**TRƯỜNG ĐẠI HỌC MỞ HÀ NỘI**

**KHOA CÔNG NGHỆ THÔNG TIN**

**---------------------------------**

****

**BÁO CÁO NHÓM 1**

**MÔN HỌC: ĐẢM BẢO CHẤT LƯỢNG PHẦN MỀM**

**ĐỀ TÀI: TÌM HIỂU VỀ ISO 27000**

**Giảng viên hướng dẫn: Trần Thị Hồng Oanh**

**Sinh viên thực hiện: Đinh Tuấn Anh – 18A01**

**Đinh Văn Chương – 18A03**

**Nguyễn Văn Đoàn – 18A03**

**Nguyễn Hữu Hậu – 15A02**

**Phạm Thị Khánh Huyền – 18A02**

**Lưu Văn Nam – 18A01**

**Đỗ Thế Tài – 18A02**

**Nguyễn Minh Tuân – 18A02**

**Hà Nội – 2021**

**Mục Lục**

[**I. Giới thiệu chung 2**](#_Toc82861386)

[**II. Tổng quan về an toàn thông tin hiện nay 2**](#_Toc82861387)

[**1. Các khái niệm cơ bản của an toàn thông tin 3**](#_Toc82861388)

[**2. Các lý do gây ra rò rỉ và ảnh hưởng đến thông tin 5**](#_Toc82861389)

[**2.2. Lỗi và sự bỏ sót, cố tình bỏ qua: 5**](#_Toc82861390)

[**2.3. Lừa đảo và lấy cắp thông tin 6**](#_Toc82861391)

[**2.4. Hacker (Tin tặc) 6**](#_Toc82861392)

[**2.5. Lây lan mã độc 7**](#_Toc82861393)

[**2.6. Tấn công từ chối dịch vụ 8**](#_Toc82861394)

[**2.7. Tấn công Social engineering 8**](#_Toc82861395)

[**III. Giới thiệu về ISO 9**](#_Toc82861396)

[**IV. Giới thiệu về ISO 27000 10**](#_Toc82861397)

[**1. Giới thiệu chung về ISO 27000 10**](#_Toc82861398)

[**2. Lịch sử hình thành của ISO 27000 11**](#_Toc82861399)

[**3. Lợi ích khi sử dụng ISO 27000 11**](#_Toc82861400)

[**4. Đối tượng áp dụng 12**](#_Toc82861401)

[**V. Tìm hiểu chi tiết về ISO 27001:2013 12**](#_Toc82861402)

[**1. Doanh nghiệp cần làm gì để xây dựng và áp dụng ISO 27001:2013 13**](#_Toc82861403)

[**2. Công ty tư vấn làm gì để giúp Doanh nghiệp áp dụng ISO 27001? 13**](#_Toc82861404)

[**3. Các yêu cầu của tiêu chuẩn quốc tế ISO 27001:2013 14**](#_Toc82861405)

[**4. Quy trình áp dụng ISO 27001:2013 vào doanh nghiệp 15**](#_Toc82861406)

[**5. Quy trình đánh giá và cấp chứng chỉ ISO 27001 16**](#_Toc82861407)

[**6. Lợi ích của việc áp dụng và chứng nhận ISO 27001:2013 18**](#_Toc82861408)

[**VI. ISMS (Information Security Management System) 19**](#_Toc82861409)

[**1. Giới thiệu về ISMS 19**](#_Toc82861410)

[**2. Các lĩnh vực ISMS quản lý 19**](#_Toc82861411)

[**3. Tầm quan trọng và lợi ích của việc triển khai ISMS 19**](#_Toc82861412)

[**4. Xây dựng hệ thống ISMS đạt chứng chỉ ISO 27001 20**](#_Toc82861413)

[**4.1 Liệt kê tài sản 20**](#_Toc82861414)

[**4.2 Định giá tài sản 22**](#_Toc82861415)

[**4.3 Xác định hiểm nguy 22**](#_Toc82861416)

[**4.4 Tính toán các nguy cơ 23**](#_Toc82861417)

[**4.5 Tính toán các thiệt hại 24**](#_Toc82861418)

[**4.6 Các giải pháp làm giảm thiểu thiệt hại 25**](#_Toc82861419)

[**4.7 Đánh giá chi phí cho giải pháp và đưa ra quyết định 26**](#_Toc82861420)

# Giới thiệu chung

* 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, số hóa giao dịch. Điều này mang đến nhiều lợi ích về kinh tế nhưng vì quá phụ thuộc về các hệ thống mạng máy tính cũng mang đến nhiều vấn đề nghiêm trọng thậm chí có thể là tê liệt hoàn toàn hoạt động của các đơn vị đó khi các hệ thống này gặp sự cố như rò rỉ thông tin, các cuộc tấn công mạng, xâm nhập hệ thống từ các hacker…
* Khi mà các tổ chức hacker ngày càng nhiều, các cuộc tấn công mạng ngày càng có quy mô lớn hơn, có tính tổ chức hơn và gây thiệt hại ngày càng lớn thì các doanh nghiệp trên toàn cầu đang hướng dần đến 1 giải pháp giúp họ có thể phòng ngừa các vấn đề trên và giúp họ có thể có được 1 hệ thống thông tin có tính bảo mật, tin cậy và toàn vẹn thông tin để mang đến lợi nhuận cao về kinh tế cũng như uy tín của doanh nghiệp đối với đối tác,…
* Đáp ứng nhu cầu đó, bộ tiêu chuẩn ISO 27000 được ra đời mang đến giải pháp bảo mật thông tin được sử dụng trên toàn thế giới.

# Tổng quan về an toàn thông tin hiện nay

* Để có thể tìm hiểu bộ tiêu chuẩn ISO 27000 một cách tốt nhất thì chúng ta cần tìm hiểu tổng quan về các khái niệm và tình hình của an ninh thông tin hiện nay.
* Từ chính phủ, quân đội, các tập đoàn, bệnh viện, cơ sở kinh doanh… đến người dùng đều có những thông tin bí mật riêng về khách hàng, nhân viên, sản phẩm, nghiên cứu… Hầu hết các thông tin đó hiện nay đều được thu thập, xử lý và lưu trữ bởi máy tính, trung tâm dữ liệu. Dữ liệu đó cũng có thể được chuyển qua mạng để về trung tâm lưu trữ, đến các nhánh công ty con, hoặc gửi cho bạn bè, người thân… Nếu thông tin đó lọt vào tay đối thủ cạnh tranh thì cực kỳ nguy hiểm.
* Vì thế, bảo vệ thông tin trở thành một yêu cầu không thể thiếu trong mọi hoạt động nói chung và hoạt động điện tử nói riêng. An toàn thông tin trong thời đại số là quan trọng hơn bao giờ hết.

## **Các khái niệm cơ bản của an toàn thông tin**

* Khi nhắc đến khái niệm của anh toàn thông tin, người ta thường nhắc tới tam giác CIA (Confidentiality: Tính bảo mật, Integrity: Tính toàn vẹn, Availability: Tính sẵn sàng) vì nó được coi là khái niệm cơ bản, cốt lõi của an toàn thông tin.
* Từng khía cạnh của tam giác CIA và một số tính chất khác trong an toàn thông tin mạng:
  + ***Tính bảo mật:*** Bảo mật là thuật ngữ được sử dụng để tránh lộ thông tin đến những đối tượng không được xác thực hoặc để lọt vào các hệ thống khác. Ví dụ: một giao dịch tín dụng qua Internet, số thẻ tín dụng được gửi từ người mua hàng đến người bán, và từ người bán đến nhà cung cấp dịch vụ thẻ tín dụng. Hệ thống sẽ cố gắng thực hiện tính bảo mật bằng cách mã hóa số thẻ trong suốt quá trình truyền tin, giới hạn nơi nó có thể xuất hiện (cơ sở dữ liệu, log file, sao lưu (backup), in hóa đơn…) và bằng việc giới hạn truy cập những nơi mà nó được lưu lại. Nếu một bên không được xác thực (ví dụ người dùng không có trong giao dịch, hacker…) lấy số thẻ này bằng bất kỳ cách nào, thì tính bảo mật không còn nữa.

Tính bảo mật rất cần thiết (nhưng chưa đủ) để đảm bảo sự riêng tư của người có thông tin được hệ thống lưu giữ.

* + ***Tính toàn vẹn:*** Trong an toàn thông tin, toàn vẹn có nghĩa rằng dữ liệu không thể bị chỉnh sửa mà không bị phát hiện. Nó khác với tính toàn vẹn trong tham chiếu của cơ sở dữ liệu, mặc dù nó có thể được xem như là một trường hợp đặc biệt của tính nhất quán như được hiểu trong hô hình cổ điển ACID (tính nguyên tử (Atomicity), tính nhất quán (Consistency), tính tính cách ly (Isolation), tính lâu bền (Durability) – là một tập các thuộc tính đảm bảo rằng cơ sở dữ liệu đáng tin cậy) của xử lý giao dịch. Tính toàn vẹn bị xâm phạm khi một thông điệp bị chỉnh sửa trong giao dịch. Hệ thống thông tin an toàn luôn cung cấp các thông điệp toàn vẹn và bí mật.
  + ***Tính sẵn sàng:*** Mọi hệ thống thông tin đều phục vụ mục đích riêng của nó và thông tin phải luôn luôn sẵn sàng khi cần thiết. Điều đó có nghĩa rằng hệ thống tính toán sử dụng để lưu trữ và xử lý thông tin, có một hệ thống điều khiển bảo mật sử dụng để bảo vệ nó, và kênh kết nối sử dụng để truy cập nó phải luôn hoạt động chính xác. Hệ thống có tính sẵn sàng cao hướng đến sự sẵn sàng ở mọi thời điểm, tránh được những rủi ro cả về phần cứng, phần mềm như: sự cố mất điện, hỏng phần cứng, cập nhật, nâng cấp hệ thống… đảm bảo tính sẵn sàng cũng có nghĩa là tránh được tấn công từ chối dịch vụ.
  + ***Tính xác thực:*** Trong hoạt động tính toán, kinh doanh qua mạng và an toàn thông tin, tính xác thực là vô cùng cần thiết để đảm bảo rằng dữ liệu, giao dịch, kết nối hoặc các tài liệu (tài liệu điện tử hoặc tài liệu cứng) đều là thật (genuine). Nó cũng quan trọng cho việc xác nhận rằng các bên liên quan biết họ là ai trong hệ thống.
  + ***Tính không thể chối cãi:*** Không thể chối cãi có nghĩa rằng một bên giao dịch không thể phủ nhận việc họ đã thực hiện giao dịch với các bên khác. Ví dụ: trong khi giao dịch mua hàng qua mạng, khi khách hàng đã gửi số thẻ tín dụng cho bên bán, đã thanh toán thành công, thì bên bán không thể phủ nhận việc họ đã nhận được tiền, (trừ trường hợp hệ thống không đảm bảo tính an toàn thông tin trong giao dịch).
* Trong năm 1992 và sửa đổi năm 2002, hướng dẫn của tổ chức OECD về bảo mật cho các hệ thống thông tin mạng đã để xuất 9 nguyên tắc cơ bản sau: tính nhận thức (Awareness), tính trách nhiệm (Responsibility), tính phản hồi (Response), đạo đức (Ethics), tính dân chủ (Democracy), đánh giá rủi ro (Risk Assessment), thiết kế bảo mật và thực thi, quản lý bảo mật, và đánh giá lại (Reassessment). Tiếp nối từ đó, năm 2004, tổ chức NIST đã đưa ra các luật bảo mật thông tin, trong đó đề xuất 33 nguyên tắc.
* Năm 2002, Donn Parker đã đề xuất một mô hình tương đường với tam giác CIA, được gọi là 6 nhân tố cơ bản của thông tin. Các nhân tố đo là: bí mật (confidentiality), sở hữu (possession), toàn vẹn (integrity), xác thực (authenticity), sẵn sàng (availability) và tiện ích (utility).

## **Các lý do gây ra rò rỉ và ảnh hưởng đến thông tin**

Nhìn từ quan điểm hacker, có vô số cách để tấn công, lấy cắp thông tin của một hệ thống. Lỗ hổng của ứng dụng, lỗ hổng dịch vụ trực tuyến (website, gmail…), lỗ hổng hệ điều hành… Vì thế, rất khó để có thể thiết lập và duy trì bảo mật thông tin.

### **Lỗi và sự bỏ sót, cố tình bỏ qua:**

* Nguy cơ này được xếp vào hàng nguy hiểm nhất. Khi lập trình, các cảnh báo và lỗi do trình biên dịch đưa ra thường bị bỏ qua và nó có thể dẫn đến những sự việc không đáng có, ví dụ như tràn bộ đệm, tràn heap. Khi người dùng vô tình (hay cố ý) sử dụng các đầu vào không hợp lý thì chương trình sẽ xử lý sai, hoặc dẫn đến việc bị khai thác, đổ vỡ (crash). Kỹ thuật lập trình đóng vai trò rất quan trọng trong mọi ứng dụng. Và lập trình viên phải luôn luôn cập nhật thông tin, các lỗi bị khai thác, cách phòng chống, sử dụng phương thức lập trình an toàn.
* Một cách tốt nhất để phòng tránh là sử dụng chính sách “least privilege” (có nghĩa là ít quyền hạn nhất có thể). Người dùng sẽ chỉ được xử lý, truy cập đến một số vùng thông tin nhất định.
* Một chính sách khác nhất thiết phải có, đó là phải sao lưu dữ liệu thường xuyên.

### **Lừa đảo và lấy cắp thông tin**

* Tưởng tượng rằng có những đồng nghiệp trong công ty đi làm không phải để làm việc, mà để lấy cắp những thông tin quan trọng của công ty. Chuyện này hoàn toàn có thể xảy ra, đặc biệt là những công ty làm việc về quân sự, cơ quan nhà nước… Rất nhiều công ty bị lộ thông tin từ bên trong. Rất khó phát hiện kẻ tấn công từ bên trong. Việc lấy cắp có thể được thực hiện dưới nhiều hình thức: lấy cắp văn bản in hay lấy cắp thông tin số, cung cấp thông tin nội bộ cho bên ngoài.
* Cách tốt nhất để phòng tránh nguy cơ này là: phải có những chính sách bảo mật được thiết kế tốt. Những chính sách có thể giúp người quản lý bảo mật thông tin thu thập thông tin, từ đó điều tra và đưa ra những kết luận chính xác, nhanh chóng. Khi đã có một chính sách tốt, người quản trị có thể sử dụng các kỹ thuật điều tra số (forensics) để truy vết các hành động tấn công.
* Ví dụ như hình thức lấy cắp thông tin số, nếu một nhân viên truy cập vào khu vực đặt tài liệu bí mật của công ty, hệ thống sẽ ghi lại được thời gian, IP, tài liệu bị lấy, sử dụng phần mềm gì để truy cập, phần mềm bị cài đặt trái phép… từ đó, người quản trị sẽ chứng minh được ai đã làm việc này.

### **Hacker (Tin tặc)**

* Có rất nhiều cách hacker tấn công hệ thống. Mỗi kẻ tấn công đều có những thủ thuật, công cụ, kiến thức, hiểu biết về hệ thống. Và cũng có vô số các cuốn sách, diễn đàn đăng tải những nội dung này.
* Trước tiên, hacker thu thập thông tin về hệ thống, nhiều nhất có thể. Càng nhiều thông tin, thì khả năng thành công của việc tấn công sẽ càng lớn. Những thông tin đó có thể là: tên ứng dụng, phiên bản ứng dụng, hệ điều hành, email quản trị… Bước tiếp theo là quét hệ thống để tìm lỗ hổng. Các lỗ hổng này có thể gây ra bởi ứng dụng xử lý thông tin hoặc do hệ điều hành, hoặc bất kỳ thành phần nào có liên quan. Từ đó, họ sẽ lợi dụng các lỗ hổng tìm được, hoặc sử dụng các tài khoản mặc định nhằm chiếm quyền truy cập vào ứng dụng. Khi đã thành công, hacker sẽ cài đặt các phần mềm, mã độc để có thể xâm nhập vào hệ thống trong các lần sau. Bước cuối cùng là xóa vết tấn công.
* Các trang mạng nổi tiếng như: The World Street Journals, The New York Times mới đây đều công bố rằng mình đã bị hacker tấn công.
* Để phòng tránh nguy cơ này, các ứng dụng tương tác với người dùng, dữ liệu cần phải giấu đi những thông tin quan trọng (nếu có thể) như phiên bản, loại ứng dụng, các thành phần kèm theo… Sử dụng các phần mềm phát hiện truy cập trái phép, rà soát hệ thống thường xuyên xem có phần mềm lạ không, cấu hình tường lửa hợp lý, chính sách truy cập của từng nhóm người dùng, quản lý truy cập…

### **Lây lan mã độc**

* Có rất nhiều loại mã độc có thể kể đến như: virus, sâu máy tính, Trojan horse, logic bomb… Nguy cơ do chúng gây ra là hoàn toàn rõ ràng, và vô cùng phong phú. Khi đã xâm nhập vào máy nạn nhân, mã độc có thể: mở cổng hậu (back door) để kẻ tấn công có thể truy cập và làm mọi việc trên máy nạn nhân; ghi lại thông tin sử dụng máy tính (thao tác bàn phím, sử dụng mạng, thông tin đăng nhập…). Đã có rất nhiều công ty bị cài đặt mã độc. Mới đây, Facebook cũng bị một nhóm hacker tấn công[2] do máy tính của một số nhân viên bị cài mã độc.
* Cài mã độc vào máy tính có thể qua nhiều con đường: lỗ hổng phần mềm (điển hình như adobe Flash, rất nhiều lỗ hổng 0-days được phát hiện, hay Java Runtime Environment thời gian gần đây cũng liên tục đưa ra bản vá bảo mật); hệ thống đã bị hacker điều khiển; sử dụng phần mềm crack, không có giấy phép sử dụng;
* Cách tốt nhất để tránh nguy cơ này là luôn cập nhật phần mềm xử lý dữ liệu, hệ điều hành và phần mềm an ninh mạng, diệt virus.

### **Tấn công từ chối dịch vụ**

* Nếu một hacker không thể cướp quyền truy cập vào một hệ thống, họ sẽ tìm cách tấn công từ chối dịch vụ (làm hệ thống không thể phục vụ người dùng được trong một khoảng thời gian, bằng cách truy cập đến hệ thống liên tục, số lượng lớn, có tổ chức). Có 2 kiểu tấn công từ chối dịch vụ:
* DoS (Deny of Service – tấn công từ chối dịch vụ): tấn công này có thể xảy ra với cả ứng dụng trực tuyến và ứng dụng offline. Với ứng dụng trực tuyến, hacker sử dụng các công cụ tấn công (tấn công Syn floods, Fin floods, Smurfs, Fraggles) trên một máy tính để tấn công vào hệ thống, khiến nó không thể xử lý được yêu cầu, hoặc làm nghẽn băng thông khiến người dùng khác khó mà truy cập được. Với ứng dụng offline, hacker tạo ra những dữ liệu cực lớn, hoặc các dữ liệu xấu (làm cho quá trình xử lý của ứng dụng bị ngưng trệ, treo)
* DDoS (Distributed Deny of Service – tấn công từ chối dịch vụ phân tán): một hình thức cao cấp của DoS, các nguồn tấn công được điều khiển bởi một (một vài) server của hacker (gọi là server điều khiển), cùng tấn công vào hệ thống. Loại tấn công này khó phát hiện ra hơn cho các hệ thống phát hiện tự động, giúp hacker ẩn mình tốt hơn.
* Để chống lại nguy cơ này, hệ thống cần có nhiều server phục vụ, server phân tải, cơ chế phát hiện tấn công DoS hiệu quả.

### **Tấn công Social engineering**

* Thuật ngữ này khá phổ biến trong công nghệ thông tin và an toàn thông tin. Đây là một kỹ thuật khai thác nhằm vào điểm yếu con người. Con người trực tiếp quản lý phần mềm, hệ thống. Do đó, họ nắm được mọi thông tin quan trọng nhất.
* Kỹ thuật này ngày càng hữu ích và có độ chính xác tương đối cao. Điển hình cho hình thức này là hacker nổi tiếng: Kevin Mitnick. Trong một lần, anh chỉ cần vài thông tin quan trọng của tổng thống Mỹ, đã gọi điện cho thư ký của ông và lấy được toàn bộ thông tin về thẻ tín dụng của tổng thống!

# Giới thiệu về ISO

* ISO (International Organization for Standardization) là Tổ chức tiêu chuẩn hóa quốc tế ,là một tổ chức quốc tế độc lập, phi chính phủ hoạt động trong lĩnh vực tiêu chuẩn hóa lớn nhất thế giới, là hệ thống các quy chuẩn quốc tế được đặt ra dựa trên kinh nghiệm của những nhà quản lý thành công hàng đầu thế giới. Đây là tổ chức phát triển các tiêu chuẩn, và nó làm để chứng nhận các doanh nghiệp hoặc tổ chức. Chứng nhận được xử lý của bên thứ ba và được kiểm tra hàng năm. ISO có trụ sở tại Geneva, Thụy Sĩ. Được thành lập năm 1946 và đi vào hoạt động vào ngày 23 tháng 2 năm 1947. Tính đến tháng 10 năm 2020 , ISO có 165 quốc gia thành viên. Việt Nam gia nhập vào ISO năm 1977, là thành viên thứ 77 của tổ chức này.
* ISO là cơ quan thiết lập tiêu chuẩn quốc tế, đưa ra các tiêu chuẩn thương mại và công nghiệp trên phạm vi toàn thế giới. ISO với các tiêu chuẩn hóa thống nhất quốc tế giúp cho quá trình trao đổi này thuận lợi hơn.
* Nhiệm vụ của ISO: Thúc đẩy sự phát triển về vấn đề tiêu chuẩn hoá nhằm tạo điều kiện thuận lợi cho việc trao đổi hàng hóa, dịch vụ quốc tế. Với ích lợi và tính hiệu quả của việc áp dụng ISO, ngày nay người ta mở rộng phạm vi áp dụng cho mọi tổ chức không phân biệt loại hình, quy mô và sản phẩm vào cả lĩnh vực quản lý hành chính, sự nghiệp.
* Khi tham gia ISO, doanh nghiệp/tổ chức sẽ có cơ hội mở rộng, tiếp xúc với các đối tác trong nước và quốc tế. Khi áp dụng các tiêu chuẩn ISO đề ra doanh nghiệp có thể cung cấp 1 cách ổn định các sản phẩm đáp ứng yêu cầu về chất lượng của khách hàng. Đồng thời mở ra cơ hội để khách hàng gắn bó được bền lâu với doanh nghiệp. Khi tham gia ISO tổ chức doanh nghiệp có được hệ thống nhân sự hoạt động chuyên nghiệp, giảm bớt các thủ tục dư thừa từ đó giảm thiểu sự lãng phí về thời gian cũng như kinh phí hoạt động.
* Các quy trình ISO mang đến cho doanh nghiệp hoạt động xuyên suốt không gián đoạn giúp cho sản phẩm được thúc đẩy tăng cao không chỉ về số lượng mà còn cả chất lượng. Vì thế năng lực hoạt động của công ty ngày càng cao. Có thể đáp ứng được các yêu cầu của các doanh nghiệp lớn mạnh.

# Giới thiệu về ISO 27000

## **Giới thiệu chung về ISO 27000**

* ISO 27000 là bộ sản phẩm an toàn đồng nhất do Tổ chức Tiêu chuẩn hóa Quốc tế (ISO) phối hợp với Ủy ban Kỹ thuật điện quốc tế (IEC) xây dựng nhằm giúp các tổ chức có được một công cụ cần thiết áp dụng các quy phạm an toàn thông tin tốt nhất vào hoạt động kinh doanh hàng ngày. Cho dù đó là một công ty lớn hay nhỏ, thì ISO 27000 TOOLKIT cũng đều có thể đưa ra một phạm vi thông tin toàn diện nhất nhằm đảm bảo an toàn cho thông tin của công ty đó.
* ISO 27000 TOOLKIT được xây dựng dựa trên kinh nghiệm phong phú của các chuyên gia cao cấp trong lĩnh vực an toàn thông tin từ nhiều ngành khác nhau, những người mà bản thân họ đã điều hành các dự án an toàn hệ thống kinh doanh một cách thành công trên thế giới. ISO 27000 TOOLKIT đưa ra một phạm vi rộng lớn về khung chính sách mà có thể thay đổi và áp dụng theo nhu cầu riêng của từng tổ chức và từ đó có thể xây dựng văn hóa an ninh thông tin một cách toàn diện.
* Bộ tiêu chuẩn ISO 27000 đã và sẽ bao gồm những tiêu chuẩn cụ thể sau:

1. ISO 27000 quy định các vấn đề về từ vựng và định nghĩa (thuật ngữ)
2. ISO 27001:2005 xác định các yêu cầu đối với hệ thống quản lý an toàn thông tin
3. ISO 27002:2007 đưa ra quy phạm thực hành mô tả mục tiêu kiểm soát an toàn thông tin một cách toàn diện và bảng lựa chọn kiểm soát thực hành an toàn tốt nhất
4. ISO 27003:2007 đưa ra các hướng dẫn áp dụng
5. 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
6. ISO 27005 tiêu chuẩn về quản lý rủi ro an toàn thông tin
7. 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

## **Lịch sử hình thành của ISO 27000**

* ISO 27000 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 quy 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 hóa 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.
* ISO /IEC 27001 là tiêu chuẩn nổi tiếng nhất trong bộ tiêu chuẩn này, nó cung cấp các yêu cầu để xây dựng một hệ thống quản lý an ninh thông tin (ISMS)

## **Lợi ích khi sử dụng ISO 27000**

* Giúp nhận biết, đánh giá được các rủi ro, xây dựng các biện pháp và tạo ý thức và trách nhiệm của nhân viên trong việc bảo vệ thông tin của tổ chức.
* Thể hiện trách nhiệm của tổ chức trong việc quản lý hệ thống thông tin, biểu hiện bảo mật thông tin trên mọi mức độ của tổ chức.
* Thể hiện tính tuân thủ luật pháp và quy tắc trong lĩnh vực quản lý thông tin.
* Quản lý rủi ro, dẫn đến hiểu biết tốt hơn về hệ thống an toàn thông tin, điểm yếu của chúng và cách bảo vệ chúng.
* Các đối tác, cổ đông và khách hàng yên tâm khi họ thấy được sự quan trọng trong bảo vệ thông tin của tổ chức.
* Xác định các thông tin quan trọng, các rủi ro có thể để giảm thiểu các rủi ro đó, xác định các mức chi phí bảo hiểm tốt nhất cho các rủi ro.
* Phát triển nhận thức của nhân viên trong an toàn và trách nhiệm của họ đối với tổ chức.

## **Đối tượng áp dụng**

* Tiêu chuẩn này thích hợp với mọi tổ chức, không phân biệt quy mô, loại hình hay khu vực. Đặc biệt, tiêu chuẩn ISO 27001 thích hợp với các công ty, doanh nghiệp, tổ chức mà việc bảo mật thông tin là rất quan trọng
* Tiêu chuẩn ISO 27001 cũng đặc biệt hiệu quả đối với các công ty thực hiện việc quản lý thông tin cho các tổ chức khác. Tiêu chuẩn ISO 27001 được sử dụng như một lời khẳng định với khách hàng rằng thông tin của họ đang được bảo mật an toàn tuyệt đối.

# Tìm hiểu chi tiết về ISO 27001:2013

ISO /IEC 27001 là một tiêu chuẩn phổ biến trong bộ tiêu chuẩn ISO 27000, nó cung cấp các yêu cầu để xây dựng một hệ thống quản lý an ninh thông tin (ISMS)

Được nâng cấp từ phiên bản ISO 27001:2005 và ISO 27002:2005

Tiêu chuẩn ISO 27001:2013 có cấu trúc bao gồm 2 phần là “Điều khoản” và “Biện pháp kiểm soát”.

## **Doanh nghiệp cần làm gì để xây dựng và áp dụng ISO 27001:2013**

* Doanh nghiệp phải cải tiến cách quản lý hiện tại theo cách quản lý được mô tả trong tiêu chuẩn ISO 27001:2013. Nếu doanh nghiệp nào chưa đáp ứng thì cần bổ sung
* Một số hoạt động cốt lõi của Hệ thống quản lý an ninh thông tin sẽ phải được tiến hành tại Doanh nghiệp:

1. Xác định yêu cầu của Hệ thống quản lý an ninh thông tin
2. Xác định ra những quá trình đảm bảo an ninh thông tin.
3. Đưa ra Chính sách và Mục tiêu an ninh thông tin để định hướng cho từng cá nhân trong Doanh nghiệp
4. Xác định các trách nhiệm quyền hạn của từng bộ phận, cá nhân liên quan đến an ninh thông tin
5. Lập ra các quy trình triển khai để đảm bảo các quá trình được thực hiện theo một phương pháp thống nhất trong Doanh nghiệp.
6. Đào tạo và hướng dẫn các quy trình đến toàn bộ cán bộ công nhân viên
7. Thực hiện đánh giá nội bộ để kiểm tra mức độ tuân thủ các quy trình và hướng dẫn.
8. Thực hiện các biện pháp khắc phục phòng ngừa mỗi khi có sự không phù hợp được phát hiện.

## **Công ty tư vấn làm gì để giúp Doanh nghiệp áp dụng ISO 27001?**

* Khảo sát hoạt động của Doanh nghiệp trước khi áp dụng để xác định ra những việc cần cải tiến cho phù hợp với yêu cầu của ISO 27001: 2013 bao gồm các yêu cầu về cải tiến hạ tầng thông tin nếu có.
* Đào tạo các kiến thức về ISO 27001: 2013 cho cán bộ công nhân viên của Doanh nghiệp.
* Hướng dẫn Doanh nghiệp soạn thảo các quy trình liên quan tới hệ thống.
* Hướng dẫn Doanh nghiệp áp dụng các quy trình đã ban hành
* Đào tạo các kiến thức về đánh giá nội bộ cho đội ngũ đánh giá viên của Doanh nghiệp.
* Chuyển giao các kỹ năng đánh giá hệ thống quản lý an toàn thông tin cho các đánh giá viên của doanh nghiệp thông qua đánh giá thực tế.
* Tư vấn cho doanh nghiệp lựa chọn tổ chức chứng nhận phù hợp.

## **Các yêu cầu của tiêu chuẩn quốc tế ISO 27001:2013**

* Hệ thống quản lý an ninh thông tin
* Trách nhiệm lãnh đạo
* Đánh giá nội bộ Hệ thống ISMS
* Xem xét của lãnh đạo về Hệ thống ISMS
* Cải tiến Hệ thống ISMS

Trích phụ lục A – ISO 27001:2013 14 mục tiêu và biện pháp kiểm soát



1. Chính sách An ninh thông tin
2. Tổ chức đảm bảo ANTT
3. An ninh nguồn nhân lực
4. Quản lý tài sản
5. Kiểm soát truy cập
6. Mã hóa
7. An ninh vật lý và môi trường
8. An ninh vận hành
9. An ninh truyền tin
10. Tiếp nhận, phát triển và duy trì hệ thống

11.Mối quan hệ với các nhà cung cấp

12. Quản lý sự cố an ninh thông tin

13. Quản lý tính liên tục trong kinh doanh

14. Tuân thủ

Các nguyên tắc để đảm bảo ATTT trong việc vận hành, phát triển, duy trì các hệ thống CNTT…

Các lĩnh vực kiểm soát của Phụ lục A. Mỗi lĩnh vực kiểm soát lại được cụ thể hóa với các mục tiêu kiểm soát cần đạt được. Và các biện pháp cụ thể để đạt được mục tiêu đó. Các biện pháp kiểm soát này có thể được lựa chọn, loại bỏ hoặc bổ sung thêm để phù hợp với mỗi tổ chức. Tuy nhiên, các loại bỏ chỉ được chấp nhận khi tổ chức đưa ra các lý giải phù hợp

## **Quy trình áp dụng ISO 27001:2013 vào doanh nghiệp**

* Tại mỗi doanh nghiệp, việc xây dựng, triển khai ISMS có những giải pháp khác nhau. Nó phụ thuộc vào quy mô, đặc trưng của tổ chức cũng như yêu cầu của tổ chức đó. Tuy nhiên, khi triển khai Hệ thống quản lý an toàn thông tin theo ISO 27001. Mỗi tổ chức cần phải thực hiện các bước cơ bản sau để đạt được chứng nhận ISO 27001:
* Bước 1*:* Khảo sát hiện trạng của tổ chức
* Bước 2: Lập kế hoạch xây dựng ISMS
* Bước 3: Xây dựng hệ thống tài liệu và triển khai áp dụng
* Bước 4: Thực hiện đánh giá nội bộ trong tổ chức
* Bước 5: Đánh giá chứng nhận

## **Quy trình đánh giá và cấp chứng chỉ ISO 27001**

* Quy trình đánh giá sẽ được thực hiện bởi một tổ chức chứng nhận. Tổ chức này phải là tổ chức khác với tổ chức đã tư vấn về ISMS cho doanh nghiệp
* Mỗi tổ chức chứng nhận sẽ có cách đánh giá, triển khai, áp dụng các tiêu chuẩn của ISO 27001 khác nhau, nhưng vẫn phải thực hiện đủ các 8 bước sau đây:
* Đăng ký chứng nhận
* Xem xét hợp đồng và lập kế hoạch đánh giá
* Đánh giá tài liệu
* Đánh giá hiện trường
* Thẩm xét hồ sơ
* Cấp giấy chứng nhận hiệu lực 3 năm
* Đánh giá giám sát định kỳ
* Đánh giá chứng nhận lại



Làm cho quá trình chứng nhận ISO 27001 trở nên đơn giản. Chứng nhận ISO 27001. Trước khi đánh giá chứng nhận, doanh nghệp cần tự kiểm tra thông qua những bước sau:

1. Phân tích thiếu sót

Đây là một công việc thông qua đó Doanh nghiệp có cái nhìn gần hơn với hệ thống quản lý an toàn của bạn và so sánh nó với những tiêu chuẩn của ISO 27001. Bước này giúp Doanh nghiệp nhận ra những khu vực cần chú ý nhiều hơn trước khi tiến hành đánh giá chính thức nhằm tiết kiệm thời gian và tiền bạc cho doanh nghiệp của bạn

2. Đánh giá chính thức

Đánh giá chính thức trải qua hai giai đoạn. Đầu tiên, GOODVN sẽ xem lại công tác chuẩn bị cho việc đánh giá của tổ chức của bạn. thông qua việc đánh giá những quy trình cần thiết ISO/IEC 27001 và biện pháp kiểm soát đã được áp dụng. GOODVN sẽ đưa ra những điểm chưa phù hợp trong tài liệu hệ thống nếu có. Doanh nghiệp có thể khắc phục những điểm chưa phù hợp đó.

Nếu tất cả những yêu cầu tài liệu được đáp ứng theo tiêu chuẩn. GOODVN sẽ tiến hành đánh giá việc thực hiện quy trình và việc kiểm soát trong tổ chức của bạn để đảm bảo rằng doanh nghiệp của bạn đang hoạt động một cách hiệu quả như yêu cầu của tiêu chuẩn ISO 27001.

3. Chứng nhận và sau khi chứng nhận

Khi doanh nghiệp của bạn đã được đánh giá và đạt yêu cầu. Doanh nghiệp của bạn sẽ nhận được một chứng chỉ ISO/IEC 27001 và có giá trị trong vòng 03 năm. GOODVN sẽ hỗ trợ khách hàng ở những năm tiếp theo. Nhằm đảm bảo hệ thống của bạn duy trì việc tuân thủ và được cải tiến..

## **Lợi ích của việc áp dụng và chứng nhận ISO 27001:2013**

Lợi ích của việc áp dụng ISO 27001:2013

* Tăng nhận thức và trách nhiệm của nhân viên
* Chuẩn hóa vận hành hệ thống
* Giảm chi phí nhân lực
* Giúp doanh nghiệp đưa ra các quyết định phù hợp
* Nhận diện các rủi ro và đối phó kịp thời
* Giám sát liên tục và cải thiện hiệu suất

Lợi ích của chứng nhận ISO 27001:2013

* Chứng minh cam kết về việc bảo mật an toàn thông tin
* Quản lý thông tin, dữ liệu ở phạm vi rộng
* Tăng khả năng trúng thầu và cơ hội ký kết hợp đồng
* Tăng năng lực hoạt động
* Tăng lợi nhuận

# ISMS (Information Security Management System)

## **Giới thiệu về ISMS**

* ISMS (Information Security Management System) là một bộ quy định (như chính sách, quy trình, hướng dẫn, biểu mẫu…). ISMS được thực hiện trong một tổ chức (doanh nghiệp, trường học) để đảm bảo hệ thống thông tin của tổ chức được an ninh an toàn một cách phù hợp với mục tiêu kinh doanh của tổ chức.

## **Các lĩnh vực ISMS quản lý**

* Hệ thống an ninh thông tin bao gồm tất cả các kiểm soát mà tổ chức đặt trong vị trí thích hợp để đảm bảo an ninh thông tin, xuyên suốt trong 10 lĩnh vực sau:
* Chính sách an ninh (Security policy)
* Tổ chức an ninh (Security organization)
* Phân loại và kiểm soát tài sản (Asset classification and control)
* An ninh nhân sự (Personnel security)
* An ninh môi trường và vật lý (Physical and Environmental Security)
* Quản lý tác nghiệp và truyền thông (Communications and Operations management)
* Kiểm soát truy cập (Access Control)
* Duy trì và phát triển các hệ thống (Systems Development and Maintenance)
* Quản lý sự liên tục trong kinh doanh (Business Continuity Management)
* Tuân thủ (Compliance)

## **Tầm quan trọng và lợi ích của việc triển khai ISMS**

* Đảm bảo ATTT của tổ chức, đối tác và khách hàng, giúp cho hoạt động của tổ chức luôn thông suốt và an toàn.
* Giúp nhân viên tuân thủ việc đảm bảo ANTT trong hoạt động nghiệp vụ thường ngày; Các sự cố ATTT do người dùng dây ra sẽ được hạn chế tối đa khi nhân viên được đào tạo, nâng cao nhận thức ATTT.
* Giúp hoạt động đảm bảo ATTT luôn được duy trì và cải tiến. Các biện pháp kỹ thuật và chính sách tuân thủ được xem xét, đánh giá, đo lường hiệu quả và cập nhật định kỳ.
* Đảm bảo hoạt động nghiệp vụ của tổ chức không bị gián đoạn bởi các sự cố liên quan đến ATTT.
* Nâng cao uy tín của tổ chức, tăng sức cạnh tranh, tạo lòng tin với khách hàng, đối tác, thúc đẩy quá trình toàn cầu hóa và tăng cơ hội hợp tác quốc tế.

## **Xây dựng hệ thống ISMS đạt chứng chỉ ISO 27001**

Áp dụng mô hình PDCA để triển khai hệ thống ISMS.

* Plan: Thiết lập ISMS
* Do: Thi hành và điều hành ISMS
* Check: Kiểm soát và xem xét ISMS
* Act: Duy trì và cải tiến ISMS

Để xây dựng hệ thống ISMS đạt chứng chỉ ISO 27001 phải trải qua 7 giai đoạn:

### **Liệt kê tài sản**

Tài sản bao gồm các loại sau:

* Tài sản thông tin: Tài sản thông tin là loại hình tài sản của Công ty áp dụng đối với các loại tài sản hữu hình và vô hình. Tài sản thông tin bao gồm:
* Các cơ sở dữ liệu và các file dữ liệu, các bản ghi âm.
* Các tài liệu, hồ sơ về bí quyết, bản quyền, về dự án, kỹ thuật và tiêu chuẩn công nghệ, phát triển hệ thống thông tin, hoạt động của hệ thống, bảo trì hệ thống.
* Văn bản về hệ thống, thông tin tìm kiếm, hướng dẫn sử dụng, tài liệu tập huấn, các thủ tục khai thác hoặc hỗ trợ, các kế hoạch nghiệp vụ. Các thông tin kiểm toán, và thông tin thu thập được.
* Hợp đồng và thỏa thuận, thông tin khách hàng.
* Tài sản phần cứng/vật lý:
* Phần cứng và vật lý là loại hình tài sản của Công ty áp dụng đối với tất cả các phần cứng hoặc thiết bị vật lý đang được sử dụng phục vụ sản xuất, kinh doanh và các hoạt động nghiệp vụ khác của Công ty.
* Bao gồm máy tính, thiết bị truyền thông, thiết bị di động, máy in, máy photocopy, máy fax, máy chủ, cơ sở hạ tầng (phòng, đồ nội thất) và các thiết bị khác.
* Tài sản được thống kê theo phần cứng và thiết bị vật lý.
* Tài sản phần mềm
* Tài sản phần mềm là loại hình tài sản của Công ty áp dụng đối với tất cả các phần mềm được sử dụng phục vụ sản xuất, kinh doanh và các hoạt động nghiệp vụ khác của Công ty.
* Bao gồm các phần mềm ứng dụng, hệ điều hành, công cụ phát triển, các tiện ích và các sản phẩm do công ty phát triển, tạo ra.
* Tài sản được thống kê theo: Phần mềm ứng dụng; Hệ điều hành; Công cụ phát triển; Các tiện ích; Các hệ thống thông tin của công ty; Sản phẩm của công ty.
* Tài sản con người
* Bao gồm nhân viên công ty (trình độ, kỹ năng, kinh nghiệm), khách hàng của công ty và các nhà cung cấp dịch vụ của công ty.
* Tài sản được thống kê theo lãnh đạo, trưởng phòng ban và nhân viên.
* Tài sản dịch vụ
* Tài sản dịch vụ bao gồm các dịch vụ đang được sử dụng để phục vụ các hoạt động của Công ty. - Tài sản dịch vụ bao gồm dịch vụ truyền thông, các tiện ích chung như điện, chiếu sáng, điều hòa nhiệt độ, cơ sở hạ tầng
* Tài sản dịch vụ được thống kê theo các dịch vụ truyền thông, các tiện ích chung (điện, chiếu sáng, điều hòa nhiệt độ, cơ sở hạ tầng)
* Tài sản vô hình: Tài sản vô hình bao gồm hình ảnh và danh tiếng của Công ty.

### **Định giá tài sản**

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

### **Xác định hiểm nguy**

* Bước tiếp theo là xác định các threat. Ý tưởng ở đây là phải liệt kê ra các hiểm nguy, đe dọa có thể đối với khối tài sản mà chúng ta đã liệt kê ở trên. Chúng ta cần liệt kê hết, kể cả những đe dọa rất xa vời như ngày tận thế. Đến những hiểm nguy cụ thể hơn như mất mật khẩu, mất máy tính xách tay. Vì tính chất liệt kê hết những mối đe dọa mà chưa tính đến liệu nó có thể xảy ra trên thực tế hay chỉ do chúng ta tưởng tượng ra, cho nên tôi chọn cách dịch từ threat là hiểm nguy hay đe dọa.
* Mối nguy cơ (T): Các nguy cơ được coi là nguyên nhân tiềm tàng gây ra các sự cố không mong muốn, chúng có khả năng gây ra thiệt.
* Cần phải nhận biết các điểm yếu có thể bị khai thác các nguy cơ về an toàn thông tin và là nguyên nhân gây thiệt hại cho các tài sản, cho tổ chức.
* Điểm yếu được nhận biết trong các vấn đề sau:
* Tổ chức Quy trình.
* Thủ tục.
* Thủ tục quản lý.
* Nhân sự.
* Môi trường vật lý.
* Cấu hình hệ thống thông tin.
* Phần cứng, phần mềm, thiết bị truyền thông.
* Sự phụ thuộc vào các thành phần bên ngoài.
* Một điểm yếu mà không có nguy cơ tương ứng thì có thể không cần thiết phải triển khai một biện pháp nào nhưng các thay đổi cần được phát hiện và giám sát chặt chẽ. Ngược lại, một nguy cơ mà không có điểm yếu tương ứng thì có thể không gây ra bất kỳ một rủi ro nào. Trong khi đó, một biện pháp được thực hiện không đúng cách, quy trình hoặc sau chức năng hoặc áp dụng không đúng cũng có thể là một điểm yếu. Biện pháp có hiệu quả hay không còn phụ thuộc vào môi trường vận hành hệ thống. Một điểm yếu có thể liên quan đến các thuộc tính của tài sản bị sử dụng khác với mục đích và cách thức khi được mua sắm hoặc sản xuất, cần phải xem xét các điểm yếu phát sinh từ nhiều nguồn khác nhau. Đầu ra của việc nhận biết về điểm yếu là một danh sách các điểm yếu liên quan đến các tài sản, các mối đe dọa và các biện pháp xử lý. Một danh sách các điểm yếu không liên quan đến bất kỳ nguy cơ nào đã được nhận biết để soát xét.

### **Tính toán các nguy cơ**

* Như vậy chúng ta đã có 2 thứ trong tay. Đó là danh sách tài sản cùng giá trị của chúng và tập hợp các hiểm nguy. Giờ chúng ta sẽ liệt kê dạng “vét cạn” mối hiểm nguy với mỗi tài sản. Với mỗi cặp (tài sản, hiểm nguy) chúng ta cần đưa ra đánh giá khả năng nó xảy ra trên thực tế thế nào. Nói theo thuật ngữ khoa học là tính xác suất của hiểm nguy. Nó biểu thị dưới dạng liệu nó xảy ra bao nhiêu lần trong tháng, trong năm.
* Đây là một đánh giá khó khăn và rất kỹ thuật. Ví dụ, chúng ta có 10 nhân viên, mỗi người có 2 mật khẩu. Vậy khả năng lộ mật khẩu là bao nhiêu trong tháng, trong năm? Tổ chức có thể bị lộ trung bình 1 mật khẩu trong 1 tháng hay không? Danh sách khách hàng của chúng ta liệu có bị lộ 1 lần trong 1 năm không? Nếu chúng ta làm được những đánh giá này thì thật tuyệt vời vì chúng ta có thể lượng hóa tất cả những nguy cơ do mất an ninh gây ra.
* Trên thực tế, việc này không đơn giản nên người ta có thể chấp nhận đánh giá dạng định tính, không chính xác nhưng dễ làm hơn. Ví dụ như việc mất mật khẩu xảy ra với nguy cơ “cao”, lộ bảng lương cán bộ công nhân viên xảy ra với khả năng “thấp”.
* Có 2 phương pháp để đánh giá rủi ro là đánh giá rủi ro định tính và định lượng
* Phương pháp đánh giá định lượng là việc gán một giá trị cụ thể tới các mất mát có thể xảy ra.
* Phương pháp đánh giá định tính đưa ra giá trị chưa xác định đối với việc mất mát dữ liệu chứ không chú trọng vào những thiệt hại về kinh tế đơn thuần.
* Rủi ro là kết hợp của khả năng xảy ra rủi ro và ảnh hưởng của rủi ro.
* Khả năng xảy ra rủi ro cho biết xác suất một điểm yếu của thể bị khai thác trong nguy cơ.
* Ảnh hưởng của rủi ro thể hiện sự mất mát của Công ty từ một nguy cơ.
* Mức độ ảnh hưởng = Nguy cơ \* Điểm yếu
* Mức độ rủi ro đối với một tài sản thông tin thể hiện qua xác suất/tần suất và mức độ ảnh hưởng nếu sự việc diễn ra.
* Đánh giá mức độ rủi ro dựa theo công thức bên dưới:
* Giá trị rủi ro = Xác suất xảy ra \* Mức độ ảnh hưởng \* Giá trị tài sản
* Để xác định giá trị rủi ro công ty cần phải xác định xác suất xảy ra, nguy cơ, điểm yếu, giá trị tài sản

### **4.5 Tính toán các thiệt hại**

* Nếu chúng ta làm tốt các bước trên thì bước đánh giá thiệt hại khi mất an ninh chỉ còn là bài toán số học. Chúng ta có thể lấy tích của giá trị tài sản với khả năng mất chúng. Kết quả để lượng giá được khả năng mất tiền trong một năm nếu chúng ta cứ tiếp tục duy trì hoạt động của tổ chức như hiện nay. Với những nguy cơ lớn và giá trị tài sản mất cao. Thiệt hại nhiều khi có thể khiến công ty phải đóng cửa. Ở phần này, ta không có công thức sẵn sàng để sử dụng. Chúng ta cần phải đề xuất cách thức tính phù hợp với nhu cầu của tổ chức. Ví dụ một cách tính khác là:
* Thiệt hại = xác suất xảy ra sự cố + hậu quả của sự cố + giá trị tài sản bị mất.
* Trong đó các thành phần của công thức đều được định tính hóa cho đơn giản. Như “hậu quả sự cố” bằng điểm 3/2/1 ứng với mức cao/vừa/thấp.
* Với các kết quả tính toán các thiệt hại có thể xảy ra, chúng ta đứng trước câu hỏi: Vậy giờ chúng ta cần làm gì?
* Chấp nhận. Không làm gì thêm cả và chấp nhận thiệt hại nếu nguy cơ trở thành hiện thực.
* Giảm thiểu. Cần có các biện pháp để giảm thiểu khả năng xảy ra nguy cơ xuống mức độ có thể chấp nhận được. Đây là lựa chọn phổ biến nhất khi chúng ta bắt tay vào xây dựng ISMS.
* Chuyển tiếp nguy cơ. Tìm cách để chia sẻ nguy cơ này với đối tác khác. Hình thức phổ biến nhất là mua bảo hiểm. Tổ chức bảo hiểm sẽ cùng chia sẻ thiệt hại cho ta nếu nguy cơ xảy ra thật.

### **4.6 Các giải pháp làm giảm thiểu thiệt hại**

* Nếu chúng ta chọn phương án giảm thiểu thì chúng ta có ngay một câu hỏi tiếp theo là giảm thiểu bằng biện pháp nào. Đây là công đoạn mà các nhà kỹ thuật phải vào cuộc. Để bảo vệ một tài sản thông tin hoặc liên quan tới thông tin. Chúng ta có mấy biện pháp thông thường như sau:
* Xây dựng hệ thống bảo vệ bằng các trang thiết bị chuyên dụng như tường lửa, phát hiện xâm nhập…
* Tăng thêm nhân viên về số lượng và/hoặc chất lượng.
* Đào tạo huấn luyện nhân viên.
* Xây dựng các quy trình, hướng dẫn, biểu mẫu để mọi người phải tuân thủ.
* Xác định trách nhiệm cá nhân thật rõ ràng. Quy định rõ ai chịu trách nhiệm tới đâu với từng tài sản, từng nguy cơ nếu xảy ra là một công tác bắt buộc và được nhấn mạnh trong công cuộc xây dựng hệ thống ISMS.
* Xây dựng hệ thống dự phòng để nếu xảy ra cả những nguy cơ lớn nhất thì chúng ta cũng không bị “đóng cửa”.

### **4.7 Đánh giá chi phí cho giải pháp và đưa ra quyết định**

* Đề ra các biện pháp giảm thiểu nguy cơ là một công việc rất kỹ thuật. Vì vậy, chi phí để thực hiện nó là điều mà các nhà kỹ thuật rất ít quan tâm, hoặc không có khả năng đánh giá. Chúng ta đừng quên là các biện pháp trên là để bảo vệ tài sản. Và tài sản có giá trị nhất định (thường là hữu hạn) của nó. Chúng ta không thể đầu tư 10 đồng để bảo vệ tài sản trị giá 5 đồng. Nếu các bạn trả lời “có thể” thì tôi nghĩ chúng ta nên quay lại phần định giá giá trị tài sản. Có lẽ nó còn quan trọng hơn điều chúng ta nghĩ hoặc chúng ta còn đánh giá thiếu điều gì chăng? Ở bước này, chúng ta sẽ phải làm một bài toán kinh tế thuần túy là đầu tư bao nhiêu để giảm thiểu thiệt hại xuống bao nhiêu. Trả lời câu hỏi “kế hoạch này có đúng trên phương diện kinh tế không? Sau khi đã giảm thiểu nguy cơ và giá trị có thể bị mất, nguy cơ và thiệt hại còn lại có chấp nhận được hay không đối với tổ chức?”. Với mỗi câu trả lời “không”, chúng ta lại phải rà soát lại tất cả những công đoạn đã thực hiện ở trên, xem xét lại các phương án, giải pháp để giảm thiểu nguy cơ cùng chi phí của nó. Cho đến khi tất cả các câu trả lời là “có” thì chúng ta đã hoàn thành một kế hoạch xây dựng hệ thống ISMS.