QUẢN LÝ AN TOÀN THÔNG TIN

BÀI 2:
LẬP KẾ HOẠCH AN TOÀN THÔNG TIN

Nội dung

- Giới thiệu về An toàn thông tin
  - Tam giác CIA và các phần mở rộng
  - Nguyên tắc quản lý an toàn thông tin
- Lập kế hoạch an toàn thông tin

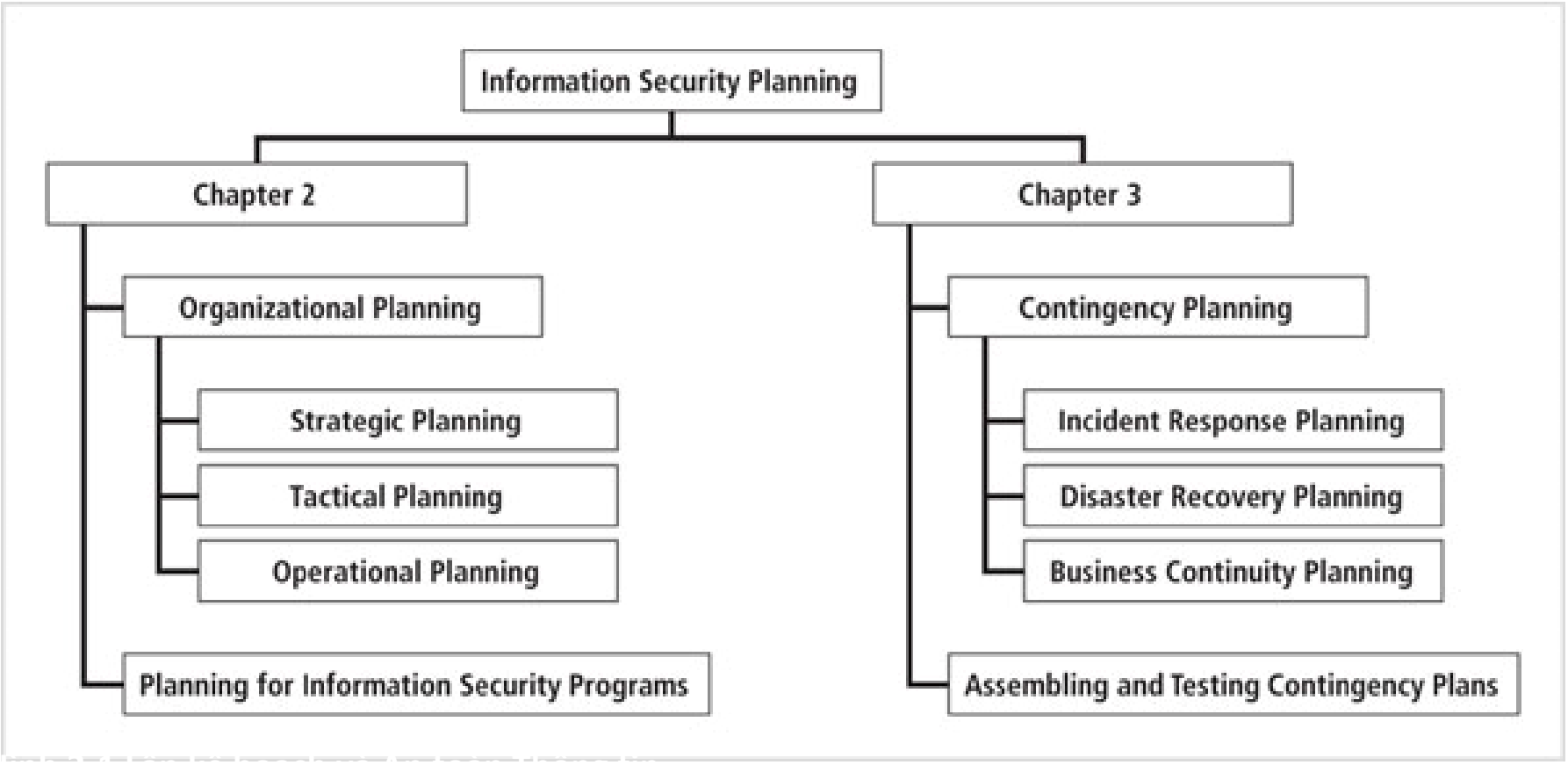
Nguyên tắc quản lý ATTT

Các đặc điểm sau sẽ là trọng tâm của khóa học hiện tại (sáu chữ P):

1. Lập kế hoạch Chương 2 & 3
2. Chính sách
3. Các chương trình
4. Sự bảo vệ
5. Con người
6. Quản lý dự án

http://csrc.nist.gov/publications/PubsTC.html

Lập kế hoạch an toàn thông tin



Vai trò của lập kế hoạch

- Các tổ chức thành công đều sử dụng kế hoạch

- Lập kế hoạch liên quan đến
  - Nhân viên
  - Ban quản lý
  - Cổ đông
  - Các bên liên quan khác bên ngoài công ty
  - Môi trường vật lý và công nghệ
  - Môi trường chính trị và luật pháp
  - Môi trường cạnh tranh

Vai trò của Lập kế hoạch (tiếp theo)

- Hoạch định chiến lược bao gồm:
  - Tầm nhìn chiến lược
  - Tuyên bố sứ mệnh
  - Chiến lược
  - Các kế hoạch phối hợp cho các đơn vị con

Các việc cần làm trước khi lập kế hoạch

- Tuyên bố giá trị
  - Thiết lập các nguyên tắc tổ chức
- Tầm nhìn chiến lược
  - Điều mà tổ chức muốn trở thành
- Tuyên bố sứ mệnh
  - tổ chức làm gì và cho ai

Các giá trị, tầm nhìn và tuyên bố sứ mệnh cùng nhau cung cấp nền tảng cho việc lập kế hoạch

Our company
Stay informed about Microsoft – from company facts and news to our worldwide locations and more.

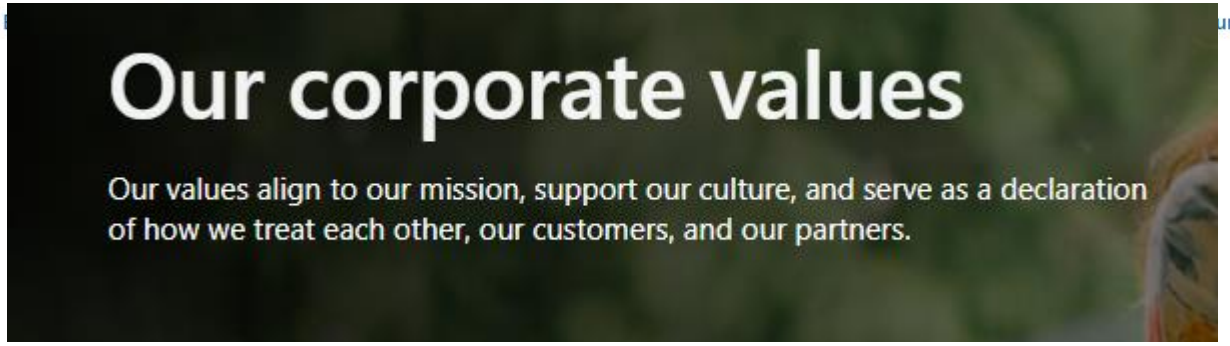
Who we are
Get to know some of our people, explore engaging stories, and meet the leaders who shape our vision.

What we value
See how we utilize technology to build platforms and resources to help make a lasting positive impact.

ur values >

Contact us
Get in touch. We're here

Get the support you ne



Các việc cần làm trước khi lập kế hoạch

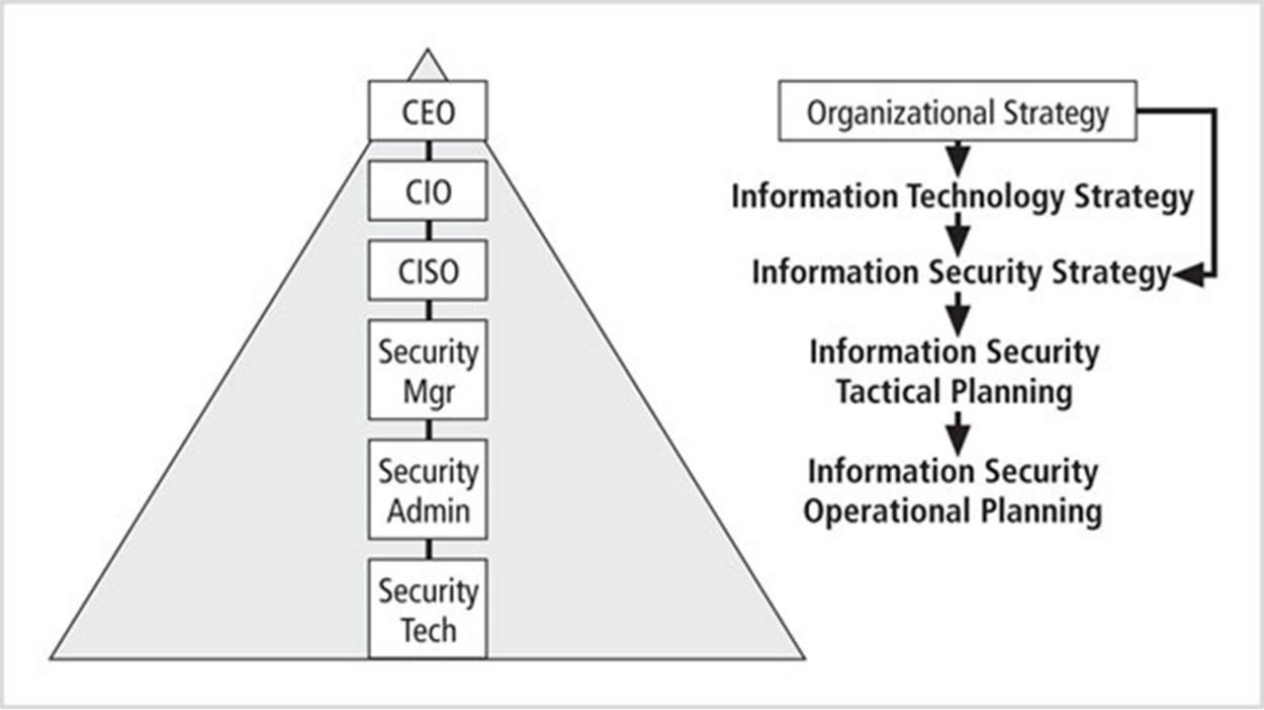
- Tuyên bố sứ mệnh
  - tổ chức làm gì và cho ai

Bộ phận An toàn Thông tin chịu trách nhiệm xác định, đánh giá và quản lý thích hợp các rủi ro đối với hệ thống thông tin và thông tin của Công ty X. Nó đánh giá các phương án để đối phó với những rủi ro này, và làm việc với các bộ phận trong toàn Công ty X để quyết định và sau đó thực hiện các phương án ứng phó một cách thích hợp và chủ động với những rủi ro tương tự. Bộ phận cũng chịu trách nhiệm phát triển các yêu cầu áp dụng cho toàn bộ tổ chức cũng như các hệ thống thông tin bên ngoài mà Công ty X có trách nhiệm sử dụng (ví dụ: các mạng bên ngoài) [các yêu cầu này bao gồm các chính sách, tiêu chuẩn và thủ tục]. Đầu mối cho tất cả các vấn đề liên quan đến bảo mật thông tin, Bộ phận này chịu trách nhiệm cuối cùng về tất cả các nỗ lực trong Công ty X nhằm tránh, ngăn chặn, phát hiện, sửa chữa hoặc phục hồi khỏi các mối đe dọa đối với thông tin hoặc hệ thống thông tin.

Information Security Roles and Responsibilities Made Easy, by Charles Cresson Wood.

Lập kế hoạch chiến lược

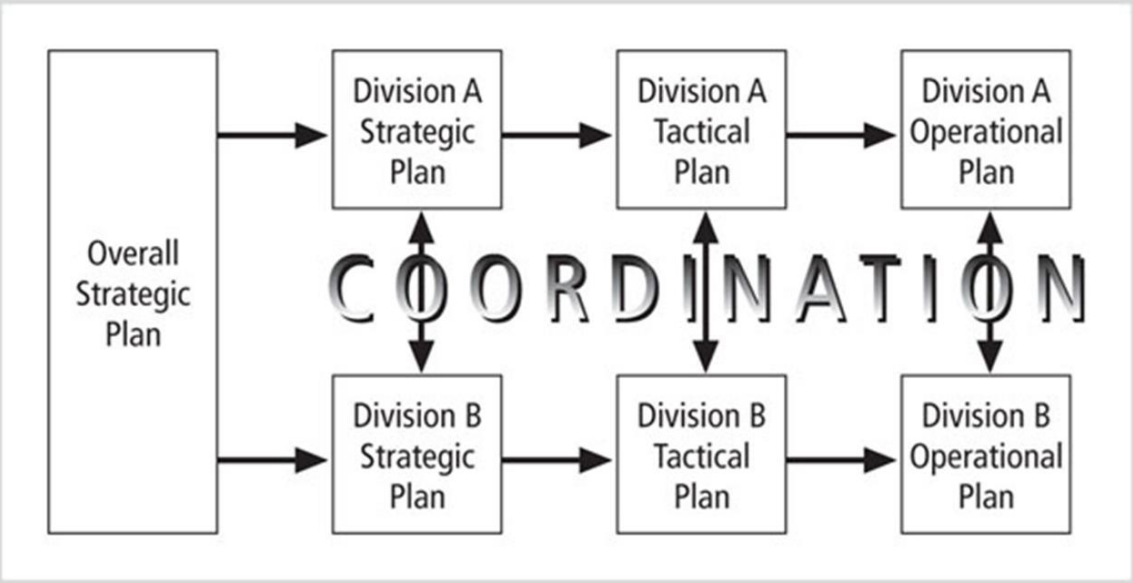
- Chiến lược là cơ sở để định hướng lâu dài
- Lập kế hoạch chiến lược dẫn hướng cho các nỗ lực của tổ chức



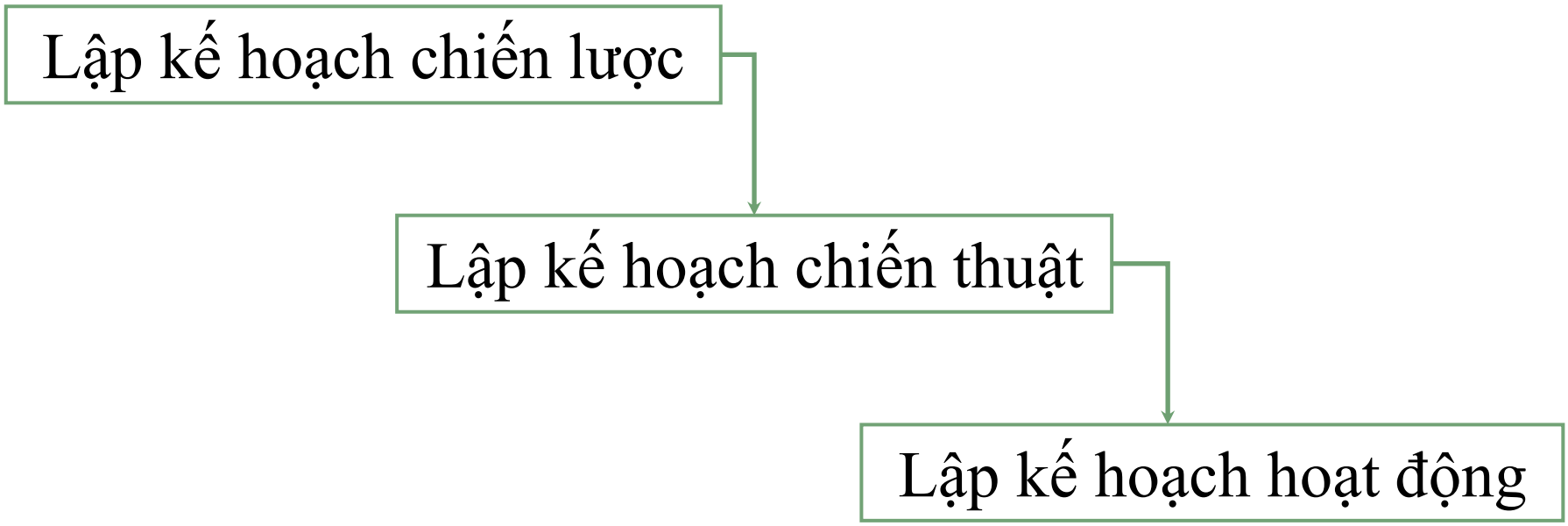
Các cấp độ lập kế hoạch

- Các mục tiêu chiến lược được chuyển thành các nhiệm vụ
  - Mục tiêu phải **SMART**

- Sau đó, Kế hoạch chiến lược bắt đầu chuyển đổi từ các mục tiêu chung sang các mục tiêu cụ thể



Các cấp độ lập kế hoạch (tiếp theo)



Lập kế hoạch và CISO

- Các yếu tố của một kế hoạch chiến lược
  - Tóm tắt điều hành
  - Tuyên bố sứ mệnh và tuyên bố tầm nhìn
  - Hồ sơ và lịch sử tổ chức
  - Các vấn đề chiến lược và giá trị cốt lõi
  - Mục đích và mục tiêu của chương trình
  - Mục đích và mục tiêu quản lý / hoạt động
  - Phụ lục (tùy chọn) [điểm mạnh, điểm yếu, cơ hội và mối đe dọa (SWOT) phân tích, khảo sát, ngân sách, v.v.]

Quản trị An toàn Thông tin

- Quản trị an toàn thông tin là một trách nhiệm hoạch định chiến lược
  - Tầm quan trọng tăng lên trong những năm gần đây

- Các mục tiêu an toàn thông tin phải được giải quyết ở cấp cao nhất của đội ngũ quản lý của tổ chức
  - Để có hiệu quả và cung cấp một cách tiếp cận bền vững

Kết quả mong muốn

Liên kết chiến lược

Quản lý rủi ro

Quản lý nguồn tài nguyên

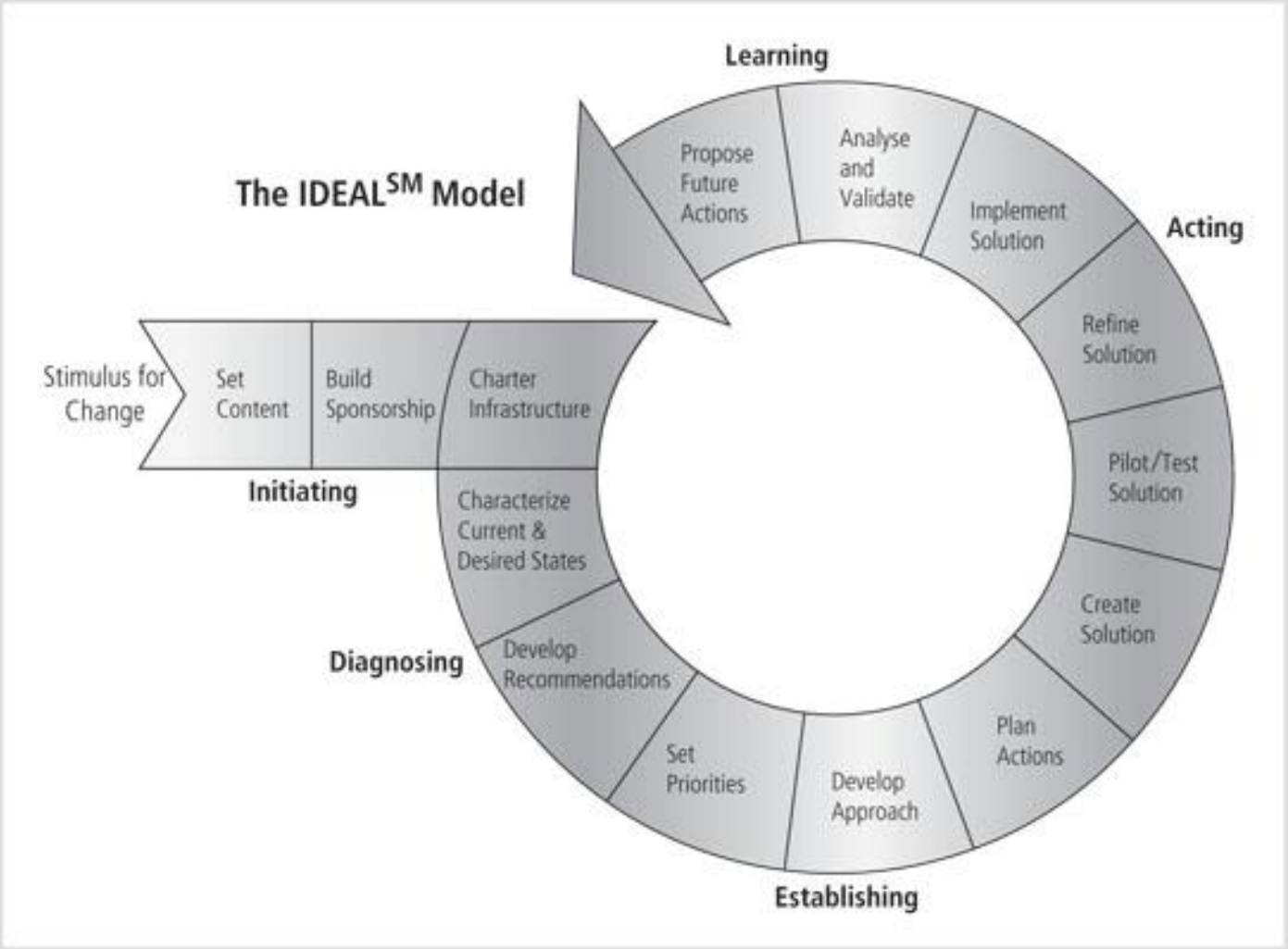
Đo lường hiệu suất

Phân phối giá trị

Thực hiện quản trị an toàn thông tin

I	**Initiating**	Lay the groundwork for a successful improvement effort.
D	**Diagnosing**	Determine where you are relative to where you want to be.
E	**Establishing**	Plan the specifics of how you will reach your destination.
A	**Acting**	Do the work according to the plan.
L	**Learning**	Learn from the experience and improve your ability to adopt new improvements in the future.

Thực hiện Quản trị An toàn thông tin (tiếp theo)

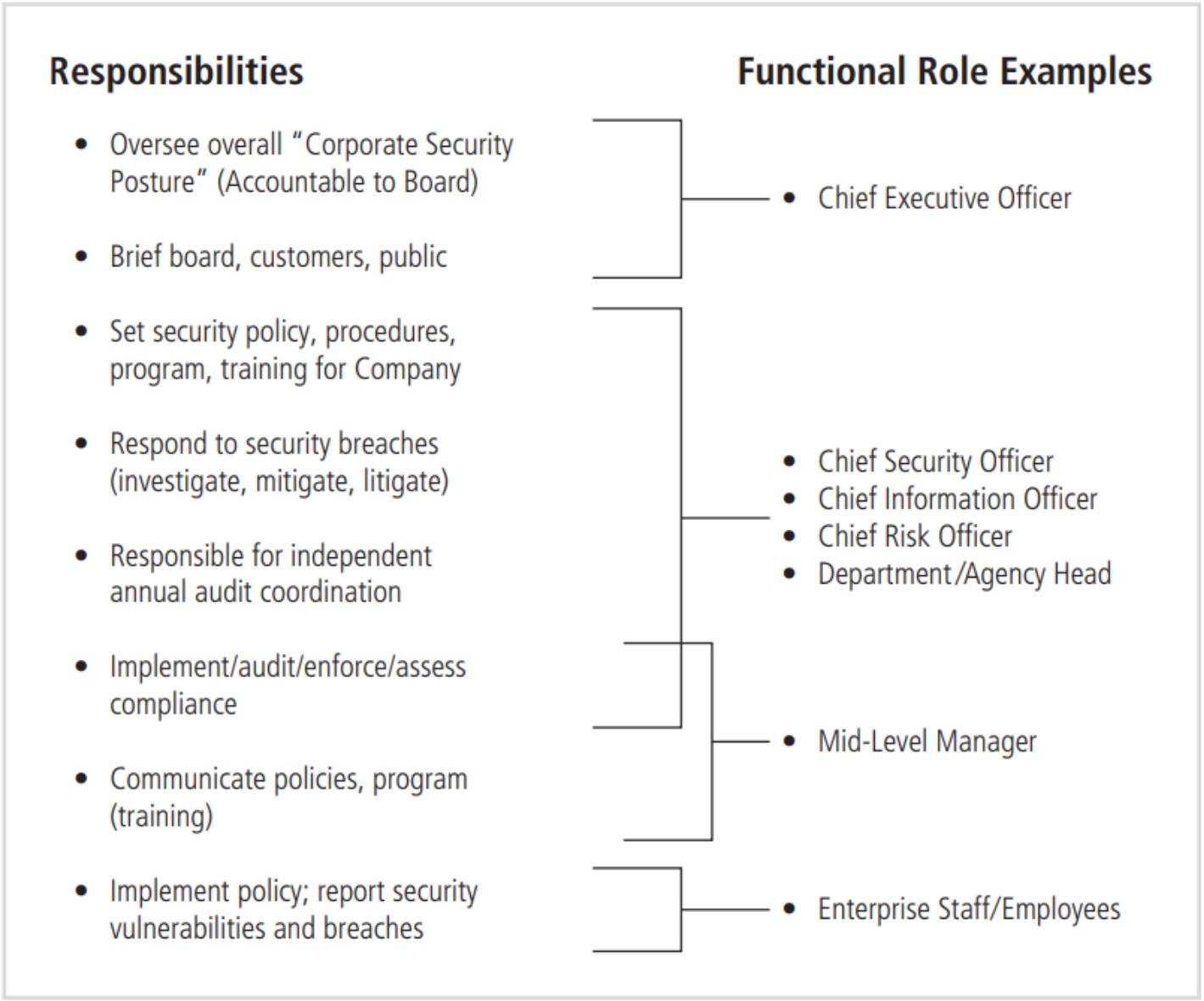


GRC Điều 1: Forrestor Framework

- Các tuyến phòng thủ

- Đóng góp và kỳ vọng của các bên liên quan

Thực hiện Quản trị An toàn thông tin (tiếp theo)

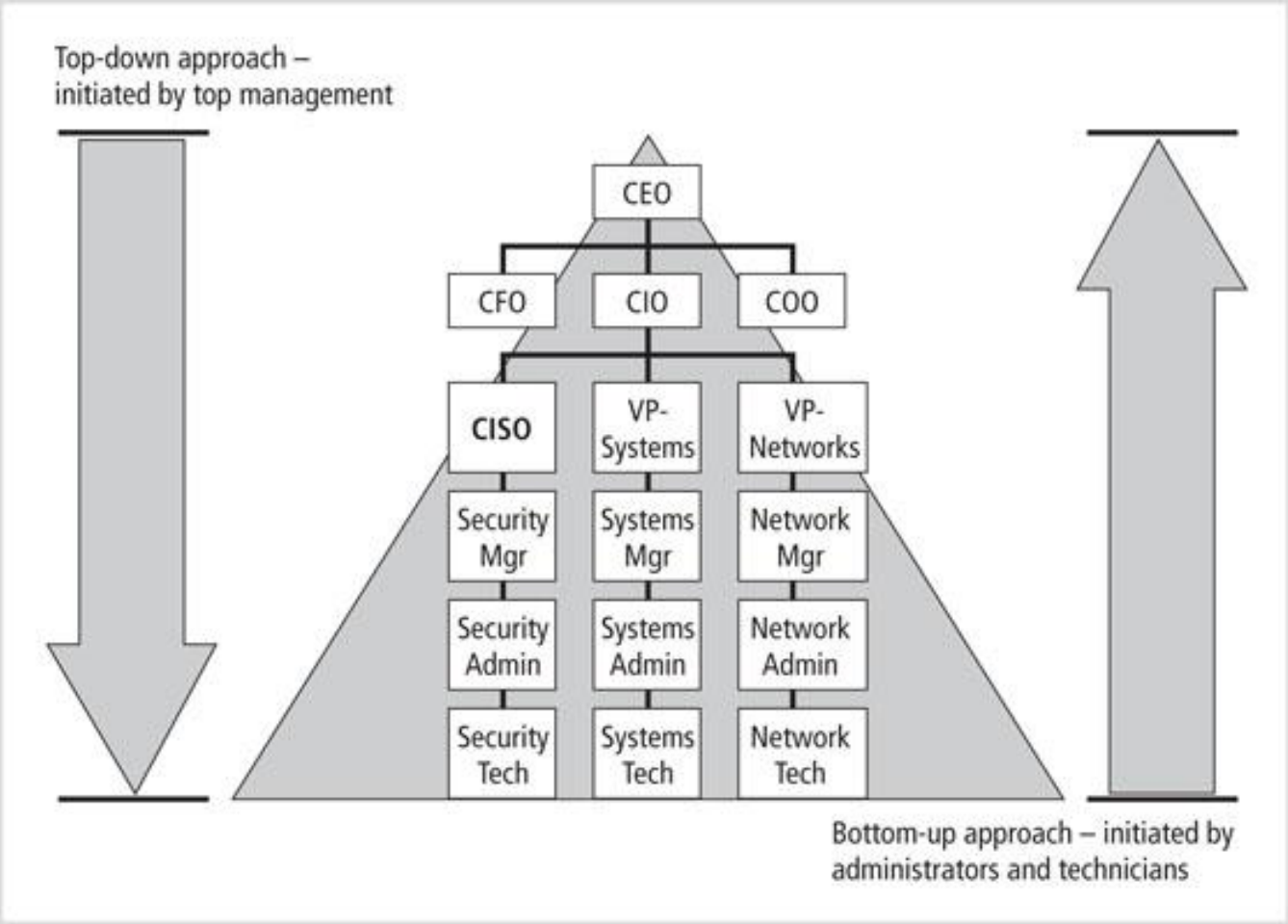


Lập kế hoạch triển khai an toàn thông tin

- Việc triển khai có thể bắt đầu
  - Sau khi kế hoạch đã được chuyển thành các mục tiêu CNTT và an toàn thông tin, và các kế hoạch chiến thuật và hoạt động

- Phương pháp thực hiện
  - Từ dưới lên
  - Từ trên xuống

Lập kế hoạch triển khai an toàn thông tin (tiếp theo)



Vòng đời phát triển hệ thống

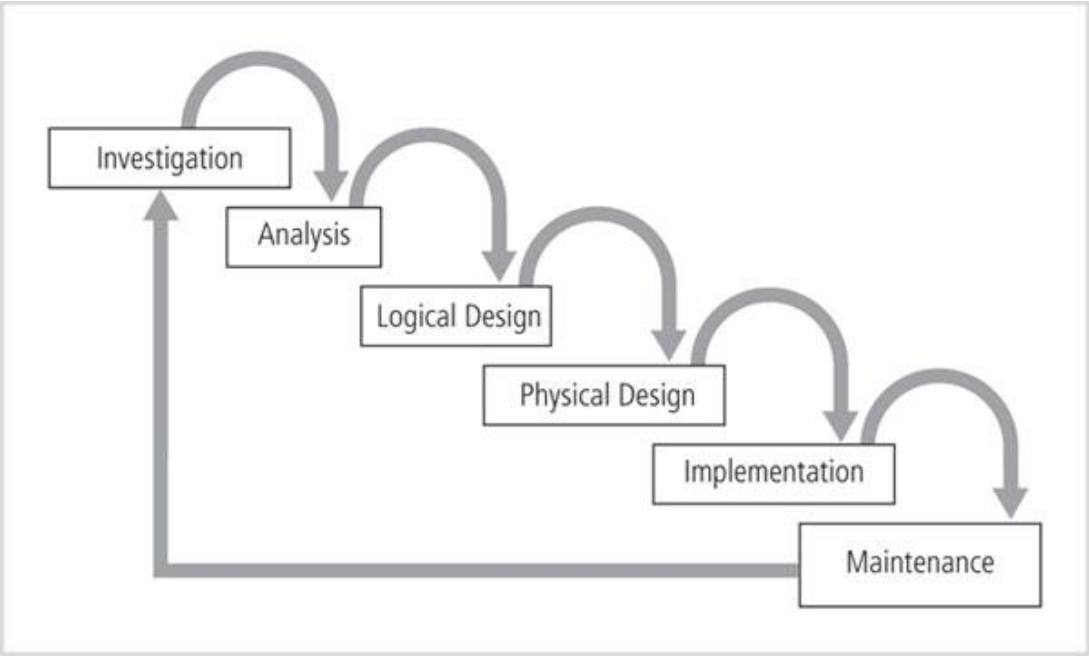
- Phương pháp luận để thiết kế / triển khai hệ thống thông tin

- Phương pháp SecSDLC tương tự như SDLC

Vòng đời phát triển hệ thống an ninh

Xác định các mối đe dọa cụ thể và rủi ro mà chúng đại diện

Thiết kế và thực hiện các biện pháp kiểm soát cụ thể để chống lại những mối đe dọa đó và quản lý rủi ro gây ra cho tổ chức

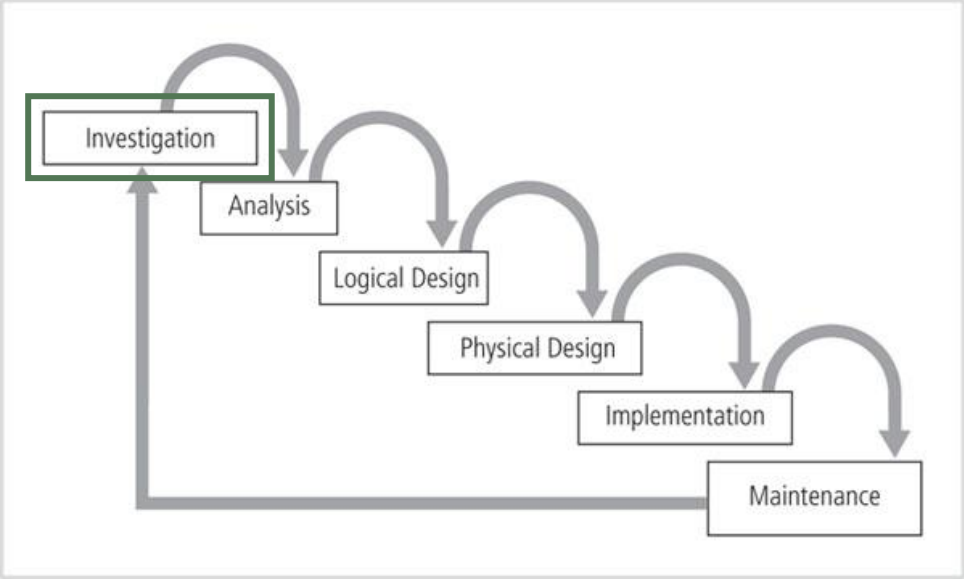


SecSDLC: Điều tra

Giai đoạn bắt đầu với chỉ thị của ban quản lý cụ thể hóa quá trình, kết quả và mục đích của dự án cùng với ngân sách được cấp

Phân tích tính khả thi

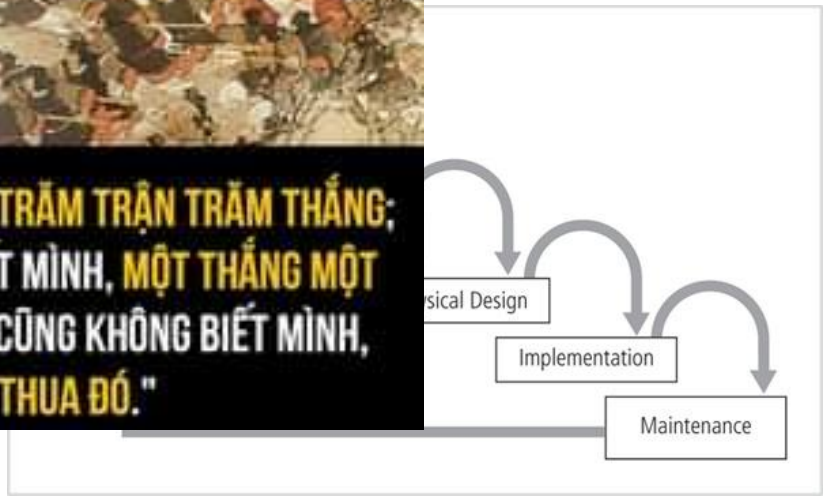
- Xác định xem tổ chức có đủ nguồn lực và cam kết để thực hiện phân tích và thiết kế bảo mật thành công hay không



SecSDLC: Phân tích

Chuẩn bị phân tích các chính sách và chương trình bảo mật hiện có, cùng với các mối đe dọa đã biết và các biện pháp kiểm soát hiện tại

Phân tích các vấn đ ; đến thiết kế của giải pháp bả



SecSDLC: Phân tích

Chuẩn bị phân tích các chính sách và chương trình bảo mật hiện có, cùng với các mối đe dọa đã biết và các biện pháp kiểm soát hiện tại

Phân tích các vấn đề pháp lý liên quan có thể ảnh hưởng đến thiết kế của giải pháp bảo mật

Categories of threat	Examples
1. Acts of human error or failure	Accidents, employee mistakes
2. Compromises to intellectual property	Piracy, copyright infringement
3. Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
4. Deliberate acts of information extortion	Blackmail of information disclosure
5. Deliberate acts of sabotage or vandalism	Destruction of systems or information
6. Deliberate acts of theft	Illegal confiscation of equipment or information
7. Deliberate software attacks	Viruses, worms, macros, denial-of-service
8. Deviations in quality of service from service providers	Power and WAN service issues
9. Forces of nature	Fire, flood, earthquake, lightning
10. Technical hardware failures or errors	Equipment failure
11. Technical software failures or errors	Bugs, code problems, unknown loopholes
12. Technological obsolescence	Antiquated or outdated technologies

Bảng: Các mối đe dọa đối với an ninh thông tin

Phân tích SecSDLC: Các mối đe dọa đối với ATTT

Ví dụ:bản vá các lỗ hổng Java
….và một tuần sau đó

Phân tích SecSDLC: Các cuộc tấn công phổ biến

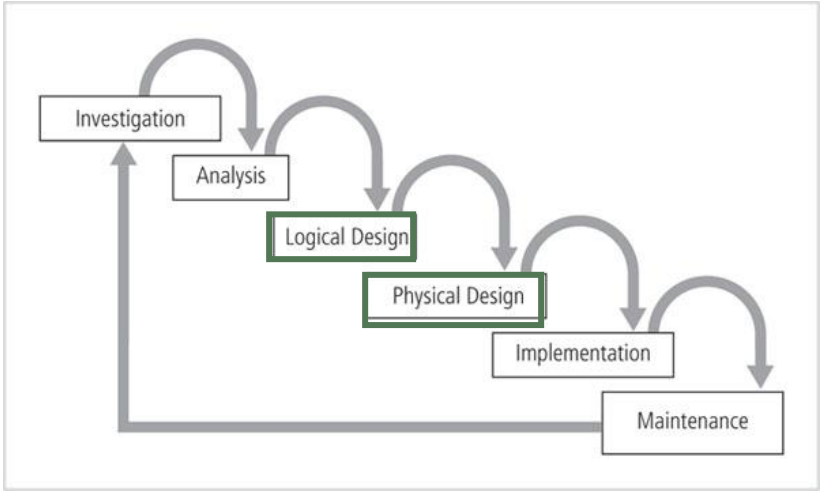
- Mã độc
- Hoax
- Cửa hậu
- Crack mật khẩu
  - Vét cạn
  - Từ điển
- Từ chối dịch vụ (DoS) và từ chối dịch vụ phân tán (DDoS)
- Giả mạo
- Man-in-the-middle
- Thư rác
- Đánh bom thư
- Nghe trộm
- Kỹ thuật lừa đảo
- Tràn bộ nhớ đệm
- Xác định Thời gian

Phân tích SecSDLC: Quản lý rủi ro

- Xếp hạng rủi ro do từng kiểu đe dọa gây ra
- Xác định và đánh giá giá trị của tài sản thông tin
  - Chỉ định xếp hạng hoặc điểm rủi ro so sánh cho từng tài sản thông tin cụ thể

SecSDLC: Thiết kế

- Thiết kế trong SecSDLC
  - Tạo và phát triển một kế hoạch chi tiết về bảo mật
  - Kiểm tra và thực hiện các chính sách chính
  - Đánh giá công nghệ cần thiết để hỗ trợ kế hoạch bảo mật
  - Tạo các giải pháp thay thế
  - Đồng thuận về thiết kế cuối cùng
- Các mô hình bảo mật có thể được sử dụng để hướng dẫn quá trình thiết kế



SecSDLC: Thiết kế

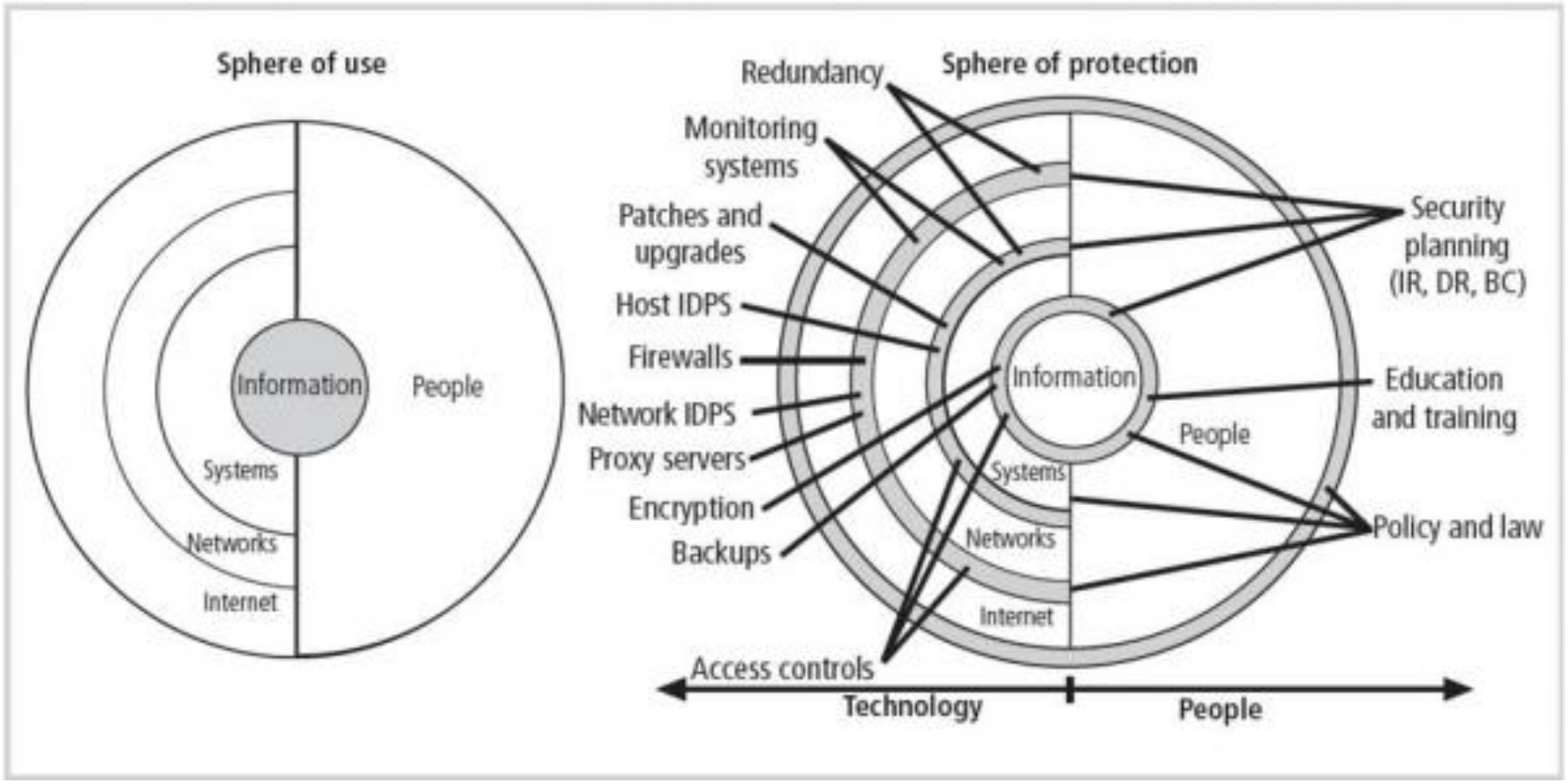
- Một yếu tố thiết kế quan trọng của chương trình an toàn thông tin là chính sách an toàn thông tin
- Ban quản lý phải xác định các loại chính sách bảo mật
- Phần tích hợp của thiết kế: Chương trình SETA
  - Bao gồm: Giáo dục an ninh, đào tạo an ninh và nâng cao nhận thức về an ninh (**S**ecurity **e**ducation, security **t**raining, and security **a**wareness)
  - Mục đích: tăng cường bảo mật

SecSDLC: Thiết kế

- Kiểm soát thiết kế và các biện pháp bảo vệ
  - Được sử dụng để bảo vệ thông tin khỏi các cuộc tấn công bởi các mối đe dọa

- Kiểm soát thiết kế và các biện pháp bảo vệ (Danh mục):
  1. Kiểm soát quản lý
  2. Kiểm soát hoạt động
  3. Kiểm soát kỹ thuật

SecSDLC: Thiết kế



SecSDLC: Thiết kế

- Lập kế hoạch dự phòng (Chương 3)
  - Chuẩn bị, phản ứng và phục hồi từ các tình huống đe dọa tổ chức

- Các loại lập kế hoạch dự phòng
  - Lập kế hoạch ứng phó sự cố (IRP)
  - Lập kế hoạch khôi phục thảm họa (DRP)
  - Lập kế hoạch liên tục kinh doanh (BCP)

  - Incident response planning (IRP)
  - Disaster recovery planning (DRP)
  - Business continuity planning (BCP)

SecSDLC: Thiết kế

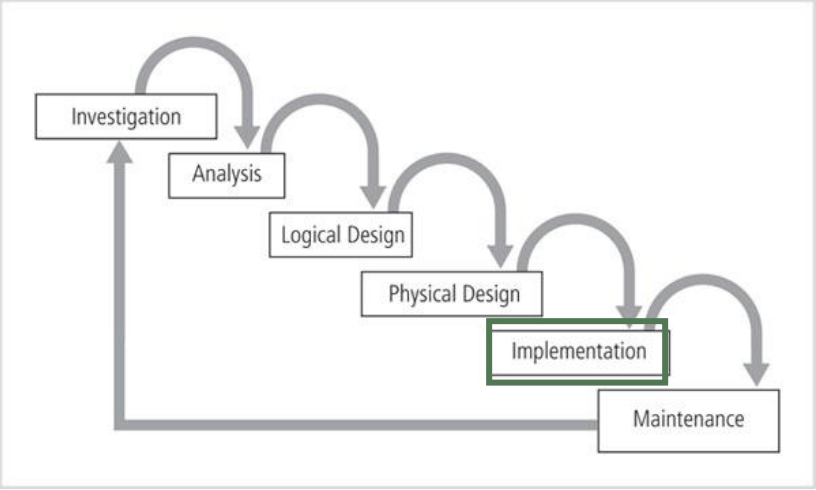
- Bảo mật vật lý
  - Thiết kế, thực hiện và duy trì các biện pháp đối phó để bảo vệ các tài nguyên vật lý của một tổ chức

- Nguồn lực vật chất bao gồm
  - Con người
  - Phần cứng
  - Các yếu tố hệ thống thông tin hỗ trợ

SecSDLC: Thực hiện

Các giải pháp bảo mật được mua lại, 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

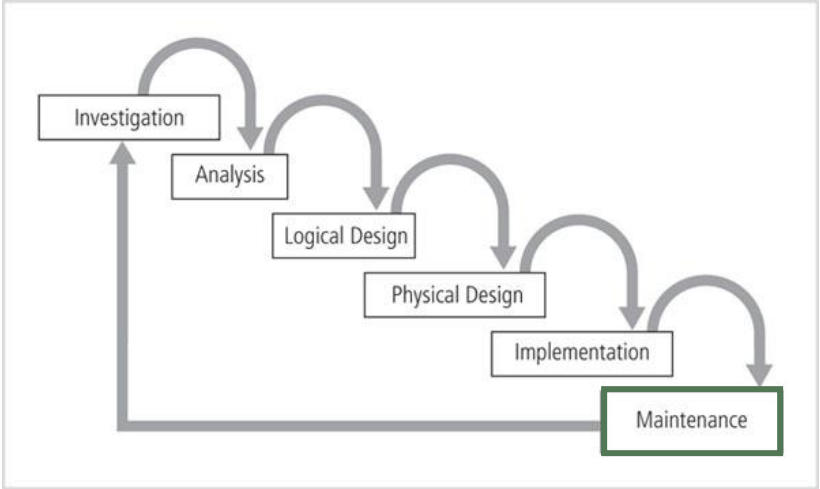


SecSDLC: Bảo trì

Khi chương trình được triển khai, nó phải:

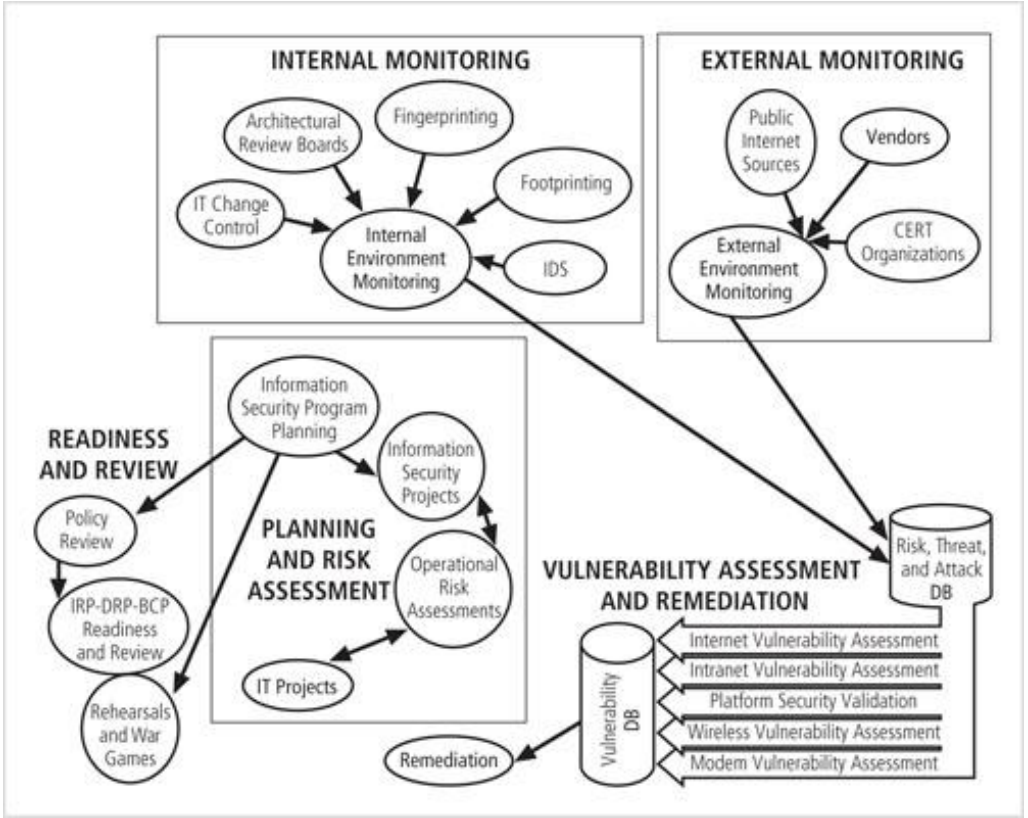
- Hoạt động
- Được quản lý đúng cách
- Kịp thời (tức là cập nhật bằng cách sử dụng các quy trình đã thiết lập)

Nếu chương trình không điều chỉnh thích hợp với những thay đổi trong môi trường bên trong hoặc bên ngoài, có thể cần phải bắt đầu lại chu trình



SecSDLC: Bảo trì

- Các khía cạnh của một mô hình bảo trì
  - Giám sát bên ngoài
  - Giám sát nội bộ
  - Lập kế hoạch và đánh giá rủi ro
  - Đánh giá và khắc phục lỗ hổng bảo mật
  - Sẵn sàng và kiểm tra xem xét
  - Đánh giá lỗ hổng bảo mật



Hình 2-11 Mô hình bảo trì

SecSDLC: Bảo trì

- Quản lý chương trình bảo mật (Chương 6)
  - Một tiêu chuẩn quản lý chính thức có thể cung cấp một số thông tin chi tiết về các quy trình và thủ tục cần thiết
  - Các ví dụ bao gồm mô hình BS7799 / ISO17799 / ISO27xxx hoặc các mô hình NIST được mô tả trước đó

Điều 2: Đối phó với GRC

- GRC trong một thế giới ngày càng phức tạp, tập trung vào thông tin
- Thách thức
- Gợi ý
- Xây dựng nền tảng GRC

Tóm lược

- Quản trị an toàn thông tin
- Lập kế hoạch triển khai an toàn thông tin
- Giới thiệu về vòng đời phát triển hệ thống an ninh

Bài tập và thảo luận

Bài tập và thảo luận