CHƯƠNG 3

QUẢN LÝ VÀ XÂY DỰNG KẾ HOẠCH CHIẾN LƯỢC AN TOÀN THÔNG TIN

Chương 03 - MỤC TIÊU

- Giúp sinh viên xác định các bên liên quan chính của tổ chức tham gia tích cực vào việc lập kế hoạch và vai trò của họ
- Hướng dẫn sinh viên nắm và viết được kế hoạch An toàn thông tin.

QUẢN LÝ VÀ XÂY DỰNG KẾ HOẠCH CHIẾN LƯỢC ATTT

- Vai trò của việc xây dựng kế hoạch
- Xây dựng kế hoạch chiến lược
- Quản trị an toàn thông tin
- Xây dựng kế hoạch triển khai đảm bảo ATTT
- Câu hỏi ôn tập

Vai trò của việc xây dựng kế hoạch

- Lập kế hoạch là phương tiện chủ đạo để quản lý tài nguyên trong các tổ chức
- đòi hỏi việc liệt kê một chuỗi các hành động nhằm đạt được các mục tiêu, cụ thể trong một khoảng thời gian xác định và kiểm soát việc thực hiện các bước này.
- cung cấp định hướng cho tương lai của tổ chức.

TỔNG QUAN VỀ QUẢN LÝ AN TOÀN THÔNG TIN

- Vai trò của việc xây dựng kế hoạch
- **Xây dựng kế hoạch chiến lược**
- Quản trị an toàn thông tin
- Xây dựng kế hoạch triển khai đảm bảo ATTT
- Câu hỏi ôn tập

Xây dựng kế hoạch chiến lược…

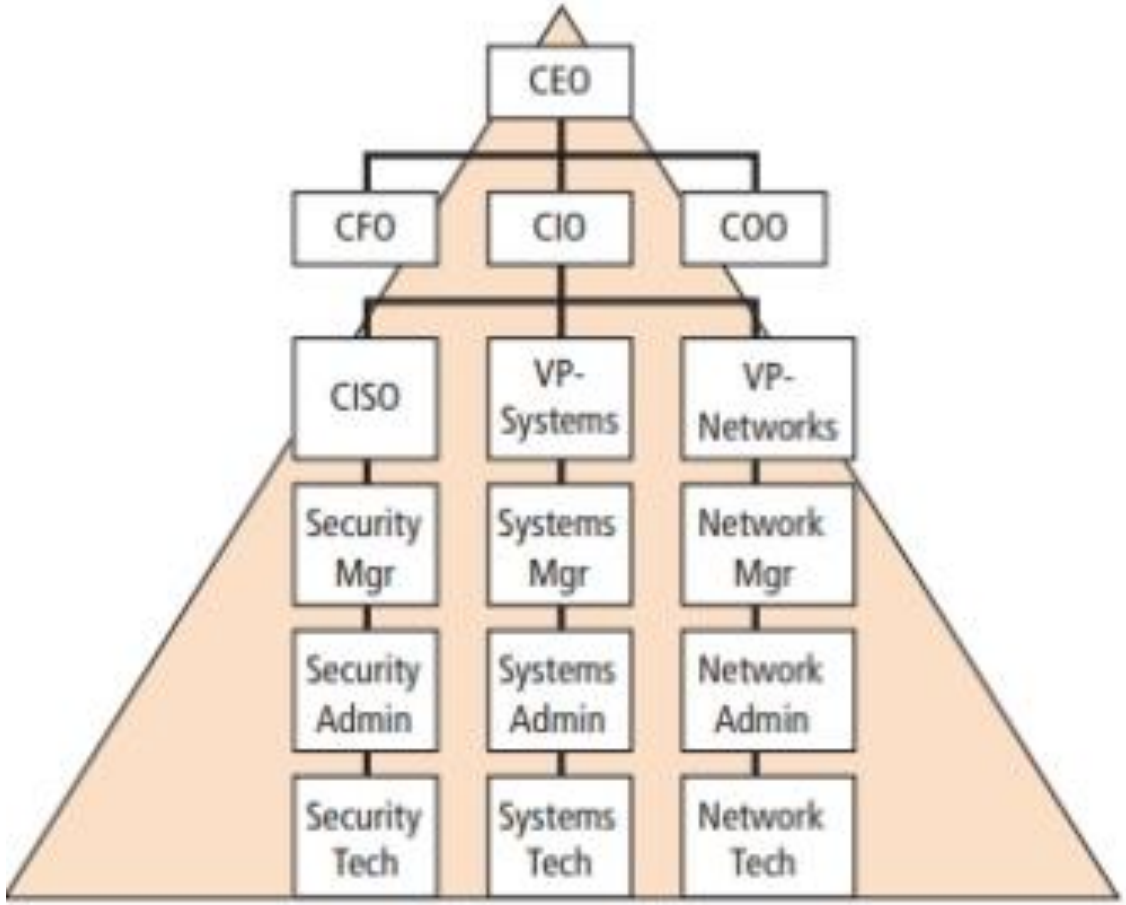
- Là quá trình xác định và chỉ rõ định hướng (chiến lược) dài hạn mà một tổ chức thực hiện, và việc phân bổ, thu nhận các nguồn lực cần thiết để theo đuổi nỗ lực này.

Xây dựng kế hoạch chiến lược…

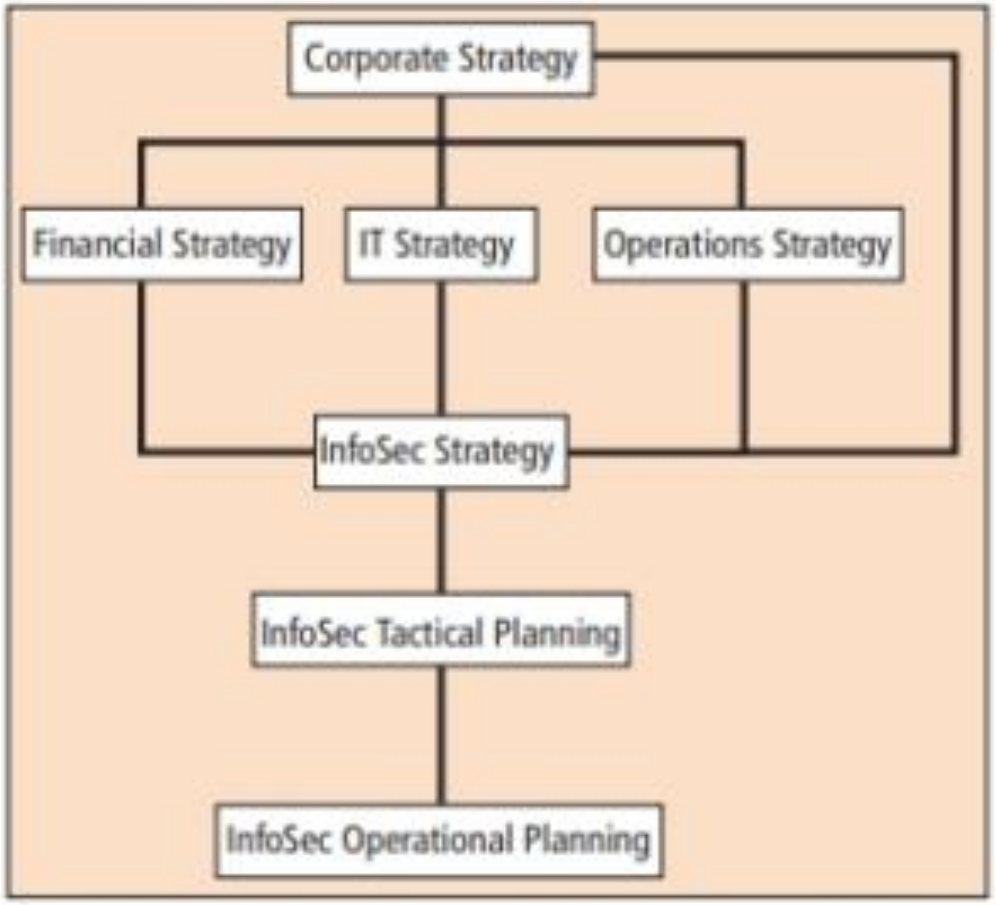
- lập kế hoạch sử dụng quy trình ba bước:
  - xác định mục tiêu cho một lĩnh vực cần cải tiến hoặc nhu cầu về khả năng mới, sau đó tổ chức ghi lại tiến trình hiện tại để hoàn thành mục tiêu đó (hiện tại chúng ta đang ở đâu?).
  - lãnh đạo chỉ rõ vị trí tổ chức tìm kiếm để đạt được mục tiêu (chúng ta đang đi đâu?).
  - lập kế hoạch làm cách nào để đạt được mục tiêu đó (chúng ta sẽ đạt được mục tiêu đó như thế nào?).

Xây dựng kế hoạch chiến lược…

- Lập kế hoạch chiến lược từ trên xuống



Hệ thống phân cấp tổ chức



Lập kế hoạch phân cấp

Xây dựng kế hoạch chiến lược…

- Nhóm An toàn thông tin phải hiểu và hỗ trợ các kế hoạch chiến lược (hay chiến lược) của tất cả các đơn vị kinh doanh. Vai trò này đôi khi có thể mâu thuẫn với vai trò của bộ phận CNTT, vì vai trò của IT là cung cấp thông tin và tài nguyên thông tin một cách hiệu quả và hiệu quả, trong khi vai trò của An toàn thông tin là bảo vệ tất cả các tài sản thông tin.
- An toàn có thể bắt đầu như một nỗ lực cơ bản (cách tiếp cận từ dưới lên) hoặc với các kế hoạch do quản lý cấp cao xây dựng (cách tiếp cận từ trên xuống).

Xây dựng kế hoạch chiến lược…

- Để phát triển và thực hiện việc lập kế hoạch hiệu quả:
  - phải tạo ra các tài liệu đại diện cho các quan điểm triết học, đạo đức và kinh doanh của công ty - cụ thể: sứ mệnh, tầm nhìn, giá trị và chiến lược của tổ chức.
  - Lập kế hoạch chiến lược đưa ra định hướng dài hạn mà tổ chức sẽ thực hiện và hướng dẫn các nỗ lực của tổ chức.
  - Chiến lược chung ban đầu được chuyển thành chiến lược cụ thể và sau đó được chuyển thành kế hoạch chiến thuật và hoạt động cấp thấp hơn.

Xây dựng kế hoạch chiến lược

- Các thành phần cơ bản của một kế hoạch chiến lược cấp tổ chức điển hình:

1. Tóm tắt
2. Tuyên bố về Sứ mệnh, Tầm nhìn và Giá trị
3. Hồ sơ và lịch sử tổ chức
4. Các vấn đề và thách thức chiến lược
5. Mục tiêu của Tổ chức
6. Mục tiêu của Đơn vị Kinh doanh Chính (hoặc Sản phẩm/Dịch vụ)
7. Phụ lục (nếu có, bao gồm phân tích thị trường, khảo sát nội bộ/bên ngoài, ngân sách và dự kiến R&D).

TỔNG QUAN VỀ QUẢN LÝ AN TOÀN THÔNG TIN

- Vai trò của việc xây dựng kế hoạch
- Xây dựng kế hoạch chiến lược
- **Quản trị an toàn thông tin**
- Xây dựng kế hoạch triển khai đảm bảo ATTT
- Câu hỏi ôn tập

Quản trị an toàn thông tin…

- Quản trị ATTT là quá trình tạo và duy trì cấu trúc tổ chức quản lý chức năng ATTT trong một tổ chức.
- có 05 mục tiêu chính:
  - điều chỉnh chiến lược ATTT và các mục tiêu kinh doanh;
  - sử dụng các phương pháp quản lý rủi ro để hướng dẫn việc ra quyết định của ATTT;
  - thực hiện các thực hành quản lý tài nguyên hợp lý cho các chương trình ATTT;
  - đo lường hiệu suất của các chức năng ATTT;
  - mang lại giá trị cho tổ chức.

Quản trị an toàn thông tin…

- khuyến nghị bốn thực hành cần thiết cho hội đồng quản trị:
  - Đặt ATTT vào chương trình làm việc của hội đồng quản trị.
  - Xác định các nhà lãnh đạo ATTT, quy trách nhiệm cho họ và đảm bảo hỗ trợ họ.
  - Đảm bảo tính hiệu quả của CSATTT của tổ chức thông qua việc xem xét và phê duyệt.
  - Chỉ định ATTT cho một ủy ban chính và đảm bảo hỗ trợ đầy đủ cho ủy ban đó.

Quản trị an toàn thông tin…

- Lợi ích:
  - Gia tăng giá trị cổ phiếu cho các tổ chức
  - Tăng khả năng dự đoán và giảm tính không chắc chắn của hoạt động kinh doanh bằng cách giảm rủi ro liên quan đến ATTT xuống mức có thể xác định và chấp nhận được
  - Bảo vệ khỏi nguy cơ ngày càng tăng về trách nhiệm dân sự hoặc pháp lý do TT không chính xác hoặc thiếu sự quan tâm thích hợp
  - Tối ưu hóa việc phân bổ các nguồn lực AT hạn chế
  - Đảm bảo tuân thủ CS và CSATTT hiệu quả
  - Một nền tảng vững chắc để quản lý rủi ro hiệu quả, cải tiến quy trình và ứng phó sự cố nhanh chóng
  - Đảm bảo phần nào rằng các quyết định quan trọng không dựa trên TT sai
  - Trách nhiệm giải trình đối với việc bảo vệ TT trong các hoạt động kinh doanh quan trọng, chẳng hạn như sáp nhập và mua lại, khôi phục quy trình kinh doanh và phản ứng theo quy định.

Quản trị an toàn thông tin…

- Chương trình quản trị ATTT bao gồm:
  - Phương pháp quản lý rủi ro ATTT
  - Một chiến lược AT toàn diện được liên kết rõ ràng với các mục tiêu kinh doanh và CNTT
  - Một cơ cấu tổ chức an toàn hiệu quả
  - Một chiến lược AT nói về giá trị của thông tin được bảo vệ và cung cấp
  - Các CSAT giải quyết từng khía cạnh của chiến lược, kiểm soát và quy định
  - Một bộ tiêu chuẩn AT hoàn chỉnh cho từng CS để đảm bảo rằng các thủ tục, hướng dẫn tuân thủ CS
  - Các quy trình giám sát được thể chế hóa để đảm bảo tuân thủ và cung cấp phản hồi về tính hiệu quả và giảm thiểu rủi ro
  - Một quy trình để đảm bảo tiếp tục đánh giá và cập nhật các CS, tiêu chuẩn, thủ tục và rủi ro AT

Quản trị an toàn thông tin…

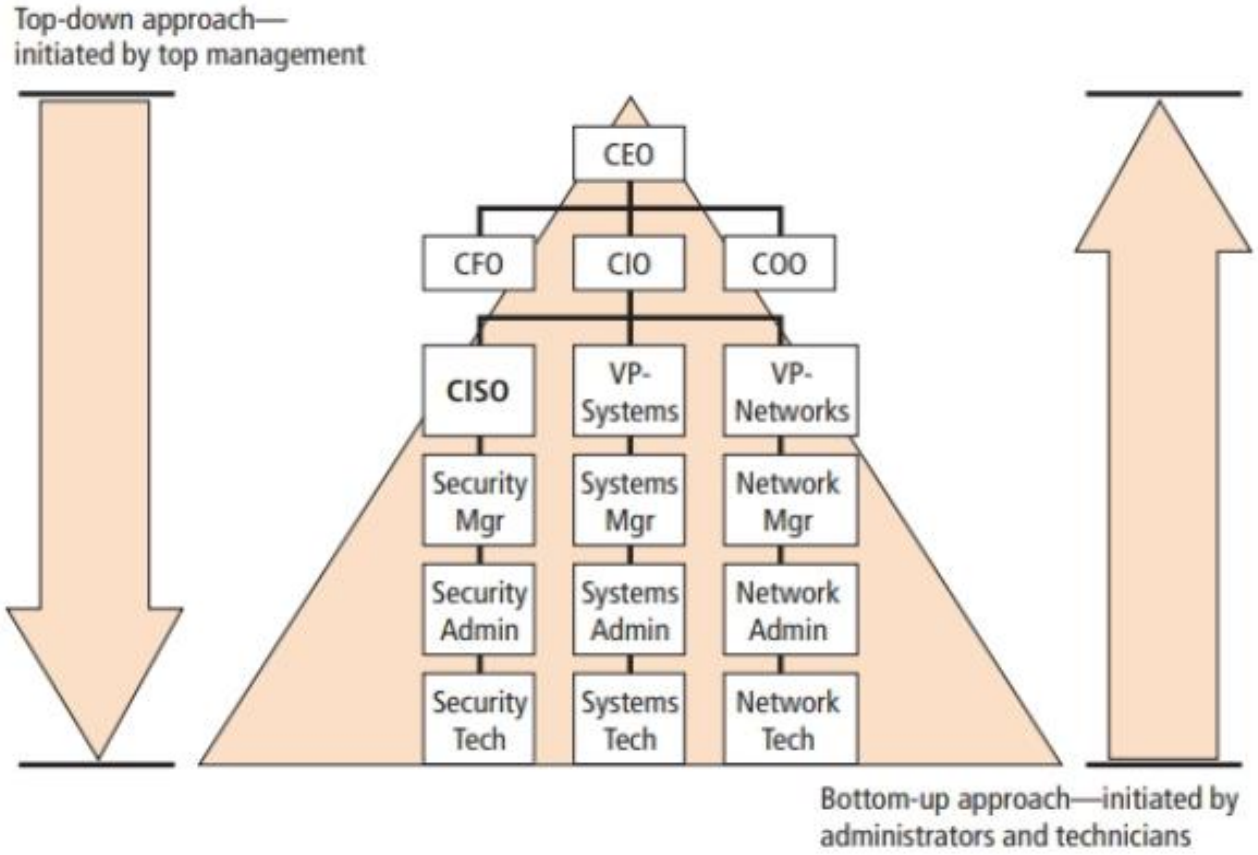
- Một số tham khảo:
  - Khung công nghiệp NCSP (National Cyber Security Partnership) về quản trị an toàn thông tin
  - ISO 27014:2013 là tiêu chuẩn thuộc chuỗi ISO 27000 về Quản trị An toàn Thông tin. Tài liệu ngắn đáng chú ý này (11 trang) cung cấp các khuyến nghị ngắn gọn để đánh giá một chương trình quản trị an toàn thông tin.

TỔNG QUAN VỀ QUẢN LÝ AN TOÀN THÔNG TIN

- Vai trò của việc xây dựng kế hoạch
- Xây dựng kế hoạch chiến lược
- Quản trị an toàn thông tin
- **Xây dựng kế hoạch triển khai đảm bảo ATTT**
- Câu hỏi ôn tập

Xây dựng kế hoạch triển khai đảm bảo ATTT…

- Việc triển khai ATTT thường được bắt đầu theo một trong hai cách: từ dưới lên hoặc từ trên xuống.



Xây dựng kế hoạch triển khai đảm bảo ATTT…

- Hướng tiếp cận từ trên xuống:
  - để thành công, quản lý cấp cao phải nỗ lực và cung cấp hỗ trợ đầy đủ cho tất cả các bộ phận
  - Sự tham gia và hỗ trợ của người dùng cuối cũng rất quan trọng đối với sự thành công này. Người dùng cuối chính cần được chỉ định cho các nhóm lập kế hoạch và thiết kế tương tự như nhóm thiết kế ứng dụng chung (JAD) được sử dụng trong phát triển hệ thống.
  - các quy trình và thủ tục phải được lập thành văn bản và tích hợp vào văn hóa tổ chức, phải được xác nhận, thúc đẩy và hỗ trợ bởi ban quản lý của tổ chức.

Trách nhiệm trong kế hoạch ATTT…

- Giám đốc Thông tin (CIO): chịu trách nhiệm phát triển và duy trì một chương trình ATTT toàn cơ quan và có các trách nhiệm sau đối với việc lập kế hoạch ATTT:
  - Chỉ định một nhân viên ATTT của cơ quan cấp cao (SAISO), người sẽ thực hiện trách nhiệm của CIO về lập kế hoạch ATTT
  - Phát triển và duy trì các CS, thủ tục và kỹ thuật kiểm soát ATTT để giải quyết việc lập kế hoạch ATTT
  - Quản lý việc xác định, thực hiện và đánh giá các biện pháp kiểm soát AT chung
  - Đảm bảo rằng nhân viên có vai trò quan trọng đối với các kế hoạch ATTT được đào tạo
  - Hỗ trợ các quan chức cơ quan cấp cao về trách nhiệm của họ đối với các kế hoạch ATTT
  - Xác định và điều phối các biện pháp kiểm soát AT chung cho tổ chức.

Trách nhiệm trong kế hoạch ATTT…

- Chủ sở hữu HTTT chịu trách nhiệm về việc mua sắm, phát triển, tích hợp, sửa đổi tổng thể hoặc vận hành và bảo trì HTTT:
  - Xây dựng kế hoạch ATTT với sự phối hợp của chủ sở hữu TT, người quản trị HT, nhân viên AT HTTT, nhân viên ATTT của cơ quan cấp cao và "người dùng cuối“
  - Duy trì kế hoạch ATTT và đảm bảo rằng HT được triển khai và vận hành theo các yêu cầu AT đã thỏa thuận
  - Đảm bảo rằng người dùng HT và nhân viên hỗ trợ nhận được khóa đào tạo AT cần thiết (ví dụ: hướng dẫn về các quy tắc hành vi)
  - Cập nhật kế hoạch ATTT bất cứ khi nào xảy ra thay đổi quan trọng
  - Hỗ trợ xác định, triển khai và đánh giá các biện pháp kiểm soát AT chung.

Trách nhiệm trong kế hoạch ATTT…

- Chủ sở hữu TT: có thẩm quyền theo luật định hoặc hoạt động đối với TT cụ thể và chịu trách nhiệm thiết lập các biện pháp kiểm soát đối với việc tạo ra, thu thập, xử lý, phổ biến, loại bỏ TT đó và có các trách nhiệm liên quan đến các kế hoạch ATTT sau:
  - Thiết lập các quy tắc để sử dụng và bảo vệ thích hợp dữ liệu/TT của đối tượng (các quy tắc hành vi)
  - Cung cấp đầu vào cho chủ sở hữu HTTT về các yêu cầu AT và kiểm soát AT đối với (các) HTTT chứa TT
  - Quyết định ai có quyền truy cập vào HTTT và với những loại đặc quyền hoặc quyền truy cập
  - Hỗ trợ xác định và đánh giá các biện pháp kiểm soát AT chung ở vị trí TT cư trú.

Trách nhiệm trong kế hoạch ATTT…

- Cán bộ ATTT của cơ quan cấp cao: chịu trách nhiệm là người liên lạc chính của CIO với chủ sở hữu HTTT của cơ quan và cán bộ AT HTTT:
  - Thực hiện các trách nhiệm của CIO đối với việc lập kế hoạch ATTT,
  - Phối hợp việc phát triển, xem xét và chấp nhận các kế hoạch ATTT với chủ sở hữu HTTT, cán bộ AT HTTT và quan chức có thẩm quyền,
  - Điều phối việc xác định, thực hiện và đánh giá các biện pháp kiểm soát an toàn chung,
  - Có trình độ chuyên môn, bao gồm đào tạo và kinh nghiệm, được yêu cầu để phát triển và xem xét các kế hoạch ATTT.

Trách nhiệm trong kế hoạch ATTT…

- Nhân viên ATTT là quan chức cơ quan được SAISO giao trách nhiệm, ủy quyền cho quan chức, viên chức quản lý hoặc chủ sở hữu HTTT để đảm bảo rằng trạng thái an toàn hoạt động thích hợp được duy trì cho một HT hoặc chương trình thông tin. Cán bộ ATTT có các trách nhiệm sau liên quan đến kế hoạch ATTT:
  - Hỗ trợ nhân viên ATTT của cơ quan cấp cao trong việc xác định, thực hiện và đánh giá các biện pháp kiểm soát an toàn chung,
  - Đóng vai trò tích cực trong việc phát triển và cập nhật kế hoạch ATTT cũng như phối hợp với chủ sở hữu HTTT bất kỳ thay đổi nào đối với HT và đánh giá tác động an toàn của những thay đổi đó.

Trách nhiệm trong kế hoạch ATTT…

- Cán bộ ủy quyền là quan chức quản lý cấp cao hoặc nhà điều hành có thẩm quyền chính thức đảm nhận trách nhiệm vận hành HTTT ở mức độ rủi ro có thể chấp nhận được đối với hoạt động của cơ quan, tài sản của cơ quan và có các trách nhiệm sau liên quan đến các kế hoạch AT:
  - Phê duyệt các kế hoạch AT HT
  - Cho phép vận hành HTTT
  - Cấp một ủy quyền tạm thời để vận hành HTTT theo các điều khoản và điều kiện cụ thể
  - Từ chối ủy quyền vận hành HTTT (hoặc nếu HT đã hoạt động thì tạm dừng hoạt động) nếu tồn tại các rủi ro AT không thể chấp nhận được.

Trách nhiệm trong kế hoạch ATTT

- Phê duyệt kế hoạch ATTT:
  - Chính sách tổ chức cần xác định rõ ai chịu trách nhiệm phê duyệt kế hoạch ATTT và các thủ tục được phát triển để đệ trình kế hoạch, bao gồm bất kỳ ngôn ngữ ghi nhớ đặc biệt nào hoặc tài liệu khác do cơ quan yêu cầu.
  - Viên chức cấp phép được chỉ định, độc lập với chủ sở hữu HT, thường phê duyệt kế hoạch.

Lập kế hoạch ATTT…

1. Tên và mã định danh HT
2. Phân loại hệ thống
3. Chủ sở hữu hệ thống
4. Ủy quyền chính thức
5. Địa chỉ liên hệ được chỉ định khác
6. Phân công trách nhiệm an toàn
7. Tình trạng hoạt động của HT
8. Loại hệ thống thông tin
9. Mô tả chung/Mục đích
10. Môi trường hệ thống
11. Kết nối hệ thống/Chia sẻ TT
12. Luật, Quy định và Chính sách ảnh hưởng đến Hệ thống
13. Lựa chọn kiểm soát an toàn
14. Kiểm soát an toàn tối thiểu
15. Ngày hoàn thành và phê duyệt
16. Duy trì kế hoạch an toàn hiện thời

2. Phân loại hệ thống

	KHẢ NĂNG TÁC ĐỘNG		
Mục tiêu an toàn	**THẤP**	**TRUNG BÌNH**	**CAO**
Bí mật: Duy trì các hạn chế được phép đối với quyền truy cập và tiết lộ TT, gồm các phương tiện để bảo vệ quyền riêng tư cá nhân và thông tin độc quyền.	Việc tiết lộ thông tin trái phép có thể được cho là sẽ có tác động bất lợi hạn chế đến hoạt động của tổ chức, tài sản của tổ chức hoặc cá nhân	Việc tiết lộ thông tin trái phép có thể gây ảnh hưởng xấu nghiêm trọng đến hoạt động của tổ chức, tài sản của tổ chức hoặc cá nhân.	Việc tiết lộ TT trái phép có thể gây ra tác động tiêu cực nghiêm trọng hoặc nghiêm trọng đến hoạt động của tổ chức, tài sản của tổ chức hoặc cá nhân.
Toàn vẹn Bảo vệ chống lại việc sửa đổi hoặc phá hủy TT không phù hợp, và bao gồm việc đảm bảo TT không bị từ chối và xác thực.	Việc sửa đổi hoặc phá hủy TT trái phép có thể sẽ có tác động bất lợi hạn chế đến hoạt động của tổ chức, tài sản của tổ chức hoặc cá nhân.	Việc sửa đổi hoặc phá hủy TT trái phép có thể gây ảnh hưởng xấu nghiêm trọng đến hoạt động của tổ chức, tài sản của tổ chức hoặc cá nhân.	Việc sửa đổi hoặc phá hủy trái phép TT có thể gây ra tác động bất lợi nghiêm trọng hoặc nghiêm trọng đến hoạt động của tổ chức, tài sản của tổ chức hoặc cá nhân.
Sẵn sàng Đảm bảo truy cập và sử dụng thông tin kịp thời và đáng tin cậy.	Việc gián đoạn truy cập hoặc sử dụng TT hoặc HTTT có thể sẽ có tác động bất lợi hạn chế đến hoạt động của tổ chức, tài sản của tổ chức hoặc cá nhân	Việc gián đoạn truy cập hoặc sử dụng TT hoặc HTTT có thể gây ảnh hưởng xấu nghiêm trọng đến hoạt động của tổ chức, tài sản của tổ chức hoặc cá nhân	Việc gián đoạn truy cập hoặc sử dụng TT hoặc HTTTcó thể gây ra tác động tiêu cực nghiêm trọng hoặc nghiêm trọng đến hoạt động của tổ chức, tài sản của tổ chức hoặc cá nhân

3. Chủ sở hữu hệ thống

- là đầu mối liên hệ chính (POC) của HT và chịu trách nhiệm điều phối các hoạt động vòng đời phát triển HT (SDLC) cụ thể cho HT.
- phải có kiến thức chuyên môn về các khả năng và chức năng của HT.
- Việc chỉ định chủ sở hữu HT phải được lập thành văn bản và kế hoạch phải bao gồm các thông tin liên hệ sau:
  - Tên
  - Tiêu đề
  - Đơn vị
  - Địa chỉ nhà
  - Số điện thoại
  - Địa chỉ email

4. Uỷ quyền chính thức

- Người ủy quyền phải được xác định trong kế hoạch AT cho mỗi hệ thống
- là người quản lý cấp cao, có thẩm quyền cho phép vận hành (công nhận) HTTT (ứng dụng chính hoặc hệ thống hỗ trợ chung) và chấp nhận rủi ro tồn tại liên quan đến HT
- Việc chỉ định phải được thực hiện bằng văn bản và trong kế hoạch phải bao gồm các TT liên hệ như chủ sở hữu HT.

5. Địa chỉ liên hệ được chỉ định khác

- bao gồm các nhân viên liên hệ chính khác, những người có thể giải quyết các thắc mắc liên quan đến đặc điểm và hoạt động của hệ thống
- Các thông tin bao gồm cho mỗi người giống như thông tin của Chủ sở hữu HT.

6. Phân công trách nhiệm an toàn

- trách nhiệm chung có thể được giao cho SAISO (Senior Agency Information Security Officer – cán bộ ATTT Cơ quan cấp cao)
- được hỗ trợ bởi một mạng con gồm các nhân viên an toàn được chỉ định cho từng thành phần chính
- Các nhân viên này có thể được ủy quyền để giải quyết các yêu cầu AT cho tất cả các HT trong phạm vi quyền hạn của họ
- trách nhiệm này phải được chính thức hóa bằng văn bản trong Bản mô tả vị trí của nhân viên hoặc bằng Bản ghi nhớ ủy quyền
- Thông tin liên hệ tương tự như Chủ sở hữu HT.

7. Tình trạng hoạt động của hệ thống

- Liệt kê các thành phần của hệ thống và trang thái bao phủ chính của từng thành phần này:
  - Đang vận hành - hệ thống đang trong quá trình sản xuất.
  - Đang phát triển - hệ thống đang được thiết kế, phát triển hoặc triển khai.
  - Đang trải qua một sửa đổi lớn - hệ thống đang trải qua một quá trình thay đổi hoặc chuyển đổi lớn.

8. Loại hệ thống thông tin

- chỉ rõ hệ thống là một ứng dụng chính hay hệ thống hỗ trợ chung.
- Nếu hệ thống chứa các ứng dụng nhỏ, hãy mô tả chúng trong phần Mô tả chung/Mục đích của kế hoạch.
- Nếu tổ chức có các danh mục bổ sung của các loại hệ thống thông tin, hãy sửa đổi mẫu để bao gồm các danh mục khác.

9. Mô tả chung/Mục đích

- mô tả ngắn gọn (một đến ba đoạn) về chức năng và mục đích của hệ thống (ví dụ: chỉ số kinh tế, hỗ trợ mạng cho một tổ chức, phân tích dữ liệu điều tra kinh doanh, hỗ trợ báo cáo mùa màng).
- Nếu là HT hỗ trợ chung: liệt kê tất cả các ứng dụng được hỗ trợ bởi HT hỗ trợ chung.
- Xác định xem ứng dụng có phải là ứng dụng chính hay không và bao gồm tên/số nhận dạng duy nhất, nếu có.
- Mô tả chức năng của từng ứng dụng và thông tin được xử lý. Bao gồm danh sách các tổ chức người dùng, dù là nội bộ hay bên ngoài tổ chức của chủ sở hữu HT.

10. Môi trường hệ thống

- mô tả chung ngắn gọn (một đến ba hình vẽ) về HT kỹ thuật. Bao gồm bất kỳ yếu tố môi trường hoặc kỹ thuật nào gây ra các lo ngại đặc biệt về an toàn, chẳng hạn như việc sử dụng Hỗ trợ kỹ thuật số cá nhân, công nghệ không dây, v.v.

11. Kết nối hệ thống/Chia sẻ thông tin

- Liên kết hệ thống là sự kết nối trực tiếp của hai hay nhiều hệ thống CNTT nhằm mục đích chia sẻ tài nguyên thông tin
- Cần có Thỏa thuận an toàn kết nối (ISA), Biên bản ghi nhớ (MOU) hoặc Biên bản thỏa thuận (MOA) giữa các hệ thống (không phải giữa các máy trạm/máy tính để bàn hoặc các hệ thống được truy cập công khai) chia sẻ dữ liệu do các tổ chức khác nhau sở hữu hoặc vận hành.

11. Kết nối hệ thống/Chia sẻ thông tin…

- đối với mỗi kết nối giữa các HT do các tổ chức khác nhau sở hữu hoặc vận hành: cung cấp thông tin sau liên quan đến việc cho phép kết nối với các HT khác hoặc chia sẻ thông tin:
  - Tên hệ thống;
  - Tổ chức;
  - Loại kết nối (Internet, Dial-Up, v.v.);
  - Giấy phép kết nối (MOU / MOA, ISA);
  - Ngày thỏa thuận;
  - Danh mục FIPS 199;
  - Tình trạng chứng nhận và công nhận của hệ thống; và
  - Tên và chức danh của Người ủy quyền.

12. Luật, Quy định và Chính sách ảnh hưởng đến HT

- Liệt kê bất kỳ luật, quy định hoặc chính sách nào thiết lập các yêu cầu cụ thể về tính bí mật, tính toàn vẹn hoặc tính sẵn sàng của hệ thống và thông tin được hệ thống lưu giữ, truyền đi hoặc xử lý.
- Các yêu cầu AT chung của tổ chức không cần được liệt kê vì chúng yêu cầu AT cho tất cả các HT.
- Mỗi tổ chức nên quyết định mức độ luật, quy định và chính sách để đưa vào kế hoạch AT.

13. Lựa chọn kiểm soát an toàn

- Quá trình lựa chọn các biện pháp kiểm soát an toàn thích hợp và áp dụng các hướng dẫn về phạm vi để đạt được độ an toàn thích hợp là một hoạt động đa diện, dựa trên rủi ro liên quan đến các nhân viên quản lý và vận hành trong cơ quan và cần được tiến hành trước khi phần kiểm soát an toàn của kế hoạch được viết ra.
- Chọn đường cơ sở kiểm soát an toàn tối thiểu thích hợp (tác động thấp, trung bình, cao) từ NIST SP 800-53.

14. Kiểm soát an toàn tối thiểu

- Mô tả kiểm soát an toàn:
  - Tiêu đề kiểm soát an toàn;
  - Cách thức kiểm soát AT đang được thực hiện hoặc lên kế hoạch thực hiện như thế nào;
  - Hướng dẫn xác định phạm vi nào đã được áp dụng và loại hình xem xét;
  - Kiểm soát an toàn có phải là kiểm soát chung hay không và ai chịu trách nhiệm thực hiện.

15. Ngày hoàn thành và phê duyệt

- Ngày hoàn thành kế hoạch AT phải được cung cấp
- nên được cập nhật bất cứ khi nào kế hoạch được xem xét và cập nhật định kỳ.
- Kế hoạch AT cũng phải có ngày mà người ủy quyền hoặc cơ quan phê duyệt được chỉ định phê duyệt kế hoạch.
- Kế hoạch phải bao gồm: Tài liệu phê duyệt, tức là, thư công nhận, bản ghi nhớ phê duyệt.

16. Duy trì kế hoạch AT hiện thời

- điều quan trọng là phải định kỳ đánh giá kế hoạch, xem xét mọi thay đổi về trạng thái hệ thống, chức năng, thiết kế, v.v. và đảm bảo rằng kế hoạch tiếp tục phản ánh thông tin chính xác về HT.
- Một số nội dung trong đánh giá:
  - Thay đổi chủ sở hữu HTTT;
  - Thay đổi người đại diện ATTT;
  - Thay đổi kiến trúc HT;
  - Thay đổi trạng thái HT;
  - Thêm/xóa các kết nối HT;
  - Thay đổi phạm vi HT;
  - Thay đổi cán bộ ủy quyền; và
  - Thay đổi trạng thái chứng nhận và công nhận.

Mẫu kế hoạch an toàn thông tin

1. Tên/Định danh HTTT
2. Phân loại HTTT:

	LOW		MODERATE		HIGH

3. Chủ sở hữu HTTT
4. Cán bộ ủy quyền
5. Các liên hệ được chỉ định khác
6. Phân công trách nhiệm AT
7. Tình trạng hoạt động của HTTT

	Operational		Under Development		Major Modification

8. Loại hệ thống thông tin

	Major Application		General Support System

9. Mô tả chung/Mục đích
10. Môi trường HT
11. Kết nối hệ thống/Chia sẻ TT

System Name	Organization	Type	Agreement (ISA/MOU/MOA)	Date	FIPS 199 Category	C&A Status	Auth. Official

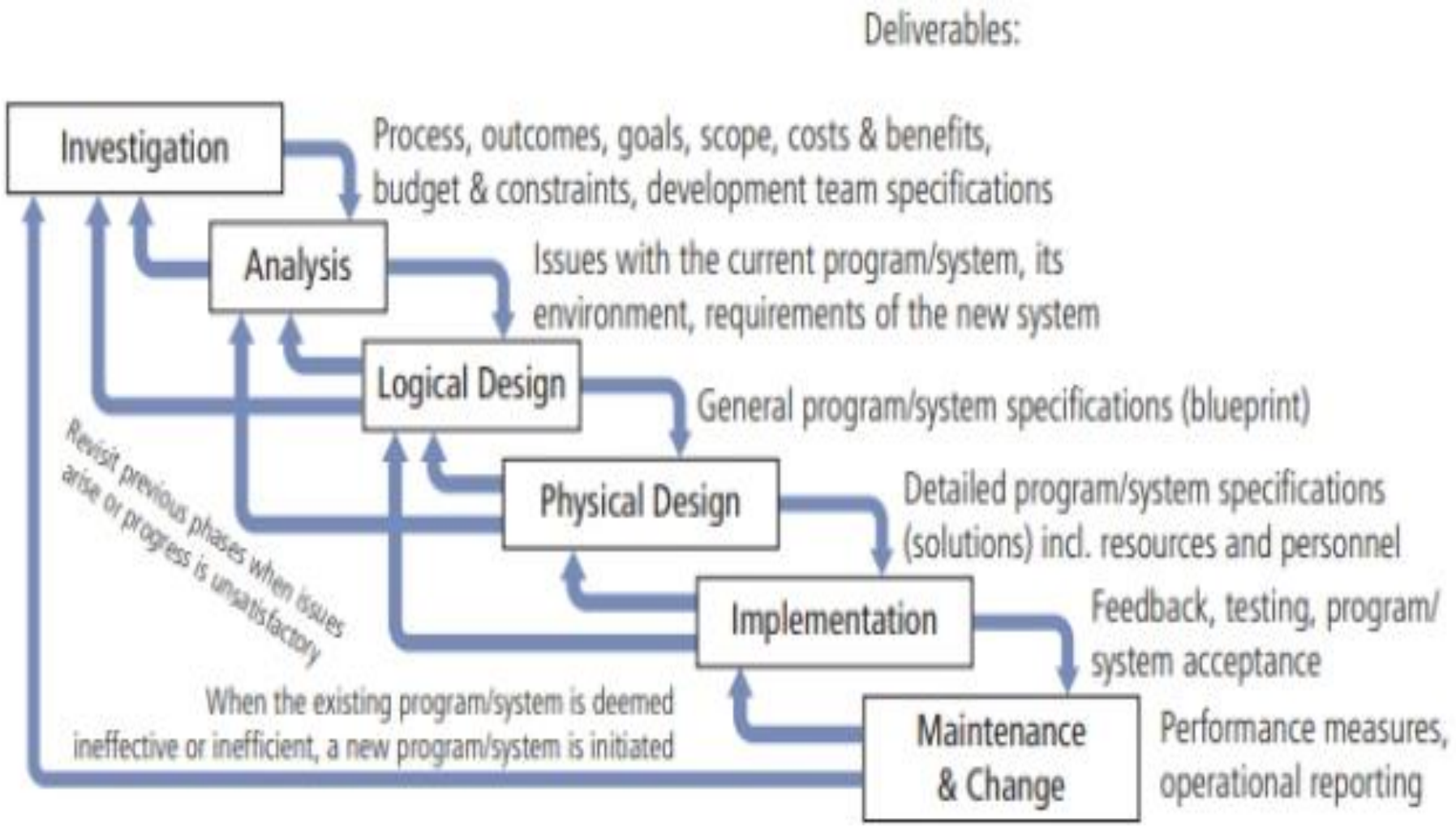
12. Luật/Quy định/CS liên quan
13. Kiểm soát an toàn tối thiểu
14. Ngày hoàn thành kế hoạch ATTT: ___
15. Ngày Phê duyệt Kế hoạch ATTT:

Xây dựng kế hoạch triển khai đảm bảo ATTT…

- Thành công của kế hoạch ATTT có thể được nâng cao bằng cách sử dụng các quy trình phân tích và thiết kế hệ thống.
- Vòng đời phát triển hệ thống (SDLC) là một phương pháp luận để thiết kế và triển khai hệ thống thông tin trong một tổ chức. Quá trình phát triển hệ thống theo từng giai đoạn được mô tả bởi SDLC truyền thống có thể được điều chỉnh để hỗ trợ việc triển khai chuyên biệt của một dự án an toàn bằng cách sử dụng **vòng đời phát triển hệ thống an toàn (SecSDLC)**.

Xây dựng kế hoạch triển khai đảm bảo ATTT…

- SecSDLC



Xây dựng kế hoạch triển khai đảm bảo ATTT…

- Giai đoạn Khảo sát:
  - bắt đầu với chỉ thị của quản lý cấp trên xác định rõ quy trình, kết quả và mục tiêu của dự án, cũng như ngân sách và các ràng buộc khác của dự án.
  - giai đoạn này bắt đầu với việc xác nhận hoặc tạo ra các chính sách an toàn mà chương trình an toàn của tổ chức đang hoặc sẽ được thành lập.
  - Các nhóm gồm các nhà quản lý, nhân viên và chuyên gia tư vấn được tập hợp để khảo sát các vấn đề, xác định phạm vi hoạt động, xác định các mục tiêu cũng như xác định bất kỳ ràng buộc bổ sung nào không được đề cập trong chính sách an toàn của tổ chức.
  - phân tích tính khả thi của tổ chức: xác định xem tổ chức có đủ nguồn lực và cam kết để thực hiện phân tích và thiết kế an toàn thành công hay không.

Xây dựng kế hoạch triển khai đảm bảo ATTT…

- Giai đoạn phân tích…:
  - nghiên cứu các tài liệu từ giai đoạn khảo sát
  - phân tích sơ bộ các CS hoặc chương trình AT hiện có, cùng với các mối đe dọa hiện tại đã được lập thành văn bản và các biện pháp kiểm soát liên quan.
  - phân tích các vấn đề pháp lý liên quan có thể ảnh hưởng đến thiết kế của giải pháp AT
  - Nhiệm vụ **quản lý rủi ro** cũng bắt đầu trong giai đoạn này. Quản lý rủi ro là quá trình xác định, đánh giá các mức độ rủi ro mà tổ chức phải đối mặt - cụ thể là các mối đe dọa đối với an toàn của tổ chức và đối với thông tin được tổ chức lưu trữ và xử lý

Xây dựng kế hoạch triển khai đảm bảo ATTT…

- Giai đoạn phân tích:
  - Nhiệm vụ tiếp theo là **đánh giá rủi ro** tương đối đối với từng tài sản thông tin thông qua một quá trình được gọi là đánh giá rủi ro. Đánh giá rủi ro ấn định xếp hạng rủi ro so sánh hoặc điểm số cho từng tài sản thông tin cụ thể.

Xây dựng kế hoạch triển khai đảm bảo ATTT…

- Giai đoạn thiết kế…:
  - thiết kế logic: các bản thiết kế an toàn được tạo ra và các **chính sách** quan trọng được kiểm tra và thực hiện. Ở giai đoạn này, các **kế hoạch dự phòng** quan trọng để ứng phó sự cố được phát triển. Tiếp theo, phân tích tính khả thi xác định xem dự án có nên tiếp tục tự thực hiện hay nên thuê ngoài.
  - thiết kế vật lý: công nghệ an toàn cần thiết để hỗ trợ các bản thiết kế này được đánh giá, các giải pháp thay thế được tạo ra, và một thiết kế cuối cùng được xác định. Tiếp tục, phân tích tính khả thi về mức độ sẵn sàng của tổ chức đối với dự án được đề xuất, sau đó giám đốc điều hành cấp cao và người sử dụng sẽ được trình bày với thiết kế (các bên có cơ hội phê duyệt (hoặc không phê duyệt) dự án trước khi bắt đầu triển khai).

Xây dựng kế hoạch triển khai đảm bảo ATTT…

- Giai đoạn thiết kế…:
  - CSATTT: một tập hợp các quy tắc bảo vệ tài sản của tổ chức, cung cấp hướng dẫn và các yêu cầu để bảo vệ tài sản thông tin của tổ chức. Có ba loại: CSATTT tổ chức hoặc chung, CSATTT các vấn đề cụ thể (ISSP) và CSATTT hệ thống cụ thể.
  - Chương trình SETA (security education, training, and awareness) là một biện pháp kiểm soát được thiết kế để giảm các vi phạm an toàn ngẫu nhiên của nhân viên.
  - xây dựng các biện pháp kiểm soát được sử dụng để bảo vệ TT khỏi các cuộc tấn công bởi các mối đe dọa, Có ba loại kiểm soát:
    - Kiểm soát quản lý: các quy trình AT được thiết kế bởi các nhà hoạch định chiến lược và được thực thi bởi cơ quan quản lý AT của tổ chức.
    - Kiểm soát hoạt động liên quan đến chức năng hoạt động AT trong tổ chức.
    - Kiểm soát kỹ thuật đề cập đến các phương pháp tiếp cận kỹ thuật được sử dụng để thực hiện AT trong tổ chức.

Xây dựng kế hoạch triển khai đảm bảo ATTT…

- Giai đoạn thiết kế:
  - tạo ra các tài liệu chuẩn bị cần thiết: kế hoạch dự phòng (bao gồm kế hoạch liên tục kinh doanh, kế hoạch khắc phục thảm họa và kế hoạch ứng phó sự cố)
  - An toàn vật lý: đòi hỏi thiết kế, triển khai và duy trì các biện pháp đối phó để bảo vệ các nguồn lực vật lý của một tổ chức. Tài nguyên vật lý bao gồm con người, phần cứng và các yếu tố hệ thống hỗ trợ và các tài nguyên liên quan đến việc quản lý thông tin ở tất cả các trạng thái của nó - truyền, lưu trữ và xử lý.

Xây dựng kế hoạch triển khai đảm bảo ATTT…

- Giai đoạn triển khai…:
  - Các giải pháp an toàn được mua (thực hiện hoặc mua), thử nghiệm, triển khai và thử nghiệm lại.
  - Các vấn đề về nhân sự được đánh giá và các chương trình đào tạo và giáo dục cụ thể được thực hiện.
  - Cuối cùng, toàn bộ gói đã kiểm tra được trình lên quản lý cấp trên để phê duyệt lần cuối.

Xây dựng kế hoạch triển khai đảm bảo ATTT…

- Giai đoạn triển khai:
  - yếu tố quan trọng nhất của giai đoạn triển khai là quản lý kế hoạch dự án. Việc thực hiện kế hoạch dự án tiến hành theo ba bước:
    1. Lập kế hoạch dự án
    2. Giám sát các nhiệm vụ và các bước hành động trong kế hoạch dự án
    3. Tóm tắt kế hoạch dự án

Xây dựng kế hoạch triển khai đảm bảo ATTT

- Giai đoạn bảo trì là giai đoạn quan trọng nhất, do tính linh hoạt và tính bền bỉ của nhiều mối đe dọa mà tổ chức phải đối mặt.
  - Các hệ thống An toàn thông tin cần theo dõi, kiểm tra, sửa đổi, cập nhật và sửa chữa liên tục
  - Nếu không điều chỉnh thích hợp với những thay đổi của môi trường bên trong hoặc bên ngoài, có thể cần phải bắt đầu lại chu trình.

TỔNG QUAN VỀ QUẢN LÝ AN TOÀN THÔNG TIN

- Vai trò của việc xây dựng kế hoạch
- Xây dựng kế hoạch chiến lược
- Quản trị an toàn thông tin
- Xây dựng kế hoạch triển khai đảm bảo ATTT
- **Câu hỏi ôn tập**

Câu hỏi cuối chương…

- Câu 1. Lập kế hoạch là gì?
- Câu 2. Chiến lược là gì?
- Câu 3. Quản trị An toàn thông tin là gì?
- Câu 4. Năm kết quả cơ bản cần đạt được thông qua quản trị ATTT là gì?

Câu hỏi cuối chương…

- Câu 5. Mô tả hoạch định chiến lược từ trên xuống. Nó khác với hoạch định chiến lược từ dưới lên như thế nào? Cách nào thường hiệu quả hơn trong việc triển khai an toàn trong một tổ chức lớn, đa dạng?
- Câu 6. SecSDLC khác với SDLC chung như thế nào?
- Câu 7. Mục tiêu chính của SecSDLC là gì? Các bước chính của nó là gì và mục tiêu chính của mỗi bước là gì?

Câu hỏi cuối chương

- Câu 8. Kiểm soát quản lý là gì? Kiểm soát an toàn hoạt động là gì? Kiểm soát an toàn kỹ thuật là gì?
- Câu 9. Hãy nêu những trách nhiệm trong Xây dựng kế hoạch ATTT.
- Câu 10. Tại sao cần bảo trì đối với hệ thống quản lý an toàn thông tin?
- Câu 11. Các nội dung chính trong một kế hoạch ATTT là gì?

HỌC VIỆN KỸ THUẬT MẬT MÃ
AN TOÀN THÔNG TIN

Thank You!