, và các workstation
- Bảo vệ tài sản thông tin khỏi các thiệt hại về lửa (ví dụ: các yêu cầu và các thủ tục cho việc sử dụng bình chữa cháy, vải không thấm nước, hệ thống tưới phun khô…)
- Cung cấp nguồn điện khẩn cấp (ví dụ: Nguồn dự trữ điện để nguồn điện không bị ngắt, máy phát điện tại chỗ)
- Kiểm soát độ ẩm và nhiệt độ của nơi đặt máy tính (ví dụ: hoạt động của điều hòa, phân tán nhiệt)

b. Kiểm soát các biện pháp dò tìm

Kiểm soát các biện pháp dò tìm bao gồm những điều dưới đây:

- Cung cấp bảo mật vật lý (ví dụ: sử dụng các thiết bị dò chuyển động, đóng mạch giám sát truyền hình, bộ cảm biến và báo động)
- Đảm bảo môi trường bảo mật (ví dụ: sử dụng máy phát hiện khói và lửa, cảm biến và cảnh báo)

3.2.5.6 Phân tích lợi ích chi phí

Để phân bổ tài nguyên và thực thi các kiểm soát giá hiệu quả nhất, các tổ chức, sau khi xác định tất cả các kiểm soát và đánh giá tính khả thi, tính hiệu quả nên tiến hành phân tích lợi ích chi phí cho mỗi kiểm soát được đề xuất nhằm đưa ra những kiểm soát được yêu cầu phù hợp với hoàn cảnh của họ.

Phân tích lợi ích chi phí có thể là định tính hay định lượng. Mục đích của việc này là để chứng minh rằng chi phí thực hiện các kiểm soát có thể được chứng minh

bằng cách giảm mức độ rủi ro. Ví dụ như một tổ chức không muốn dành 1000$ cho một kiểm soát để giảm thiểu rủi ro giá 200$

Phân tích chi phí lợi ích cho các kiểm soát mới được đề ra hoặc các kiểm soát nâng cao ở dưới đây:

- Xác định các tác động của việc thực thi các kiểm soát mới hoặc các kiểm soát được nâng cao
- Xác định các tác động của việc không thực thi các kiểm soát mới hoặc các kiểm soát được nâng cao.
- Ước tính chi phí thực thi. Có thể bao gồm hoặc không hạn chế những điều dưới đây:
    - Mua phần cứng và phần mềm.
    - Giảm hiệu quả hoạt động nếu hiệu suất và năng suất của hệ. thống bị giảm đối với việc tăng cường bảo mật.
    - Chi phí để thực hiện thêm các chính sách và các thủ tục được thêm vào.
    - Chi phí thuê nhân sự để thực thi các chính sách, thủ tục hay các dịch vụ đã đưa ra
    - Chi phí đào tạo
    - Chi phí bảo trì
- Đánh giá các chi phí thực thi và lợi ích đối với hệ thống và dữ liệu để xác định tầm quan trọng với tổ chức khi thực thi các kiểm soát mới, đưa ra chi phí thực hiện và tác động của các kiểm soát đó.

Tổ chức sẽ cần phải đánh giá lợi ích của các kiểm soát trong việc duy trì các nhiệm vụ có thể chấp nhận được cho tổ chức. Cũng như có các chi phí cho việc thực thi các kiểm soát cần thiết, chi phí cho việc không thực thi nó. Với các kết quả liên quan của việc không thực thi kiểm soát, tổ chức có thể xác định xem nó có khả thi để loại bỏ việc thực hiện kiểm soát đó không.

Ví dụ về phân tích chi phí lợi ích: Hệ thống lưu trữ X và xử lý thông tin quan trọng, nhạy cảm hoặc riêng tư của cá nhân, tuy nhiêm kiểm toán chưa được kích hoạt trên hệ thống này. Phân tích chi phí lợi ích đã được tiến hành để xác định xem tính năng kiểm toán đó có nên được kích hoạt cho hệ thống X hay không. Mục (1) và (2) chỉ ra các tác động không nhìn thấy được (ví dụ: các yếu tố ngăn chặn) để thực hiện hoặc không thực hiện kiểm soát mới. Mục (3) liệt kê ra các tác động có thể thấy được (ví dụ: chi phí thực tế)

1) Tác động của việc kích hoạt kiểm toán hệ thống: kiểm toán hệ thống cho phép hệ thống quản trị bảo mật theo dõi hoạt động hệ thống của người dùng nhưng sẽ làm giảm hiệu suất của hệ thống do đó điều này sẽ ảnh hưởng tới năng suất của người dùng. Ngoài ra khi thực thi thì sẽ cần thêm các nguồn tài nguyên.
2) Tác động của việc không kích hoạt kiểm toán hệ thống: Hoạt động người dùng hệ thống và các vi phạm không được theo dõi hoặc giám sát nếu chức năng kiểm toán hệ thống bị ẩn đi, vấn đề bảo mật không thể được tối đa để bảo vệ dữ liệu mật, nhiệm vụ của tổ chức.
3) Chi phí dự toán cho việc kích hoạt kiểm toán hệ thống:

Chi phí dự toán	Giá phải trả
Chi phí cho kích hoạt đặc điểm kiểm toán hệ thống – Không chi phí, xây dựng đặc điểm	0$
Thêm nhân viên để tiến hành kiểm toán và lưu trữ mỗi năm	X$
Đào tạo (ví dụ: Cài đặt hệ thống kiểm toán, phát sinh báo cáo)	Y$
Phần mềm Add-on báo cáo kiểm toán	Z$
Duy trì dữ liệu kiểm toán (ví dụ: Lưu trữ) một năm	M$

Tổng giá phải trả	X + Y + Z + M = G$

Bảng 9: Ví dụ tổng chi phí dự toán cho việc kích hoạt kiểm toán hệ thống

Người quản lý của tổ chức phải xác định rằng nên tiếp tục chấp nhận mức độ rủi ro nào. Tác động của kiểm soát có thể được đánh giá và bao gồm một trong hai kiểm soát sẽ được loại trừ hay giữ lại, sau khi tổ chức xác định một loạt các mức độ rủi ro khả thi. Phạm vi này sẽ khác nhau giữa các tổ chức tuy nhiên các quy tắc áp dụng trong việc xác định sử dụng những kiểm soát mới thì lại giống nhau:

- Nếu kiểm soát giảm được rủi ro nhiều hơn cần thiết thì nên xem liệu tốn kém một chút so với sự tồn tại của kiểm soát đó thì cái gì sẽ hơn.
- Nếu kiểm soát có chi phí nhiều hơn so với việc giảm các rủi ro thì tổ chức sẽ phải tìm kiếm một kiểm soát khác thay thế.
- Nếu kiểm soát đó không giảm rủi ro một cách đầy đủ thì tổ chức phải tìm kiếm các kiểm soát khác hoặc tìm kiếm nhiều kiểm soát hơn để thay thế.
- Nếu kiểm soát cung cấp đầy đủ cho việc giảm thiểu rủi ro và chi phí hiệu quả thì tổ chức nên sử dụng nó.

Thông thường chi phí thực hiện kiểm soát thì có thể rõ ràng hơn là chi phí của việc không thực hiện nó. Như vậy người quản lý cấp cao đóng vai trò quan trọng trong các quyết định liên quan đến việc thực thi các biện pháp kiểm soát để bảo vệ của tổ chức.

3.3.5.7 Rủi ro còn lại

Tổ chức có thể phân tích mức độ giảm thiểu rủi ro được tạo ra bởi các kiểm soát mới hay các kiểm soát nâng cao khả năng giảm thiểu các rủi ro có nguy cơ cao hoặc các tác động, hai tham số xác định mức độ rủi ro cho công việc của tổ chức. Thực hiện các kiểm soát mới hoặc các kiểm soát nâng cao có thể giảm thiểu rủi ro bằng cách:

- Loại bỏ một vài điểm yếu của hệ thống, từ đó có thể giảm được số lượng các mối đe dọa/điểm yếu.

- Thêm các mục tiêu kiểm soát để giảm động lực của các mối đe dọa
- Giảm thiểu độ lớn của các tác động bất lợi (ví dụ: hạn chế phạm vi của một điểm yếu hay chỉnh sửa mối quan hệ tự nhiên giữa hệ thống thông tin và công việc của tổ chức).

Các rủi ro sau khi thực hiện kiểm soát mới hoặc các kiểm soát nâng cao được gọi là các rủi ro còn lại. Thực tế không hệ thống thông tin nào là không có rủi ro và không thể thực hiện được tất cả các kiểm soát để loại bỏ các rủi ro đó, hoặc giảm mức độ của rủi ro xuống bằng 0.

3.3.6 Ước lượng và đánh giá

Trong hầu hết các tổ chức, mạng của tổ chức đó sẽ liên tục được mở rộng, cập nhật, thay đổi các thành phần của nó, các ứng dụng phần mềm sẽ được thay thế hay cập nhật với phiên bản mới nhất. Thêm vào đó nhân sự cũng được thay đổi, các chính sách bảo mật cũng được thay đổi theo thời gian. Ý nghĩa của việc thay đổi này đó là những rủi ro mới sẽ xuất hiện và việc giảm thiểu các rủi ro trước có thể trở thành một mối quan tâm. Như vậy quá trình quản lý rủi ro vẫn diễn ra và phát triển.

3.3.6.1 Thực thi bảo mật tốt.

Quy trình đánh giá rủi ro thường lặp đi lặp lại ít nhất 3 năm một lần. Nên có một lịch trình cụ thể cho việc đánh giá và giảm thiểu rủi ro nhưng chu kỳ thực hiện cũng cần phải linh hoạt đủ để cho phép thay đổi nơi chứng nhận, ví dụ như sự thay đổi từ hệ thống thông tin và xử lý môi trường do thay đổi kết quả từ các chính sách và công nghệ mới.

3.3.6.2 Chìa khóa của sự thành công

Một chương trình quản lý rủi ro thành công phải dựa vào:

- Sự cam kết của người quản lý cấp cao
- Sự hỗ trợ đầy đủ và sự tham gia của đội ngũ làm an toàn thông tin
- Năng lực của đội đánh giá rủi ro, phải có chuyên môn để áp dụng các phương pháp đánh giá rủi ro đến một site và hệ thống cụ thể, xác định

mục tiêu của các rủi ro, cung cấp các biện pháp bảo vệ hiệu quả đáp ứng nhu cầu của tổ chức.

- Nhận thức và hợp tác của các thành viên trong tổ chức những người mà phải tuân theo các thủ tục, thực hiện các kiểm soát nhằm bảo vệ tổ chức
- Ước lượng và đánh giá các nhiệm vụ liên quan đến thông tin phải được triển khai.

3.4 Các bước triển khai ISMS theo chuẩn ISO/IEC 27001:2005

3.4.1 Thiết lập ISMS

Các tuyên bố "shall" được định nghĩa trong ISO/IEC 27001:2005, 4.2.1 cho pha "Plan" như sau:

a. Xác định phạm vi và ranh giới của ISMS

Xác định phạm vi và ranh giới của ISMS trong đặc điểm của tổ chức, công ty, vị trí của nó, tài sản và công nghệ. Phạm vi của ISMS có thể được giới hạn là một phần của tổ chức, được định nghĩa một cách độc lập hoặc phạm vi có thể được xác định là trong toàn tổ chức. Tổ chức có thể lựa chọn phạm vi thích hợp cho ISMS nhưng trong mọi trường hợp phạm vi ISMS và ranh giới xung quanh phạm vi đó cần phải được xác định rõ rang, đầy đủ. Phạm vi cần tính đến các giao diện và sự phụ thuộc ISMS này với các phần khác của tổ chức (không phải trong phạm vi ISMS), các tổ chức khác, người cung cấp thứ 3, hay với bất kì thực thể nào khác ngoài ISMS. Thông tin chi tiết của bất kì ngoại lệ nào từ phạm vi của ISMS phải được ghi nhận và hợp lý. Khi loại trừ các bộ phận của công ty từ phạm vi ISMS, chú ý bất kì thông tin nào trao đổi với phần loại trừ của tổ chức cần được xác định và để địa chỉ sử dụng các giao diện và các phụ thuộc được miêu tả ở trên.

b. Xác định một chính sách ISMS

Xác định một chính sách ISMS phải đặt trong đặc điểm của các công ty, tổ chức, vị trí của nó, tài sản, công nghệ. Các chính sách ISMS phải được tính tới những vấn đề liên quan đến pháp lý và quy định các yêu cầu, hợp đồng hoặc nghĩa vụ của bên thứ 3 và bên phụ thuộc. Quản lý phải phê duyệt chính sách ISMS, và tất cả các nhân viên nên biết các chính sách, hiểu tầm quan trọng, mục đích của nó.

Chính sách này phải bao gồm một khuôn khổ cho việc thiết lập các đối tượng, đưa ra hướng quản lý và hành động, thiết lập các tình huống quản lý rủi ro và đưa ra biện pháp chống lại những nguy cơ đã được tính tới. Chính sách ISMS có thể được xem như là một tập cha của chính sách an toàn thông tin (điều này đã được miêu tả trong ISO/IEC 17799:2005, 5.1.1) ví dụ như các chính sách ISMS đưa ra những vấn đề mà chính sách an toàn thông tin không cần thiết phải đề cấp tới. Những chính sách này có thể được miêu tả trong một tài liệu nếu nó phù hợp cho tổ chức.

c. Xác định phương pháp tiếp cận đánh giá rủi ro của tổ chức.

Đây phải là một phương pháp tiếp cận và phương pháp đó tốt nhất là phù hợp với ISMS, với một doanh nghiệp xác định, với an toàn thông tin và với các yêu cầu pháp lý. Các tổ chức cần bao gồm những tiêu chuẩn cho phép chấp nhận rủi ro và xác định mức độ của rủi ro. Phương pháp đánh giá rủi ro mà một tổ chức thông qua là hoàn toàn quyết định vào tổ chức. Điều quan trọng cần lưu ý là bất cứ một phương pháp nào sử dụng nó cần thỏa thuận với hệ thống quản lý bao gồm tất cả các lĩnh vực ISO/IEC 27001:2005, Annex A, hoặc ISO/IEC 17799. Phương pháp này cần bao gồm những rủi ro liên quan tới tổ chức, kiểm soát nhân sự, quy trình kinh doanh, quy trình vận hành và bảo trì, thủ tục, pháp lý, các quy định, các hợp đồng và các cơ sở xử lý thông tin. Chuẩn BS 7799-3, ISMS quản lý rủi ro, cung cấp thêm thông tin về việc đánh giá rủi ro phù hợp với bước này và mục d, e ở phía dưới. Thêm vào đó phương pháp đánh giá rủi ro được sử dụng nên đảm bảo rằng kết quả đánh giá rủi ro có thể so sánh được và cho ra các kết quả, điều này đặc biệt quan trọng khi đánh giá tình hình rủi ro theo thời gian.

Đánh giá rủi ro là yêu cầu bắt buộc trong ISO/IEC 27001:2005 nhưng nó lại không yêu cầu sử dụng bất kì một công cụ phần mềm tự động nào, mặc dù trong nhiều trường hợp khi sử dụng những công cụ đó ta có được những tiện lợi nhất định. Đặc biệt trong các trường hợp khi những rủi ro cần phải được đánh giá lại và các thông tin liên quan đến như: các nguy cơ, các lỗ hổng, các tài sản cần phải được cập nhật. Sự phức tạp của phương pháp quản lý rủi ro và phương pháp tiếp cận sẽ phụ thuộc vào sự phức tạp của ISMS. Các kỹ thuật được sử dụng nên nhất quán với sự phức tạp và mức độ đảm bảo được yêu cầu bởi tổ chức.

c. Xác định rủi ro đối với tài sản

Xác định rủi ro đối với tài sản có tính tới các mối đe dọa và điểm yếu liên quan tới tài sản này và những tác động làm mất đi tính bí mật, toàn vẹn, sẵn có của tài sản. Việc xác định tài sản, mối đe dọa, các lỗ hổng cần phải liên quan đến việc kiểm soát ở các khu vực khác nhau Điều này là rất quan trọng để đảm bảo rằng tất cả tài sản trong ISMS đều được xác định vì đây là cơ sở để đánh giá rủi ro, và chủ sở hữu được xác định, tài liệu cho mỗi tài sản. Việc xác định những tác động làm mất tính bảo mật, toàn vẹn và sẵn sàng của tài sản nên tính đến những nguy hiểm mà công ty phải đối mặt như về luật pháp, quy định, hợp đồng và yêu cầu của công ty thông qua những thiệt hại đó.

e. Phân tích và đánh giá các rủi ro

Phân tích và đánh giá các rủi ro dựa trên những thông tin được xử lý tại mục d ở trên, chú ý bao gồm tất cả những khu vực điều khiển như: tổ chức, nhân sự, quy trình kinh doanh, điều hành và duy trì, pháp lý, quy định và các vấn đề về hợp đồng, cơ sở xử lý thông tin (xem chuẩn BS 7799-3, chuẩn cung cấp thông tin rõ hơn về quản lý rủi ro). Điều này sẽ liên quan đến việc tổ chức đánh giá kết quả của việc kinh doanh từ những lỗi an toàn, có tính đến hậu quả mất tính bí mật, toàn vẹn, sẵn sàng của các tài sản có thể có. Điều này cũng bao gồm khả năng đánh giá các lỗi khi xảy ra, xem xét các mối đe dọa, điểm yếu được xác định và khả năng xảy đến cùng nhau và gây ra sự cố. Khi đánh giá khả năng xảy ra của một sự cố, người ta thường xem báo cáo về sự cố đã xảy ra và tính toán các báo cáo, thống kê, tin tức và các xu hướng thu được từ mạng. Dựa trên các kết quả này tổ chức cần ước tính mức độ rủi ro và xác định những rủi ro có thể chập nhận được hoặc yêu cầu xử lý, sử dụng các yêu cầu được thiết lập trong mục c, có tính đến bối cảnh của kinh doanh.

f. Xác định và đánh giá các lựa chọn để khắc phục rủi ro.

Khi tổ chức đã xác định, đánh giá và hiểu những tác động của rủi ro có thể có trong kinh doanh thì họ sẽ có những hành động khác nhau để quản lý hay khắc phục những rủi ro đó ở tình hình kinh doanh của họ. Những hành động của tổ chức

có thể xem xét bao gồm việc áp dụng kiểm soát thích hợp giảm thiểu rủi ro, tránh những rủi ro không thông qua cam kết của một hoạt động rủi ro có liên quan, chuyển giao các rủi ro (toàn bộ hoặc một phần) cho một bên khác ví dụ như là doanh nghiệp bảo hiểm hay cố ý hoặc khách quan chấp nhận rủi ro. Những tùy chọn này hoặc kết hợp một số các tuỳ chọn khác của tổ chức, các tổ chức khác nhau với cùng một rủi ro nhưng lại có những kết luận khác nhau, điều này còn phụ thuộc vào đối tượng kinh doanh và tùy từng trường hợp. Trong bất cứ trường hợp nào điều quan trọng vẫn là xác nhận rằng các quyết định này được ghi chép tốt và tổ chức có thể cung cấp bằng chứng để quyết định này được thực hiện với đầy đủ kiến thức về rủi ro và không đơn giản chỉ là sự thiếu hiểu biết.

h. Lựa chọn đối tượng kiểm sóat và kiểm soát khắc phục rủi ro.

Nếu tổ chức quyết định áp dụng các kiểm soát để quản lý và xử lý rủi ro thì họ cần phải lựa chọn một hệ thống kiểm soát thích hợp với mục đích này. Việc lựa chọn này nên tính đến các tiêu chí chấp nhận rủi ro, bao nhiêu kiểm soát giảm thiểu được rủi ro và xác định quy phạm pháp luật, các quy định, các yêu cầu hợp đồng. Đối tượng kiểm soát và kiểm soát phải chọn lựa từ chuẩn ISO/IEC 27001:2005, phụ lục A. Tổ chức cũng có thể lựa chọn thêm các kiểm soát không có trong phụ lục A. Phụ lục A cũng có được coi như là một điểm khởi đầu để đảm bảo rằng không có miền kiểm soát quan trọng hay kiểm soát được bỏ qua. Dĩ nhiên nó có thể chọn các đối tượng không kiểm soát hoặc kiểm soát từ phụ lục A nhưng quyết định nào cũng nên chứng minh và có tuyên cáo được áp dụng. Việc lựa chọn kiểm soát nên có chi phí hiệu quả tức là chi phí thực hiện chúng không được vượt quá tác động của rủi ro về tài chính mà họ đang có ý định giảm thiểu. Tất nhiên một số tác động sẽ phi tài chính. Việc tính toán này cũng nên được thực hiện trong những tác động có liên quan đến sự an toàn, thông tin cá nhân, nghĩa vụ pháp lý, hình ảnh và danh tiếng. Thêm vào đó những nguy cơ dư thừa còn lại sau khi thực hiện các kiểm soát cần phải được đánh giá. Những nguy cơ dư thừa này nói chung là rất khó có thể đánh giá nhưng tổ chức cũng phải ước tính được nó sử dụng ít nhất bao nhiêu điểm kiểm soát để xác định yêu cầu bảo mật, để có được một dấu hiệu cho thấy có nhiều kiểm soát là cần thiết.

h. Bao gồm việc quản lý chấp thuận những nguy cơ còn sót lại.

Quản lý phải chấp thuận các rủi ro dự định sau khi kiểm sóat lựa chọn được thực thi. Các rủi ro dự định có thể vào thời điểm này chỉ là một ước tính và "giai đoạn check" sẽ chứng minh dự toán này đúng. Tuy nhiên, việc quản lý chấp thuận là rất quan trọng ở thời điểm này khi các kiểm soát được lựa chọn cần thực thi và điều này sẽ đòi hỏi tiền bạc, thời gian và các tài nguyên khác.

i. Bao gồm ủy quyền quản lý để thực thi và điều hành ISMS.

Vào cuối của giai đoạn Plan, quản lý phải cho phép thực thi và điều hành ISMS, bằng cách đưa ra tín hiệu chấp thuận và hỗ trợ họ trong các kế hoạch hành động.

k. Chuẩn bị tuyên cáo được áp dụng SOA.

SOA (Statement of Applicability - Tuyên cáo được áp dụng) là một yêu cầu bắt buộc cho các tổ chức đang tìm kiếm chứng nhận ISO/IEC 27001:2005. SOA là một văn bản trong đó trình bày các đối tượng kiểm soát và các kiểm soát đã được lựa chọn. Lựa chọn này phải liên kết tới kết quả của đánh giá rủi ro và quy trình khắc phục rủi ro. Điều liên kết này nên chứng minh những lý do cho sự lựa chọn đối tượng kiểm soát và các đối tượng.

Một danh sách các đối tượng kiểm soátvà các kiểm sóat không tạo thành một SOA hợp lệ. SOA phải nhận biết được các đối tượng kiểm soát và các kiểm soát sẵn sàng thực thi và phải chứng minh cho việc loại trừ bất kì một đối tượng kiểm soát nào hoặc các kiểm soát từ ISO/IEC 27001:2005, phụ lục A. Điều quan trọng đó là phải đánh giá rủi ro và tài liệu hỗ trợ khắc phục rủi ro liên kết với các kiểm soát được lựa chọn hoặc không được lựa chọn sau đó quay trở lại các rủi ro rồi đến các tài sản, xác định các yêu cầu và chính sách bảo mật.

3.4.2 Thực thi và điều hành ISMS

Tuyên bố "shall" định nghĩa trong ISO/IEC 27001:2005, cho pha Do được thiết kết để đảm bảo rằng tổ chức này có một bộ quy trình thích hợp ngay tại chỗ

để thực thi và điều hành ISMS, họ đã thiết lập trong pha Plan. Sự khác nhau của các bước trong pha Do là như sau:

a. Xây dựng kế hoạch xử lý rủi ro.

Kế hoạch này phải phác thảo những hành động nào cần được viện dẫn để quản lý các rủi ro được xác định, ưu tiên những hành động nào, hạn chế những yếu tố nào, thời hạn và nguồn lực cần thiết. Trách nhiệm của những người tham gia vào quá trình quản lý rủi ro an toàn thông tin phải được cấp phát rõ ràng cũng như trách nhiệm an toàn thông tin của người sử dụng và người quản lý trong ISMS. Các quy trình kinh doanh khác và lịch trình của chúng cần được phối hợp với các kế hoạch xử lý rủi ro.

b. Thực hiện kế hoạch khắc phục rủi ro.

Tổ chức phải có một tập các quy trình tại chỗ cho việc thực hiện kế hoạch khắc phục rủi ro và hệ thống kiểm soát đối tượng đã được lựa chọn, các kiểm soát, có tính tới kinh phí cho ISMS, phân bổ vai trò và trách nhiệm. Việc xác định hành động, vai trò và trách nhiệm tham gia trong quá trình này nên có trong tài liệu.

c. Thực hiện các kiểm sóat đã được lựa chọn

Để đáp ứng các mục tiêu kiểm soát, các tổ chức phải có những thủ tục tại chỗ để thực thi các kiểm sóat được lựa chọn phù hợp với các hành động, độ ưu tiên, nguồn lực, vài trò và trách nhiệm được đặt ra trong kế hoạch khắc phục rủi ro.

Mức độ (ví dụ: đào tạo, ghi lại hoặc báo cáo là bao nhiêu) của việc thực hiện nên được đánh giá tốt để tránh lãng phí tài nguyên. Nếu việc thực thi không được đánh giá tốt nó sẽ dẫn tới sự thất vọng của nhân viên bị ảnh hưởng bởi kiểm soát, nó thường dẫn tới việc giảm hiệu quả của việc kiểm soát. An toàn và kiểm soát sẽ luôn tác động tới cuộc sống và phương thức làm việc của con người nhưng nó không bao giờ trở thành một gánh nặng.

d. Xác định làm thế nào để đo lường và đánh giá hiệu quả kiểm soát.

Cùng với việc thực thi kiểm sóat được lựa chọn, có nghĩa là nó phải được đặt ở nơi cho phép đo lường và đánh giá một cách hiệu quả các kiểm soát. Các

kiểm sóat nên quản lý tốt các rủi ro thông tin mà chúng đã được chọn. Vì vậy tổ chức phải xác định họ muốn đảm bảo hiệu quả của kiểm soát và đảm bảo các kiểm soát đạt được mục tiêu đã đặt ra của họ như thế nào. Họ cũng có thể gộp lại các kiểm soát vào trong các nhóm và xác định đo lường được áp dụng vào nhóm kiểm soát đó - điều kiện là cách này phải đảm bảo đánh giá có hiệu quả và có ý nghĩa cho tất cả các kiểm soát trong nhóm.

Các biện pháp đo lường sử dụng để kiểm soát có hiệu quả phải được đưa ra để so sánh và tái sản xuất. Vấn đề này bao gồm một là xem xét hiệu quả chi phí của kiểm soát - điều này thường có nhiều mức độ thực thi cho một kiểm soát và lợi ích phải được so sánh với việc sử dụng an toàn được thêm vào trong thực tế. Đối với mục đích lấy chứng chỉ, thì phải xác định sự đo lường hiệu quả của kiểm soát dựa vào các tài liệu cung cấp bằng chứng về việc tổ chức đã đánh giá hiệu quả của kiểm soát như thế nào.

d. Thực hiện chương trình đào tạo và nhận thức.

Các tổ chức phải đưa ra một chương trình thích hợp để đào tạo và nâng cao nhận thức cho nhân viên đảm bảo rằng tất cả các nhân viên với những trách nhiệm được phân công ở ISMS đều có khả năng thực hiện nhiệm vụ của họ. Chương trình này phải xác định những năng lực cần thiết, cung cấp đào tạo để đáp ứng các yêu cầu, đánh giá hiệu quả việc đào tạo và duy trì các hồ sơ kĩ năng và bằng cấp đạt được.

Việc đào tạo nên cho phép họ làm công việc của họ với việc quản lý và kiểm soát bảo mật có hiệu quả. Nó cho phép họ chứng minh được tính trách nhiệm giải trình và thiết lập sự tin cậy mà không để lại dấu vết nghi ngờ, mặt khác còn nâng cao trình độ của họ. Từ đó nhân viên trong tổ chức sẽ sớm nhìn thấy được lợi ích của việc triển khai bảo mật thay vì sự bất tiện của nó.

f. Quản lý hoạt động của ISMS.

Tổ chức phải vận hành theo quy định của ISMS với các kiểm soát được xác định, chính sách và thủ tục. Các hoạt động hằng ngày của ISMS sẽ cung cấp thông tin cần thiết cho giai đoạn Check để đánh giá những chức năng an ninh được thiết

lập như mong đợi. Để cho phép sự đánh giá này, điều quan trọng là tất cả các tài liệu và bản ghi cần thiết phải được tập hợp trong suốt quá trình hoạt động của ISMS.

g. Quản lý tài nguyên cho ISMS.

Tổ chức phải xác định và cung cấp những tài nguyên cần thiết để điều hành, theo dõi, xem xét, duy trì và nâng cao ISMS.

h. Thực thi các thủ tục và kiểm soát để quản lý các sự cố.

Tổ chức phải thiết lập các thủ tục, các kiểm sóat để xác định, báo cáo các sự kiện an toàn thông tin, để đánh giá các sự kiện này và phản ứng với sự cố một cách hiệu quả, giới hạn thiệt hại của sự cố an toàn thông tin. Hồ sơ của tất cả các sự cố an toàn thông tin phải được làm và các tổ chức phải đưa thủ tục để đánh giá các sự cố này và học hỏi kinh nghiệm từ những sự cố đó. Các hồ sơ được sản xuất từ kế hoạch quản lý sự cố cung cấp một nguồn có giá trị để đưa ra kết quả đánh giá của việc đánh giá rủi ro và quyết định các cách khắc phục rủi ro có ý nghĩa trong thực tế, thực thi các kiểm soát theo đúng như dự định.

3.4.3 Theo dõi và xem xét ISMS

Tuyên bố "shall" định nghĩa trong ISO/IEC 27001:2005, cho giai đoạn Check được mô tả để đảm bảo rằng một tổ chức có những tập quy trình phù hợp tại chỗ để theo dõi và kiểm tra ISMS, những điều đã được thực hiện trong giai đoạn "Do". Chi tiết của giai đoạn Check bao gồm những công việc dưới đây:

a. Thực hiện các thủ tục xem xét và giám sát.

Các thủ tục và các kiểm sóat khác phải được phát hiện sai sót trong quá trình thực thi và điều hành ISMS, xác định sự thất bại và sự thành công của các vi phạm an ninh, phát hiện các sự kiện an toàn thông tin và giúp ngăn chặn những sự cố bảo mật thông tin và phải xác định xem những hành động thực tiễn nào có thể giải quyết các vi phạm hoặc phản ứng với những sự cố có hiệu quả. Thêm vào đó việc giám sát và xem lại các thủ tục phải cho phép ban quản lý phát hiện việc thực thi

các kiểm sóat có hiệu quả và trách nhiệm của người liên đới có được thự hiện một cách chính xác như dự tính trong kế hoạch khắc phục rủi ro.

Đối với mục đích chứng nhận, tổ chức cần phải có tài liệu làm bắng chứng về các hoạt dộng giám sát, đánh giá theo dõi các log, hồ sơ và các file, các hành động được thực hiện trong việc phản ứng với các kết quả của hành động giám sát.

b. Thường xuyên thực hiện đánh giá hiệu quả của ISMS.

Tổ chức phải đánh giá hiệu quả làm việc của ISMS. Điều này phải bao gồm xem xét chính sách bảo mật, các mục tiêu, đảm bảo rằng chúng được đáp ứng, tuân tủ các chính sách của kiểm soát bảo mật. Việc xem xét hoạt động phải được tính toán tới kết quả của việc bảo mật và kiểm toán để đảm bảo rằng tất cả các yếu tố này được xem xét khi xác định hiệu quả của ISMS. Bất cứ việc xác định không tuân thủ hoặc không đủ hiệu quả của ISMS nên dẫn ra những hành động khắc phục nhằm duy trì và cải thiện hoạt động của ISMS.

c. Đo lường hiệu quả các kiểm soát.

Các phương tiện đã được đưa ra để đánh giá hiệu quả thực hiện các kiểm soát phải được sử dụng để đo lường hiệu quả làm việc của các kiểm soát, và xem chúng có đạt được mục tiêu, đáp ứng được các yêu cầu đề ra như thế nào. Có rất nhiều biện pháp đo lường khác nhau được áp dụng và các biện pháp đo lường thích hợp có thể thay đổi đáng kể sự phụ thuộc vào sự xem xét các kiểm soát hoặc nhóm kiểm soát.

d. Xem xét kế hoạch đánh giá rủi ro theo chu kỳ.

Đối với các ISMS có hiệu quả trong quản lý rủi ro an toàn thông tin điều quan trọng là phải giám sát và theo dõi bất kỳ một thay đổi nào có thể ảnh hưởng tới ISMS. Việc xem xét này phải nhận biết những thay đổi từ các mối đe dọa, lỗ hổng hoặc sự thay đổi của các tác động trong:

- Môi trường kinh doanh, bối cảnh - đối tác kinh doanh mới, sự mới hoặc sự khác nhau trong dây chuyền cung cấp, sự mới, khác nhau hay sự thay đổi của các khách hàng về mặt cơ bản, mở rộng các thị trường khác nhau,

điều kiện của thị trường, sự sắp xếp bên thứ 3, gia công phần mềm, làm việc tại nhà…

- Chính sách hay mục tiêu của công ty - thay đổi chính sách hoặc mục tiêu của công ty có thể ảnh hưởng đến các quyết định khắc phục các rủi ro hoặc định giá tài sản
- Cấu trúc của tổ chức, nhân lực hoặc môi trường điều hành.
- Hiệu quả của việc thực thi các kiểm soát.
- Các mối đe dọa, các lỗ hoặc được xác định - Để được cập nhật những phát triển mới nhất trong công nghệ, thay đổi quy trình kinh doanh và sự cố đã, đang xảy ra.
- Việc sử dụng và triển khai công nghệ - các hệ thống mới và các ứng dụng mới, sự nâng cấp, mở rộng mạng lưới, sự đa dạng của các platform của hệ thống, nhân viên làm việc từ xa nhiều hơn, truy cập của bên thứ 3 nhiều hơn, có nhiều hơn các hợp đồng gia công phần mềm.
- Môi trường pháp lý và những quy định, sự thay đổi hoặc bổ sung các hợp đồng hoặc những biến đổi khác trong môi trường của tổ chức.

Những ví dụ về sự thay đổi có thể ảnh hưởng đến các rủi ro và tác động tới hoạt động kinh doanh của tổ chức. Đánh giá lại các rủi ro, mức độ của các rủi ro còn lại và mức độ chấp nhận rủi ro là cần thiết để đảm bảo ISMS vẫn hoạt động có hiệu quả. Một tổ chức có ý định đi chứng nhận có thể dùng tới tài liệu này bằng cách tạo bản cập nhật đánh giá rủi ro của họ và có thể so sánh với các kết quả đánh giá rủi ro khác, để nhận biết sự tiến bộ của họ theo thời gian.

e. Tiến hành kiểm toán nội bộ.

Tổ chức phải tiến hành một cuộc kiểm tóan nội bộ để đảm bảo rằng các mục tiêu kiểm soát, các kiểm soát, chính sách và thủ tục của ISMS phù hợp với các yêu cầu đặt ra. Các kiểm toán ISMS phải được hướng dẫn tại thời điểm giữa hai kế hoạch.

f. Tiến hành nghiên cứu quản lý ISMS.

Trong suốt giai đoạn kiểm tra, tổ chức phải thực hiện đánh giá việc quản lý và đánh giá lại việc quản lý ISMS: đó là những phạm vi còn giá trị, là hệ thống kiểm soát vẫn còn hiệu lực và hiệu quả, là những thủ tục vẫn có giá trị và đang được sử dụng đúng trong bối cảnh kinh doanh hiện tại, là những vai trò, trách nhiệm được giao, là những hoạt động an ninh vẫn được tiến hành như mong đợi, là quy trình xử lý sự cố an ninh vẫn còn thích hợp, có kết quả của quy trình xử lý sự cố an ninh được giải quyết đúng và các kế hoạch kinh doanh vẫn còn thích hợp? Quá trình này cũng sẽ phải được xác định sự cần thiết để cải tiến những điều được thực thi trong pha Act.

g. Cập nhật các kế hoạch bảo mật.

Các tổ chức phải có những thủ tục để sử dụng các kết quả giám sát, các hoạt động rà vi phạm và thực hiện các kế hoạch một cách có hiệu quả nhất.

h. Ghi lại các hành động và sự kiện.

Các kết quả của đánh giá quản lý, bảo mật và kiểm tóan ISMS nội bộ, kiểm tra hệ thống, các báo cáo về sự cố an ninh, kết quả của hoạt động giám sát, và những phản hồi, đề xuất từ chủ sở hữu hệ thống an toàn thông tin, người quản lý, người sử dụng nên được ghi lại để đảm bảo rằng tất cả những cải tiến cần thiết đều được xác định. Điều này cũng giúp xác dịnh được các phần làm việc hiệu quả của ISMS và nên được duy trì chính xác cách thức giữ cho ISMS hoạt động tốt.

3.4.4 Duy trì và cải tiến ISMS

Tuyên bố "shall" được định nghĩa trong chuẩn ISO/IEC 27001:2005 cho pha Act được miêu tả để đảm bảo rằng một tổ chức có những tập quy trình thích hợp để quản lý và cải hiện ISMS theo quy trình thực hiện trong pha Check. Việc duy trì và cải tiến ISMS bao gồm các bước dưới đây:

a. Thực thi xác định cải tiến.

Theo dõi và xem xét các quy trình trong pha Check có thể đã thay đổi nhận định rằng cần cải tiến ISMS để đảm bảo rằng các rủi ro an toàn thông tin được quản lý đúng cách. Tổ chức nên thực thi việc cải tiến này và cũng cần có những

hành động cần thiết khác để thực hiện những việc này, dựa trên các hồ sơ và phản hồi nhận từ pha Check. Thực hiện xác định việc cải tiến không thực sự khác nhau từ các hành động cần được đặt ra khi thực thi các kiểm soát với các thủ tục trong thời gian đầu . Điều quan trọng là phải tính đến các kiểm soát đó đã thực hiện và đảm bảo rằng những cải tiến được xác định làm việc tốt cùng với chúng

b. Đưa ra các hành động khắc phục và phòng ngừa thích hợp.

Tổ chức phải có một tập các quy trình để có thể tiếp tục cải tiến hiệu quả ISMS. Điều này sẽ liên quan đến việc sử dụng kết quả từ việc kiểm toán, xem xét, phân tích các hoạt động giám sát , các sự cố, các hành động khắc phục và ngăn ngừa phải được đưa ra để loại bỏ bất kì sự không phù hợp nào trong quá trình thực thi, điều hành ISMS và để ngăn ngừa sự tái phát của chúng. Tổ chức này cũng cần học các bài học từ các những việc đã xảy ra, họ cũng có thể sử dụng một số kinh nghiệm từ các tổ chức khác, phân tích các xu hướng hoặc các nguồn thông tin mà họ có quyền truy cập và muốn sử dụng chúng.

c. Truyền đạt những hành động và những cải tiến cho tất cả các bên quan tâm.

Một khía cạnh quan trọng là đảm bảo rằng tất cả các hành động, các phương pháp khắc phục và phòng ngừa được ghi lại mà các kênh truyền thông thích hợp được đặt ra để truyền đạt các kết quả của cái tiến ISMS cho những người thích hợp trong tổ chức và thực hiện những hành động thực sự như kết quả truyền đạt. Điều này không chỉ bao gồm những nhân viên trong tổ chức mà còn phải bao gồm người dùng của bên thứ 3, nhà thầu hoặc những bên khác có ảnh hưởng bởi sự cải tiến này và phải làm theo với những thay đổi ở chính sách, thủ tục và kiểm soát. Ngoài ra tất cả những thay đổi cần phải được thực hiện sau những cải tiến đã được truyền đạt, đảm bảo rằng tất cả mọi người đều nhận thức được những thay đổi này ảnh hưởng tới môi trường làm việc hàng ngày và chức năng làm việc của họ như thế nào.

d. Đảm bảo các cải tiến đạt được những mục tiêu trong dự định.

Các tổ chức phải đảm bảo rằng việc thực thi các cải tiến đáp ứng được yêu cầu mong muốn và đạt được những mục tiêu đã đề ra. Điều này bao gồm xem xét và khắc phục những hành động ngăn ngừa đã đặt ra. Các số liệu và các phương pháp đo lường đã được đưa ra để đo lường hiệu quả của các tiến trình ISMS và các kiểm sóat để có thể giúp xác định sự thành công của việc cải tiến, có thể sử dụng tài liệu để ghi lại các tiến độ mà tổ chức đang làm trong việc quản lý rủi ro của tổ chức theo thời gian.

3.4.5 Kết quả nhận được

Kết quả đạt được sau khi thực thi ISMS theo chuẩn ISO/IEC 27001:2005 là một văn bản trong đó là những danh sách các kiểm soát được lựa chọn thêm vào với các kiểm soát đang được thực thi ở thời điểm hiện tại hoặc không được thực thi (các kiểm soát ngoại lệ) với những bằng chứng/nguyên nhân chứng minh tại sao những kiểm soát ấy không được hoặc được thực hiện, văn bản đó được gọi là SOA (Statement of Applicability – Tuyên cáo được áp dụng). SOA bao gồm:

- Các đối tượng kiểm soát và các kiểm soát được lựa chọn, nguyên nhân cho sự lựa chọn đó.
- Tất cả các kiểm soát đang được thực thi tại thời điểm hiện tại
- Tất cả các đối tượng kiểm soát nào hoặc các kiểm soát nào bị loại trừ từ phụ lục A 27001 và nguyên nhân cho sự loại trừ đó

Dưới đây là danh sách các SOA cần được cho vào tài liệu, đây là một phần khuyến cáo được trích trong phụ lục A – ISO 27001

A.5 Chính sách bảo mật		
A.5.1 Chính sách bảo mật thông tin Đối tượng: Cung cấp hướng quản lý và hỗ trợ cho việc bảo mật thông tin thích hợp với các yêu cầu kinh doanh, quy phạm pháp luật và các quy định có liên quan		
A.5.1.1	Tài liệu chính sách an toàn thông tin	Kiểm sóat

		Một tài liệu chính sách an toàn thông tin phải được phê duyệt bởi quản lý và được công khai, truyền đạt tới tất cả các nhân viên, các bên có liên quan.
A.5.1.2	Xem xét chính sách an toàn thông tin	Kiểm soát Chính sách an toàn thôgn tin phải được xem xét đúng theo kỳ hạn của kế hoạch hoặc nếu có một sự thay đổi đáng kể xảy ra thì phải đảm bảo nó luôn thích hợp, thỏa đáng và hiệu quả
A.6 Tổ chức an toàn thông tin		
A.6.1 Trong tổ chức Mục tiêu: Quản lý an toàn thông tin trong tổ chức		
A.6.1.1	Quản lý cam kết bảo mật thông tin	Quản lý phải tích cực hỗ trợ bảo mật trong tổ chức thôgn qua các định hướng rõ ràng, thể hiện sự cam kết, phân công công việc rõ ràng, phân công trách nhiệm bảo mật thông tin.
A.6.1.2	Kết hợp bảo mật thông tin	Kiểm soát: Những hành động bảo mật thông tin phải được kết hợp bởi đại diện từ các bộ phận khác nhau của tổ chức với các nhiệm vụ và chức năng công việc liên quan.

A.6.1.3	Phân công trách nhiệm an toàn thông tin	Kiểm soát: Tất cả những trách nhiệm an toàn thông tin sẽ phải được định nghĩa rõ ràng.
A.6.1.4	Quá trình ủy quyền cho các điều kiện dễ dàng xử lý thông tin	Kiểm soát: Quá trình ủy quyền quản lý cho các điều kiện dễ dàng xử lý thông tin phải được định nghĩa và thực hiện
A.6.1.5	Bảo mật một cách phù hợp	Kiểm sóat: Các yêu cầu cho sự bí mật hoặc các giao kèo không được tiết lộ phản ánh sự cần thiết của tổ chức về việc bảo vệ thông tin phải được xác định và thường xuyên xem xét lại.
A.6.1.6	Liên lạc với người có thẩm quyền	Việc Dành riêng liên hệ với những người có thẩm quyền thích hợp phải được duy trì
A.6.1.7	Liên lạc với những nhóm quan tâm đặc biệt	Kiểm sóat: Việc dành riêng liên hệ với những nhóm quan tâm đặc biệt hoặc những danh sách đặc biệt các diễn đàn bảo mật và kết hợp với các chuyên gia phải được duy trì.
A.6.1.8	Độc lập xem xét việc bảo mật thông tin.	Các phương pháp tiếp cận của tổ chức để quản lý an toàn thông tin

		và sự thực thi nó (ví dụ: đối tượng kiểm sóat, các kiểm soát, các chính sách, các thủ tục, các quá trình cho bảo mật an toàn thông tin) phải được xem xét một cách độc lập theo các kế hoạch định kì học khi có những thay đổi đáng kể tới việc thực thi bảo mật xảy ra.
A.6.2 Bên ngoài tổ chức Mục tiêu: Duy trì bảo mật thông tin của tổ chức và những điều kiện dễ dàng xử lý thông tin cái mà được truy cập, xử lý, truyền tải tới hoặc quản lý bởi các thành phần bên ngoài.		
A.6.2.1	Xác định các rủi ro có liên quan tới các thành phần bên ngoài	Các rủi ro đến thông tin của tổ chức và các điều kiện dễ dàng xử lý thông tin từ quá trình kinh doanh bao gồm các thành phần bên ngòai phải được xác định và dành riêng các kiểm sóat được thực thi trước khi cấp quyền truy cập
A.6.2.2	Giải quyết vấn đề bảo mật khi giao dịch với khách hàng	Xác định tất cả các yêu cầu bảo mật phải được giải quyết trước khi cho phép khách hàng truy cập vào thông tin hoặc tài sản của tổ chức.
A.6.2.3	Giải quyết vấn đề bảo mật trong việc thỏa thuận với bên thứ 3	Việc thỏa thuận với bên thứ 3 bao gồm truy cập, xử lý, truyền đạt hoặc quản lý thông tin hay các điều kiện dễ dàng xử lý thông tin của tổ chức hay các sản phẩm

		thêm vào hoặc các dịch vụ để điều kiện dễ dàng xử lý thông tin phải bao gồm tất cả các yêu cầu bảo mật thích đáng.
A.7 Quản lý tài sản		
A.7.1 Tính chịu trách nhiệm với tài sản Mục tiêu: Đạt tới và duy trì thích hợp việc bảo vệ tài sản của tổ chức		
A.7.1.1	Kiểm kê tài sản	Kiểm soát: Tất cả các tài sản phải được xác định và được kiểm kê các bảo thảo về tầm quan trọng của tất cả các tài sản và duy trì chúng.
A.7.1.2	Chủ sở hữu tài sản	Kiểm soát: Tất cả thông tin và các tài sản kết hợp với các điều kiện xử lý thông tin phải được là chủ bởi phần chỉ định của tổ chức.
A.7.1.3	Chấp nhận sử dụng tài sản	Kiểm soát: Nội quy cho việc chấp nhận sử dụng thông tin và tài sản gắn liền với các điều kiện xử lý thông tin phải được xác đinh, viết tài liệu và thực thi.
A.7.2. Phân loại thông tin Mục tiêu: Đảm bảo rằng thông tin nhận được một mức độ bảo vệ thích hợp.		
A.7.2.1	Hướng dẫn phân loại	Kiểm sóat: Thông tin phải được phân loại cho

		đúng với giá trị của nó, các yêu cầu pháp lý, độ nhạy cảm, giới hạn tới tổ chức
A.7.2.2	Dán nhãn thông tin và điều khiển thông tin	Kiểm soát: Một tập các thủ tục thích hợp cho nhãn thông tin và điều khiển thông tin phải được phát triển và thực thi trong sự phù hợp với cấu trúc phân loại được thông qua bởi tổ chức.
A.8 Nguồn nhân lực bảo mật		
A.8.1 Trước khi làm việc Mục tiêu: Đảm bảo rằng nhân viên, nhà thầu và người sử dụng bên thứ 3 hiểu rõ trách nhiệm của họ và thích hợp cho những nhiệm vụ mà họ được xem là giảm thiểu nguy cơ gian gian lận, trộm cắp hoặc sử dụng sai các điều kiện.		
A.8.1.1	Các chức năng và tính chịu trách nhiệm	Kiểm soát: Chức năng bảo mật và tính chịu trách nhiệm của nhân viên, nhà thầu và người sử dụng bên thứ 3 phải được xác định và được viết thành văn bản phù hợp với chính sách bảo mật an toàn thông tin của tổ chức.
A.8.1.2	Thông báo	Nền xác minh kiểm tra tất cả các ứng cử viên cho nhân viên, nhà thầu, và người sử dụng bên thứ 3 phải thực hiện phù hợp với các quy phạm pháp luật thích hợp, các quy định và đạo đức, tỉ lệ

		thuận với các yêu cầu kinh doanh, sự phân loại thông tin để truy cập và nhận biết các rủi ro.
A.8.1.3	Các điều khoản và điều kiện làm việc	Kiểm soát Như là một phần của nghĩa vụ hợp đồng, các nhân viên, các nhà thầu và bên thứ ba sử dụng của họ phải đồng ý và kí các điều khoản, điều kiện của hợp đồng lao động và tính chịu trách nhiệm của tổ chức cho việc bảo mật thông tin.
A.8.2 Suốt quá trình làm việc Mục tiêu: Đảm bảo rằng tất cả nhân viên, nhà thầu và người sử dụng bên thứ 3 đều được nhận thức về các mối đe dọa an toàn thông tin và các mối quan tâm, trách nhiệm và nghĩa vụ pháp lý của họ và được trang bị để hỗ trợ các chính sách bảo mật của tổ chức trong quá trình làm việc thông thường và để giảm thiểu rủi ro do lỗi của con người mang lại.		
A.8.2.1	Quản lý tính chịu trách nhiệm	Kiểm soát: Quản lý phải yêu cầu nhân viên, nhà thầu và người sử dụng bên thứ 3 đồng ý việc bảo mật phù hợp với việc thiết lập chính sách và các thủ tục của tổ chức.
A.8.2.2	Nhận tức an toàn thông tin, giáo dụ và đào tạo	Kiểm soát: Tất cả nhân viên của tổ chức và những nơi có liên quan, các nhà thầu và người sử dụng bên thứ 3 phải nhận được việc đào tạo nhận

		thức một cách thích hợp và thường xuyên cập nhật về chính sách của tổ chức, các thủ tục như là liên quan tới chức năng công việc của họ
A.8.2.3	Quy trình xử lý kỷ luật	Kiểm soát: Phải có một form quy trình xử lý kỉ luật những nhân viên đã cam kết vi phạm bảo mật.
A.8.3 Chấm dứt hoặc thay đổi công việc Mục tiêu: Đảm bảo rằng các nhân viên, nhà thầu và người sử dụng bên thứ 3 đi khỏi một tổ chức hoặc thay đổi công việc phải có trật tự.		
A.8.3.1	Chấm dứt trách nhiệm	Kiểm sóat: Trách nhiệm thực hiện công việc chấm dứt hoặc thay đổi công việc phải được xác định và phân công một cách rõ ràng.
A.8.3.2	Trả lại tài sản	Tất cả nhân viên, nhà thầu, người sử dụng bên thứ 3 phải trả lại tất cả tài sản của tổ chức mà họ đang nắm giữ khi chấm hứt việc làm, hợp đồng hoặc các thỏa thuận của họ.
A.8.3.3	Loại bỏ các quyền truy cập	Kiểm soát: Tất cả các quyền truy cập của tất cả nhân viên, nhà thầu và người sử dụng bên thứ 3 tới thông tin và những điều kiện xử lý thông tin

		phải được xóa bỏ khi chấm dứt hợp đồng, công việc, thỏa thuận hay những điều chỉnh khi thay đổi.
A.9 Vật lý và môi trường bảo mật Mục tiêu: Ngăn ngừa truy cập vật lý trái phép, phá hoại, can thiệp tới tài sản và thông tin của tổ chức		
A.9.1.1	Bảo mật mức vật lý	Chu vi bảo mật (các rào cản như tường, thẻ kiểm sóat đăng nhập hoặc lễ tân) được sử dụng để bảo vệ các khu vực có chứa thông tin và các cơ sở xử lý thông tin
A.9.1.2	Kiểm soát các mục vật lý	Kiểm sóat: Các miền bảo mật phải được bảo vệ bởi những mục kiểm soát thích hợp để đảm bảo rằng chỉ có những người có quyền mới được phép truy cập
A.9.1.2	Bảo vệ văn phòng, các phòng và các cơ sở.	Kiểm soát: Bảo vệ vật lý cho văn phòng, các phòng và các cơ sở phải được thiết kế và được áp dụng.
A.9.1.4	Bảo vệ chống lại những đe dọa từ bên ngoài và từ trong môi trường	Kiểm soát Bảo vệ vật lý chống lại các thiệt hại từ cháy, lũ lụt, động đất, nổ, tình trạng bất ổn dân sự và các hình thức tự nhiên khác hoặc từ nhân tạo đều phải được thiết kế

		và được áp dụng
A.9.1.5	Làm việc trong miền bảo mật	Kiểm soát: Bảo vệ vật lý và hướng dẫn những việc làm trong các miền bảo mật phải được thiết kế và áp dụng.
A.9.1.6	Truy cập công cộng, các miền phân phối và loading	Các điểm truy cập ví dụ như các miền phân phối, loading và các điểm khác nơi những người truy cập trái phép có thể xâm nhập được vào tài sản sẽ phải được kiểm sóat và nếu có thể thì phải cô lập từ những cơ sở xử lý thông tin để tránh truy cập trái phép.
A.9.2 Thiết bị bảo mật Mục tiêu: Để tránh việc mất mát, hư hỏng, trộm cắp hoặc việc làm hại tới tài sản và làm gián đoạn các hoạt động của tổ chức		
A.9.2.1	Đặt thiết bị và bảo vệ thiết bị	Kiểm soát Thiết bị phải được đặt hoặc được bảo vệ để giảm thiểu rủi ro từ các đe dọa môi trường, các mối nguy hiểm và các cơ hội truy cập trái phép
A.9.2.2	Hỗ trợ các tiện ích	Kiểm soát Thiết bị phải được bảo vệ việc bị mất điện và các gián đoạn khác bởi những thất bại trong việc hỗ trợ các tiện ích

A.9.2.3	Cáp an ninh	Kiểm soát Năng lượng và việc cáp truyền mang dữ liệu hoặc hỗ trợ các dịch vụ thông tin phải được bảo vệ từ việc ngăn chặn hoặc các thiệt hại
A.9.2.4	Bảo trì thiết bị	Kiểm soát Các thiết bị phải được duy trì đúng cách để đảm mbảo rằng nó được liên tục sẵn sàng và toàn vẹn
A.9.2.5	Bảo mật các thiết bị hết hạn dùng	Kiểm soát Bảo mật phải được áp dụng tới các thiết bị chi nhánh ở xa có tính đến các rủi ro khác nhau làm việc bên ngoài phạm vi của tổ chức
A.9.2.6	Bảo mật việc xử lý hoặc tái sử dụng thiết bị	Tất cả các mục của thiết bị bao gồm tất cả các phương tiện lưu trữ phải được kiểm tra để đảm bảo rằng bất kì một dữ liệu nhảy cảm và những phần mềm được cấp phép đã được gỡ bỏ hoặc ghi đè an toàn trước khi xử lý.
A.9.2.7	Xóa bỏ quyền sở hữu tài sản	Kiểm soát Thiết bị, thông tin và phần mềm không được thực hiện ở các chi nhánh mà mà thiếu sự cấp phép
A.10 Truyền thông và các hoạt động quản lý		
A.10.1 Các thủ tục hoạt động và tính chịu trách nhiệm		

Mục tiêu: đảm bảo việc điều hành đúng và bảo mật cơ sở xử lý thông tin		
A.10.1.1	Tài liệu thủ tục hoạt động	Kiểm soát Thủ tục hoạt động phải được viết thành tài liệu, phải được duy trì và luôn sẵn sàng cho tất cả những người sử dụng người mà cần chúng
A.10.1.2	Thay đổi việc quản lý	Kiểm soát Thay đổi cơ sở xử lý thông tin và hệ thống phải được kiểm soát
A.10.1.3	Phân biệt các chức vụ	Kiểm soát Các chức vụ và các miền có tính chịu trách nhiệm phải được phân chia để giảm thiểu khả năng chỉnh sửa trái phép hoặc không chủ ý hoặc lạm dụng tài sản của tổ chức
A.10.1.4	Phân chia sự phát triển, kiểm tra và cơ sở hoạt động.	Phát triển, thử nghiệm và các cơ sở hoạt động phải được phân chia để giảm thiểu rủi ro của việc truy cập trái phép hoặc thay đổi hoạt động của hệ thống.
A.10.2 Dịch vụ bên thứ 3 phân phối quản lý Mục tiêu: Thực thi và duy trì một cách hợp lý mức độ bảo mật thông tin và dịch vụ phân phối với các dịch vụ phù hợp với thỏa thuận của bên cung cấp dịch vụ thứ 3.		
A.10.2.1	Cung cấp dịch vụ	Kiểm soát

		Điều này phải đảm bảo rằng việc các kiểm soát bảo mật, việc xác định dịch vụ và mức độ cung cấp bao gồm trong các thỏa thuận của bên cung cấp dịch vụ thứ 3 được thực hiện, điều hành và duy trì bởi bên thứ 3
A.10.2.2	Theo dõi và xem xét các dịch vụ của bên thứ 3	Kiểm soát Các dịch vụ, các báo cáo và các hồ sơ được cung cấp bởi bên thứ 3 phải được thường xuyên theo dõi và xem xét lại, kiểm toán phải được thực hiện một cách thường xuyên.
A.10.2.3	Quản lý việc các thay đổi với bên thứ 3	Kiểm soát Các thay đổi để cung cấp dịch vụ bao gồm việc duy trì và cải tiến các chính sách an toàn thông tin đang tồn tại, các thủ tục và các kiểm soát phải được quản lý, có tính đến giới hạn của hệ thống kinh doanh và các quy trình tham gia, đánh giá lại các rủi ro.
A.10.3 Quy hoạch hệ thống và sự chấp nhận Mục tiêu: Nhằm giảm thiểu rủi ro do lỗi của hệ thống		
A.10.3.1	Năng lực quản lý	Kiểm soát Việc sử dụng tài nguyên phải được

		theo dõi, điều chỉnh và dự đoán về các yêu cầu trong tương lai để đảm bảo yêu cầu về hiệu suất của hệ thống
A.10.3.2	Chấp nhận hệ thống	Kiểm soát Các tiêu chí chấp nhận cho hệ thống thông tin mới, nâng cấp và đưa ra version mới phải được thiết lập, thử nghiệm cho phù hợp với hệ thống thực hiện trong thời gian phát triển và trước khi được chấp nhận.
A.10.4 Chống lại các mã độc hại và các mã tự động Mục tiêu: Bảo vệ tính toàn vẹn của phần mềm và thông tin		
A.10.4.1	Kiểm soát chống lại các mã độc hại	Kiểm soát Dò tìm, ngăn chặn và khôi phục các kiểm soát để bảo vệ chống lại các mã độc hại và kết hợp với người sử dụng hiểu biết được các quá trình phải được thực hiện.
A.10.4.2	Các kiểm soát chống lại mã tự động	Kiểm soát Nơi mà sử dụng các mã tự động để xác thực, các cài đặt phải đảm bảo rằng việc xác thực mã tự động hoạt động theo một chính sách bảo mật được xác định rõ ràng và mã tự động trái phép thì phải được ngặn chặn từ lúc thực thi.

A.10.5 Back up Mục tiêu: Duy trì tính toàn vẹn và tính sẵn sàng của thông tin và quá trình xử lý thông tin		
A.10.5.1	Sao lưu thông tin	Kiểm soát Sao lưu thông tin và các phần mềm phải được đưa ra và kiểm tra một cách thường xuyên phù hợp với các chính sách sao lưu.
A.10.6 Quản lý bảo mật mạng Mục tiêu: Để đảm bảo bảo vệ thông tin trong mạng và đảm bảo hỗ trợ cơ sở hạ tầng.		
A.10.6.1	Kiểm soát mạng	Kiểm soát Các mạng phải được quản lý và kiểm soát đầy đủ để bảo vệ những mối đe dọa để duy trì bảo mật cho hệ thống và các ứng dụng sử dụng trong mạng bao gồm các thông tin trong quá trình truyền.
A.10.6.2	Bảo mật dịch vụ mạng	Kiểm soát Đặc điểm bảo mật, mức độ bảo mật và yêu cầu qnản lý của tất cả các dịch vụ mạng phải được định nghĩa và bao gồm trong bất kì dịch vụ mạng nào, cho dù các dịch vụ này được cung cấp trong tổ chức hay thuê của tổ chức bên ngoài.
A.10.7 Kiểm soát các phương tiện		

Mục đích: Ngăn ngừa tiết lộ trái phép, sửa đổi, loại bỏ hoặc tiêu hủy tài sản và làm gián đoạn hoạt động kinh doanh		
A.10.7.1	Quản lý các phương tiện di động	Kiểm soát Phải có các quy trình tại chỗ để quản lý các phương tiện di động
A.10.7.2	Sắp đặt các phương tiện	Kiểm soát Các phương tiện phải được kiểm soát bảo mật và an toàn tới khi không còn yêu cầu nào, sử dụng các thủ tục một cách chính thức.
A.10.7.3	Thủ tục điều khiển thông tin	Kiểm soát Các thủ tục cho việc điều khiển và lưu trữ thông tin phải được thiết lập để bảo vệ thông tin từ việc tiết lộ trái phép hoặc sử dụng sai
A.10.7.4	Bảo mật hệ thống tài liệu	Kiểm soát Hệ thống tài liệu phải được bảo vệ chống lại các truy cập trái phép
A.10.8 Trao đổi thông tin Mục đích: Để duy trì bảo mật thông tin và trao đổi phần mềm trong tổ chức và với các thực thể bên ngoài		
A.10.8.1	Chính sách trao đổi thông tin và thủ tục	Kiểm soát Chính thức trao đổi các chính sách, các thủ tục và điều khiển phải có tại chỗ để bảo vệ sự trao đổi thông tin thông qua việc sử dụng tất cả các kiểu của các loại

		phương tiện truyền thông.
A.10.8.2	Trao đổi phù hợp	Kiểm soát Sự phù hợp ohải được thiết lập cho sự trao đổi thông tin và phần mềm giữa tổ chức và đối tác bên ngoài
A.10.8.3	Phương tiện vật lý trong khi truyền	Kiểm soát Các phương tiện bao gồm thông tin phải được bảo vệ chống lại truy cập trái phép, sử dụng sai hoặc tham nhũng trong suốt quá trình truyền qua giới hạn vật lý của tổ chức.
A.10.8.4	Thư điện tử	Kiểm soát Thông tin liênq uan đến tin nhắn điện tử phải được bảo vệ một cách thích hợp.
A.10.8.5	Hệ thống thông tin doanh nghiệp	Kiểm soát Các chính sách và thủ tục được phát triển và thực thi bảo vệ thông tin kết hợp với việc kết nối các doanh nghiệp an toàn thông tin
A.10.9 Dịch vụ thương mại điện tử Mục tiêu: Để đảm bảo rằng dịch vụ bảo mật điện tử và cách sử dụng bảo mật của chúng		
A.10.9.1	Bảo mật điện tử	Kiểm soát Thong tin liên quan đến thương

		mại điện tử thong qua mạng công cộng phải được bảo vệ từ hoạt động gian lận, việc tranh chấp hợp đồng, và không được phép tiết lộ hay sửa đổi
A.10.9.2	Giao dịch trực tuyến	Kiểm soát Thông tin liên quan đến việc giao dịch trực tuyến phải được bảo vệ để ngăn ngừa việc truyền không thành công, lỗi trong việc định tuyến, thay đổi thông tin trái phép, không được phép tiết lộ, sao chép thông tin trái phép hoặc phát lại.
A.10.9.3	Công bố công khai thông tin	Kiểm soát Tính toàn vẹn của thông tin phải luôn được sẵn sàng trên hệ thống và phải được bảo vệ để ngăn ngừa sự chỉnh sửa trái phép.
A.10.10 Theo dõi Mục tiêu: Để phát hiện các hoạt động xử lý thông tin trái phép		
A.10.10.1	Kiểm toán logging	Kiểm soát Nhật ký kiểm toán ghi lại hoạt động của người dung, các trường hợp ngoại lệ và các sự kiện bảo mật thông tin phải được đưa ra và lưu giữ trong một thời gian phục vụ cho quá trình kiểm tra trong tương lai và việc kiểm soát truy

		cập
A.10.10.2	Theo dõi hệ thống sử dụng	Kiểm soát Thủ tục cho việc giám sát sử dụng các quá trình xử lý thông tin phải được thiết lập và các kết quả của hoạt động giám sát phải được xem xét thường xuyên
A.10.10.3	Bảo vệ thông tin của nhật ký	Kiểm soát Các cơ sở xử lý và nhật ký thông tin phải được bảo vệ chống lại việc giả mạo và truy cập trái phép
A.10.10.4	Quản trị và điều hành nhật ký	Kiểm soát Quản trị hệ thống và các hành động điều hành hệ thống phải được ghi nhật kí
A.10.10.5	Lỗi đăng nhập	Kiểm soát Lỗi này phải được ghi log, được phân tích và đưa ra những hành động khắc phục phù hợp
A.10.10.6	Đồng bộ thời gian	Kiểm soát Thời gian của tất cả các hệ thống xử lý thông tin có liên quan trong tổ chức hoặc miền bảo mật phải được đồng bộ với một nguồn thời gian chính xác
A.11 Kiểm soát truy cập		
A.11.1 Yêu cầu của tổ chức cho việc kiểm soát truy cập		

A.11.1.1	Chính sách kiểm sóat truy cập	Kiểm soát Một chính sách kiểm soát truy cập phải được thiết lập, lập thành tài liệu và xem xét dựa trên tình hình kinh doanh và yêu cầu bảo mật của việc truy cập
A.11.2 Quản lý truy cập người dùng Mục tiêu: Đảm bảo rằng người được phép truy cập và ngăn ngừa truy cập trái phép đến hệ thống thông tin		
A.11.2.1	Người sử dụng đăng kí	Kiểm soát Điều này phải có một form chính để ngươi sử dụng đăng kí và đăng kí lại thủ tục về việc cấp và thu hồi quyền truy cập tới tất cả hệ thống thông tin, dịch vụ.
A.11.2.2	Quản lý quyền	Kiểm soát Vị trí và quyền sử dụng phải được giới hạn và kiểm soát.
A.11.2.3	Quản lý việc sử dụng password	Kiểm soát Việc phân bổ mật khẩu phải được kiểm sóat thông qua một quy trình quản lý chính thức
A.11.2.4	Theo dõi việc người dùng truy cập	Kiểm soát Quản lý phải theo dõi sự truy cập của người dùng một cách thường xuyên theo một quy trình quản lý chính thức

Ví dụ về SOA:

	Đối tượng kiểm soát và kiểm soát	Y/P/N/NA	Bình luận và các lý do
Chính sách bảo mật thông tin			
A.5.1	Để cung cấp hướng quản lý và hỗ trợ bảo mật thông tin…	Yes	Điều này cần thiết trong mọi lúc cho toàn bộ ISMS.
A.5.1.1	Tài liệu chính sách bảo mật thông tin	Yes	Chính sách này cần thiết để hoàn thành lại tất cả các điều đã thực thi như trong ISO/IEC 17799 5.1.1
A.5.1.2	Xem lại chính sách an toàn thông tin	Yes	Chính sách này sẽ được xem lại một cách phù hợp với các thủ tục xem lại của nhà cung cấp dịch vụ
Nội bộ tổ chức			
A.6.1	Để quản lý an toàn thông tin trong tổ chức	Yes	Điều này cần có tại chỗ cho toàn bộ ISMS
A.6.1.1	……..	…….	……