An ninh thông tin có nhiệm vụ thực hiện vấn đề này. Triển khai an ninh thông tin là thiết lập một hệ thống quản lý an ninh thông tin (ISMS) nhằm đảm bảo 3 thuộc tính của nó: Tính tin cậy (Confidentiality), tính toàn vẹn (Integrity) và tính sẵn sàng (Availability). Làm thế nào để thiết lập một hệ thống ISMS nhất quán, hiệu quả và thật sự chuyên nghiệp? Bài viết này giới thiệu chuẩn ISO 27001:2005, hệ thống ISMS được triển khai, duy trì và cải tiến theo chuẩn này sẽ đáp ứng những vấn đề trên.

**I. ISO 27001:2005 là gì?**

Mục đích của ISO 27001:2005 là cung cấp cơ sở chung cho việc phát triển các chuẩn an ninh tổ chức và thực tiễn quản lý an ninh một cách hiệu quả, đồng thời cung cấp sự tin cậy trong các mối quan hệ của tổ chức.

**II. Phạm vi của chuẩn ISO 27001:2005**

**III. Lợi ích của chuẩn ISO 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 x

**1. Cấp độ tổ chức**

Sự cam kết: Chứng chỉ như là một cam kết hiệu quả của nổ 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.

**2. 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. Điều quan trọng là chuẩn đã bổ sung những chuẩn và luật tồn tại khác.

**3. 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 nhiều khả năng sẵn sàng phụ thuộc ở cả phần cứng và phần mềm.

**4. 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.

**5. Cấp độ tài chính**  
Tiết kiệm chi phí khắc phục các lỗ hỏng an ninh và có khả năng giảm chi phí bảo hiểm.

**6. 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.

**IV. Lịch sử ISO 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 the **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 ninh 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.

Mặc dù ở giai đoạn chuẩn quốc tế bản thảo cuối cùng (FDIS) nhưng tất cả nội dung của ISO 27001 như sau:

1. Phạm vi

2. Giới hạn/ Định nghĩa

3.Tài liệu tham khảo

4. ISMS

5.Trách nhiệm lãnh đạo

6. Những 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.

**V. Hệ thống quản lý an ninh thông tin (ISMS)**

Hệ thống quản lý an ninh thông tin (ISMS) là trái tim của ISO 27001:2005 và là điều kiện tiên quyết cho việc thi hành và lấy chứng chỉ toàn diện. Một hệ thống ISMS phải quản lý tất cả các mặt của an ninh thông tin bao gồm con người, các qui 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. Hệ thống an ninh thông tin bao gồm tất cảc các kiểm soát mà tổ chức đặt trong vị trí thích hợp để đảm bảo an ninh thông tin, xuyên suốt 10 lĩnh vực sau:

**1. Chính sách an ninh (Security Policy)**  
Cung cấp các chỉ dẫn quản lý và hỗ trợ an ninh thông tin

**2. Tổ chức an ninh (Security Organization)**  
Quản lý an ninh thông tin trong tổ chức, duy trì an ninh của các quá trình hỗ trợ thông tin của tổ chức và những tài sản thông tin được truy cập bởi các thành phần thứ ba và duy trì an ninh thông tin khi trách nhiệm việc xử lý thông tin đã được khoán ngoài cho tổ chức khác.

**3. Phân loại và kiểm soát tài sản (Asset Classification and Control)**  
Duy trì và đảm bảo các tài sản của tổ chức được bảo vệ ở các cấp độ thích hợp.

**4. An ninh nhân sự (Personnel Security)**  
Để giảm rủi ro về lỗi của con người, sự ăn cắp, gian lận hoặc lạm dụng. Đảm bảo người dùng nhận thức các mối đe dọa an ninh thông tin liên quan và được trang bị để hỗ trợ chính sách an ninh của tổ chức trong phạm vi công việc bình thường của họ, giảm thiểu từ những bất thường và sai chức năng an ninh và để kiểm soát cũng như học hỏi từ các bất thường như vậy.

**5. An ninh môi trường và vật lý (Physical and Enviromental Security)**  
Ngăn cản truy cập vật lý không được phép, phá hủy và can thiệp đến những thông tin và cơ ngơi doanh nghiệp. Ngăn cản sự mất mát, phá hủy hoặc tấn công những tài sản và cắt đứt các hoạt động kinh doanh. Ngăn cản sự tấn công hoặc ăn cắp thông tin và qui trình hỗ trợ xử lý thông tin.

**6. Quản lý tác nghiệp và truyền thông (Communications and Operations Management)**  
Đảm bảo tác nghiệp bảo mật và đúng hỗ trợ xử lý thông tin, giảm thiểu rủi ro lỗi của các hệ thống, bảo vệ sự nguyên vẹn của phần mềm và những thông tin từ việc phá hủy của phần mềm dã tâm. Duy trì sự nguyên vẹn và sẵn sàng của quá trình xử lý thông tin và các dịch vụ truyền thông, đảm bảo sự an toàn của thông tin trong mạng và bảo vệ cơ sở hạ tầng hỗ trợ, ngăn cản phá hủy tài sản và làm gián đoạn các hoạt động kinh doanh, ngăn cản sự mất mát, sửa đổi và lạm dụng thông tin trao đổi giữa các tổ chức.

**7. Kiểm soát truy cập (Access Control)**Kiểm soát truy cập đến thông tin, đảm bảo các quyền truy cập đến các hệ thống thông tin được cấp quyền, cấp phát tài nguyên và duy trì một cách phù hợp. Ngăn cản truy cập trái phép, phát hiện các hoạt động trái phép, bảo vệ các dịch vụ mạng, đảm bảo an ninh thông tin khi dùng máy tính di động và phương tiện điện thoại.

**8. Duy trì và phát triển các hệ thống (Systems Development and Maintenance)**  
Đảm bảo an ninh được xây dựng bên trong các hệ thống thông tin. Ngăn cản, điều chỉnh, và lạm dụng dữ liệu của người dùng trong các hệ thống ứng dụng, bảo vệ tính tin cậy, tính xác thực hoặc nguyên vẹn của thông tin. Đảm bảo các dự án CNTT và các hoạt động hỗ trợ được điều hành trong một thể thức an ninh. Duy trì an ninh của phần mềm hệ thống ứng dụng và thông tin.

**9. Quản lý sự liên tục trong kinh doanh (Business Continuity Management)**  
Chống lại sự ngưng trệ của các họat động kinh doanh và bảo vệ các quá trình kinh doanh quan trọng từ hậu quả của lỗi lớn hoặc hiểm họa.

**10. Tuân thủ (Compliance)**  
Tránh sự vi phạm của mọi luật công dân và hình sự, tuân thủ pháp luật, qui định hoặc nghĩa vụ của hợp đồng và mọi yêu cầu về an ninh. Đảm bảo sự tuân thủ của các hệ thống với các chính sách an ninh và các chuẩn. Tăng tối đa hiệu quả và giảm thiểu trở ngại đến quá trình đánh giá hệ thống.

**VI. Áp dụng mô hình PDCA để triển khai hệ thống ISMS**  
**1. Plan (Thiết lập ISMS)**  
Thiết lập chính sách an ninh, mục tiêu, mục đích, các quá trình và thủ tục phù hợp với việc quản lý rủi ro và cải tiến an ninh thông tin để phân phối các kết quả theo các mục tiêu và chính sách tổng thể của tổ chức.

**2. Do (Thi hành và điều hành ISMS)**  
Thi hành và điều hành chính sách an ninh, các dấu hiệu kiểm soát, các quá trình và các thủ tục.

**3. Check (Kiểm soát và xem xét ISMS)**  
Đánh giá, tìm kiếm sự phù hợp, đo lường hiệu năng của quá trình so với chính sách an ninh, mục tiêu, kinh nghiệm thực tế và báo cáo kết quả cho lãnh đạo xem xét.

**4. Act (duy trì và cải tiến ISMS)**  
Đưa ra các hành động khắc phục phòng ngừa trên cơ sở các kết quả xem xét để cải tiến liên tục hệ thống ISMS.

**VII. Triển khai chuẩn ISO 27001:2005 cho tổ chức  
Giai đoạn 1:**Khởi động dự án

Thi hành ISO 27001:2005 dưới các hình thức: ủng hộ cam kết từ lãnh đạo cấp cao, chọn và đào tạo tất cả các thành viên của nhóm khởi động là một phần trong dự án.

**Giai đoạn 2:**Thiết lập ISM  
Nhận dạng phạm vi và giới hạn của cơ cấu quản lý an ninh thông tin là cốt lõi cho dự án. Nghiên cứu để thiết lập yêu cầu của ISMS và sắp xếp các tài liệu an ninh đã tồn tại trong tổ chức.

**Giai đoạn 3:** Đánh giá rủi ro  
Đánh giá rủi ro là thao tác cơ bản để triển khai cơ cấu quản lý an ninh thông tin.

a) Khảo sát các cấp độ tuân thủ với ISO 27001:2005.

b) Định giá tài sản để được bảo vệ và tạo thống kê tài sản.

c) Nhận dạng và đánh giá các mối đe dọa và những nơi dễ bị tấn công.

d) Tính toán liên quan đến giá trị rủi ro.

**Giai đoạn 4:** Xử lý rủi ro   
Nhận dạng và đánh giá các khả năng có thể cho việc xử lý rủi ro. Làm cách nào để giảm rủi ro đến cấp độ có thể chấp nhận được bằng việc chọn và thi hành các kiểm soát.

**Giai đoạn 5:** Đào tạo và nhận thứ**c**  
Nhân viên có thể giới thiệu các liên kết yếu trong chuỗi an ninh. Nghiên cứu cách làm thế nào để thiết lập chương trình nhận thức an ninh thông tin.

**Giai đoạn 6:** Chuẩn bị đánh giá  
Nghiên cứu cách xác thực cơ cấu quản lý và để chuẩn bị cho việc đánh giá của chuyên gia đánh giá nội bộ.

**Giai đoạn 7:** Đánh giá  
Xem xét các bước thực hiện của chuyên gia đánh giá bên ngoài và đoàn đánh giá chứng nhận chính thức.

**Giai đoạn 8:**Kiểm soát và cải tiến liên tục  
Cải tiến hiệu quả của hệ thống ISMS phù hợp với mô hình quản lý của tổ chức được ghi nhận bởi ISO.

**VIII. Kết luận**  
Hệ thống quản lý an ninh thông tin ISMS bao gồm con người, các quá trình và các hệ thống CNTT. Lập một Hệ thống ISMS theo chuẩn ISO 27001:2005 là cách tiếp cận mang tính hệ thống để quản lý thông tin nhạy cảm của tổ chức nhằm duy trì và đảm bảo 3 thuộc tính an ninh thông tin: Tính tin cậy, tính toàn vẹn và tính sẵn sàng thông qua 10 mục tiêu, lĩnh vực chính. ISO 27001:2005 giúp cho tổ chức tạo được một hệ thống quản lý an ninh thông tin chặt chẻ và luôn được cải tiến nhằm đảm bảo an ninh và khai thác thông tin một cách hợp lý và hiệu quả nhất.