Chương 1B:

HỆ THỐNG QUẢN LÝ AN TOÀN THÔNG TIN

1

Hệ thống quản lý ATTT (ISMS)

- Bên cạnh những rủi ro về ATTT do bị tấn công phá hoại có chủ đích, tổ chức cũng có thể gặp phải những rủi ro đối với thông tin nếu: Các quy trình quản lý, vận hành không đảm bảo; Việc quản lý quyền truy cập chưa được kiểm tra và xem xét định kỳ; Nhận thức của nhân viên trong việc sử dụng và trao đổi thông tin chưa đầy đủ….
- Do đó, ngoài các biện pháp kỹ thuật, tổ chức cần xây dựng và áp dụng các chính sách, quy định, quy trình vận hành phù hợp để giảm thiểu rủi ro.

2

Hệ thống quản lý ATTT (ISMS)

- Tùy vào quy mô và lĩnh vực hoạt động, mỗi tổ chức có thể có các phương thức tiếp cận khác nhau để xây dựng hệ thống quản lý ATTT phù hợp
- ***Hệ thống quản lý ATTT (ISMS)*** giúp tổ chức thực hiện việc ***kiểm soát và định hướng cho các hoạt động đảm bảo ATTT***

3

Hệ thống quản lý ATTT (ISMS)

- Thiết kế và triển khai Hệ thống ISMS phụ thuộc vào mục tiêu, các yêu cầu về ATTT cần phải đạt được, các quy trình đang vận hành, quy mô và cơ cấu của tổ chức...
- Hệ thống ISMS cũng đòi hỏi phải luôn được xem xét, cập nhật để phù hợp với những thay đổi của tổ chức và nâng cao mức độ an toàn với Hệ thống lưu trữ, xử lý thông tin.
- Tổ chức cũng cần cân nhắc chi phí đầu tư xây dựng và triển khai ISMS phù hợp với nhu cầu đảm bảo ATTT.
- Sau khi xây dựng hệ thống ISMS thì doanh nghiệp sẽ nhận được ***Chứng chỉ An toàn bảo mật thông tin***

4

Hệ thống quản lý ATTT (ISMS)

- Việc áp dụng ISMS là quyết định mang tính chiến lược của một tổ chức. Hệ thống quản lý an toàn thông tin (ISMS) duy trì tính bảo mật, tính toàn vẹn và tính sẵn sàng của thông tin bằng cách áp dụng một quá trình quản lý rủi ro và mang lại sự tin cậy cho các bên quan tâm rằng các rủi ro đã được quản lý đầy đủ.

5

Lợi ích khi áp dụng ISMS

1) Đảm bảo ATTT của tổ chức, đối tác và khách hàng, giúp cho hoạt động của tổ chức luôn thông suốt và an toàn.
2) Giúp nhân viên tuân thủ việc đảm bảo ATTT trong hoạt động nghiệp vụ thường ngày; Các sự cố ATTT do người dùng gây ra sẽ được hạn chế tối đa khi nhân viên được đào tạo, nâng cao nhận thức ATTT.
3) 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.

6

Lợi ích khi áp dụng ISMS

4) Đảm bảo hoạt động nghiệp vụ của tổ chức không bị gián đoạn bởi các sự cố liên quan đến ATTT.
5) 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

7

Tiêu chuẩn ISO/IEC 27001:2013

- ***ISO/IEC 27001*** là tiêu chuẩn quốc tế về Hệ thống quản lý an ninh thông tin (ISMS).
- ISO/IEC 27001 là tiêu chuẩn quy định các yêu cầu đối với việc xây dựng và áp dụng hệ thống quản lý ATTT nhằm ***đảm bảo tính bảo mật (confidentiality)***, ***tính nguyên vẹn (integrity)*** và ***tính sẵn sàng (availability)*** đối với tài sản thông tin của các tổ chức.

8

Tiêu chuẩn ISO/IEC 27001:2013

- Là một tiêu chuẩn trong bộ tiêu chuẩn ISO/IEC 27000 về quản lý ATTT, được xây dựng dựa trên các tiêu chuẩn về quản lý an toàn thông tin BS 7799 của Viện Tiêu chuẩn Anh (British Standards Institute - BSI).
- Năm 2005, tiêu chuẩn này được ban hành lần 1 tiêu chuẩn ISO/IEC 27001:2005, đến năm 2013 ban hành tiêu chuẩn lần 2 ISO/IEC 27001:2013

9

Tiêu chuẩn ISO/IEC 27001:2013

- Đối tượng áp dụng: cho nhiều loại hình tổ chức (thương mại, cơ quan nhà nước, phi lợi nhuận...). Đặc biệt là các tổ chức mà các hoạt động phụ thuộc nhiều vào CNTT, máy tính, mạng máy tính, sử dụng CSDL như ngân hàng, tài chính, viễn thông, ...
- ***Một hệ thống ISMS theo tiêu chuẩn ISO/IEC 27001:2013*** sẽ đem lại sự tin tưởng của các bên liên quan như đối tác, khách hàng,... của tổ chức.
- Doanh nhiệp sẽ được cấp ***Chứng chỉ An toàn bảo mật thông tin ISO 27001:2013***

10

Tiêu chuẩn ISO/IEC 27001:2013

- Tiêu chuẩn này được xây dựng nhằm cung cấp các yêu cầu cho việc thiết lập, triển khai, duy trì và cải tiến liên tục Hệ thống quản lý an toàn thông tin (ISMS).
- ISO/IEC 27001 đặc tả các yêu cầu cần thiết cho việc thiết lập, vận hành và giám sát hoạt động của ISMS; đưa ra các nguyên tắc cơ bản cho việc khởi tạo, thực thi, duy trì và cải tiến ISMS.
- Tiêu chuẩn này đưa ra các quy tắc bảo mật thông tin và đánh giá sự tuân thủ đối với các bộ phận bên trong tổ chức, xây dựng các yêu cầu bảo mật thông tin mà đối tác, khách hàng cần phải tuân thủ khi làm việc với tổ chức.

11

Cấu trúc Tiêu chuẩn ISO 27001: 2013

- Gồm có ***07 điều khoản chính (từ phần 4 đến phần 10 của Tiêu chuẩn)***
- Các điều khoản đưa ra yêu cầu bắt buộc về các công việc cần thực hiện trong việc thiết lập, vận hành, duy trì, giám sát và nâng cấp Hệ thống ISMS của các tổ chức.
- Bất kỳ vi phạm nào của tổ chức so với các quy định nằm trong 07 điều khoản này đều được coi là không tuân thủ theo tiêu chuẩn.

12

Cấu trúc Tiêu chuẩn ISO 27001: 2013

- ***Điều khoản 4 - Phạm vi tổ chức***: Đưa ra các yêu cầu cụ thể để tổ chức căn cứ trên quy mô, lĩnh vực hoạt động và các yêu cầu, kỳ vọng của các bên liên quan thiết lập phạm vi Hệ thống quản lý ATTT phù hợp.
- ***Điều khoản 5 - Lãnh đạo***: Quy định các vấn đề về trách nhiệm của Ban lãnh đạo mỗi tổ chức trong Hệ thống ISMS, bao gồm các yêu cầu về sự cam kết, quyết tâm của Ban lãnh đạo trong việc xây dựng và duy trì hệ thống; các yêu cầu về việc cung cấp nguồn lực, tài chính để vận hành hệ thống.

13

Cấu trúc Tiêu chuẩn ISO 27001: 2013

- ***Điều khoản 6 - Lập kế hoạch***: Tổ chức cần định nghĩa và áp dụng các quy trình đánh giá rủi ro, từ đó đưa ra các quy trình xử lý. Điều khoản này cũng đưa ra các yêu cầu về việc thiết lập mục tiêu ATTT và kế hoạch để đạt được mục tiêu đó.
- ***Điều khoản 7 - Hỗ trợ***: yêu cầu đối với việc tổ chức đào tạo, truyền thông, nâng cao nhận thức cho toàn thể cán bộ, nhân viên của tổ chức về lĩnh vực ATTT và ISMS, số hóa thông tin.
- ***Điều khoản 8 - Vận hành hệ thống***: Tổ chức cần có kế hoạch vận hành và quản lý để đạt được các mục tiêu đã đề ra. Đồng thời cần định kỳ thực hiện đánh giá rủi ro ATTT và có kế hoạch xử lý.

14

Cấu trúc Tiêu chuẩn ISO 27001: 2013

- ***Điều khoản 9 - Đánh giá hiệu năng hệ thống***: Quy định trách nhiệm của Ban lãnh đạo trong việc định kỳ xem xét, đánh giá Hệ thống ISMS của tổ chức. Phần này đưa ra yêu cầu đối với mỗi kỳ xem xét hệ thống, đảm bảo đánh giá được toàn bộ hoạt động của hệ thống, đo lường hiệu quả của các biện pháp thực hiện và có kế hoạch khắc phục, nâng cấp hệ thống cho phù hợp với những thay đổi trong hoạt động của tổ chức.
- ***Điều khoản 10 - Cải tiến hệ thống***: Giữ vững nguyên tắc Kế hoạch - Thực hiện - Kiểm tra - Hành động (P-D-C-A), tiêu chuẩn cũng đưa ra các yêu cầu đảm bảo Hệ thống ISMS không ngừng được cải tiến trong quá trình hoạt động. Gồm các quy định trong việc áp dụng các chính sách mới, các hoạt động khắc phục, phòng ngừa các điểm yếu đã xảy ra và tiềm tàng để đảm bảo hiệu quả của Hệ thống ISMS.

15

Triển khai ISMS ở Việt Nam

- Bước 1: ***Khảo sát và lập kế hoạch***
- Bước 2: ***Xác định phương pháp quản lý rủi ro ATTT***
- Bước 3: ***Xây dựng hệ thống đảm bảo ATTT tại đơn vị***
- Bước 4: ***Triển khai áp dụng***: các biện pháp đã lựa chọn, đáp ứng chính sách, quy định, quy trình đã xây dựng và yêu cầu của tiêu chuẩn ISO 27001.
- Bước 5: ***Đánh giá nội bộ***: khắc phục các điểm không phù hợp với các quy định của tổ chức và yêu cầu của tiêu chuẩn. Sau khi thực hiện xong bước 5, tổ chức mời các đơn vị độc lập để ***đánh giá và cấp Chứng nhận phù hợp với tiêu chuẩn ISO 27001:2013*** cho Hệ thống quản lý ATTT đã xây dựng.

16

DN nhận CC ATTT theo tiêu chuẩn ISO/IEC 27001:2013

- Công ty Cổ phần Dịch vụ Công nghệ Tin học HPT – 12/05/2014
- Ngân hàng VIETCOMBANK - 12/12/2014 (NH đầu tiên)
- Tập đoàn Bảo Việt – 23/1/2016
- Trung tâm Internet Việt Nam (VNNIC) - 02/7/2015
- Ngân hàng TMCP Sài Gòn - Hà Nội (SHB) - 20/11/2015
- Trung tâm dữ liệu của VNPT (VNPT Data) – 1/9/2016
- Ngân hàng TMCP Quân đội (MB) - 04/2017
- .....

17

Bài tập nhóm

- **Task 1:** Hình thành nhóm từ 3-5 người
  - Tổ chức nhóm
  - Kết nối để làm việc online/offline
  - Chọn 1 công cụ/tool hỗ trợ làm việc nhóm
- **Task 2:** Tìm kiếm 1 doanh nghiệp đã nhận chứng chỉ ATTT theo tiêu chuẩn ISO/IEC 27001:2013 (hoặc tương đương). Tìm hiểu và trình bày **những điểm nổi bật** chính sách ATTT của doanh nghiệp đó.
  - Lập bản kế hoạch thực hiện bài tập (thời gian, nội dung, nhân sự)
  - Trình bày dạng trình chiếu (powerPoint) hoặc clip
  - Thuyết trình/trình bày trước lớp 10 phút

18