HỌC VIỆN KTQS
KHOA CÔNG NGHỆ THÔNG TIN

Bài 5.
Kế hoạch, chính sách cho ANTT

Học phần: BẢO ĐẢM VÀ AN TOÀN THÔNG TIN

NỘI DUNG

1. Vai trò của kế hoạch, chính sách trong an ninh thông tin
2. Phân loại chính sách
3. Một số chính sách tiêu biểu
4. Tìm hiểu về dòng tiêu chuẩn ISO27000
5. Thảo luận, bài tập

Giới thiệu

- Việc tạo chương trình bảo mật thông tin bắt đầu bằng việc tạo hoặc xem xét các chính sách, tiêu chuẩn và thực tế bảo mật thông tin của hệ thống
- Sau đó, lựa chọn hoặc tạo ra kiến trúc bảo mật thông tin và sử dụng một kế hoạch chi tiết để đảm bảo an ninh cho hệ thống
- Nếu không có chính sách, kế hoạch chi tiết và lập kế hoạch, một tổ chức không thể đáp ứng nhu cầu bảo mật thông tin

1. Sự cần thiết của các kế hoạch và chính sách

- Các vấn đề của an toàn và bảo mật xảy ra trong suốt quá trình hình thành, phát triển, tồn tại của hệ thống
- Trong chuỗi mắt xích bảo vệ, sức mạnh chuỗi bảo vệ chính là điểm yếu nhất của nó
- Ban hành chính sách -> tuyên truyền -> kiểm tra
- Phạm vi vấn đề: các loại thông tin trong hệ thống

1. Sự cần thiết của các kế hoạch và chính sách

- Nguồn tấn công vào hệ thống: 80% xuất phát từ phía nhân viên
- Tấn công liên quan đến phần cứng, tấn công mạng: 16%. Các tấn công khác liên quan đến yếu tố con người
- Chính sách, chỉ dẫn, hướng dẫn giải quyết các vấn đề liên quan đến con người
  - Cơ sở để xem xét các hành động của con người để đánh giá
  - Kết hợp với các giải pháp kỹ thuật quản lý toàn bộ hệ thống
  - Nền tảng cho việc triển khai chương trình an ninh thông tin

Ví dụ một chính sách

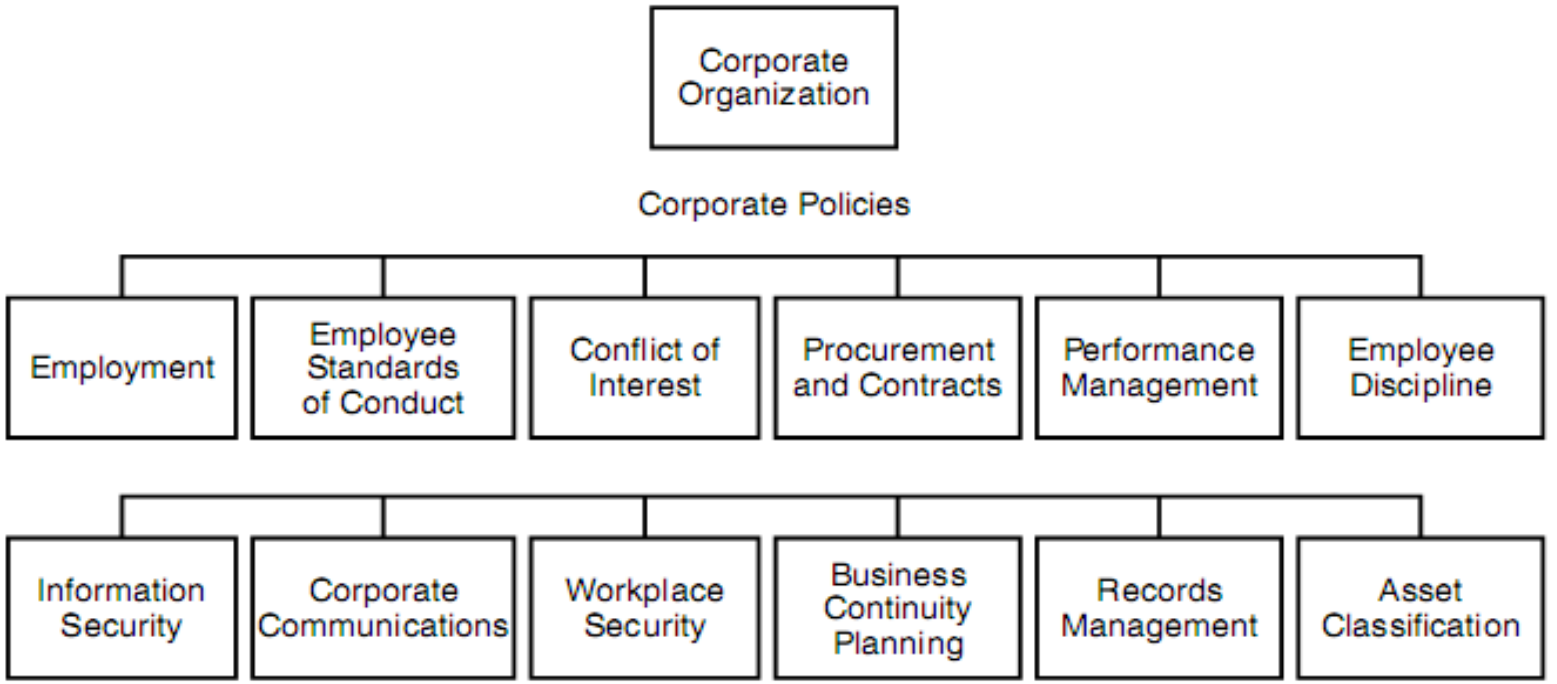


FIGURE 4.1 Corporate Policies

Các định nghĩa

1. Chính sách là một chuỗi hành động được tổ chức sử dụng để truyền đạt hướng dẫn từ quản lý đến những người thực hiện nhiệm vụ
Chính sách là luật của tổ chức
2. Tiêu chuẩn Là yêu cầu bắt buộc để hỗ trợ các chính sách riêng lẽ

Các định nghĩa

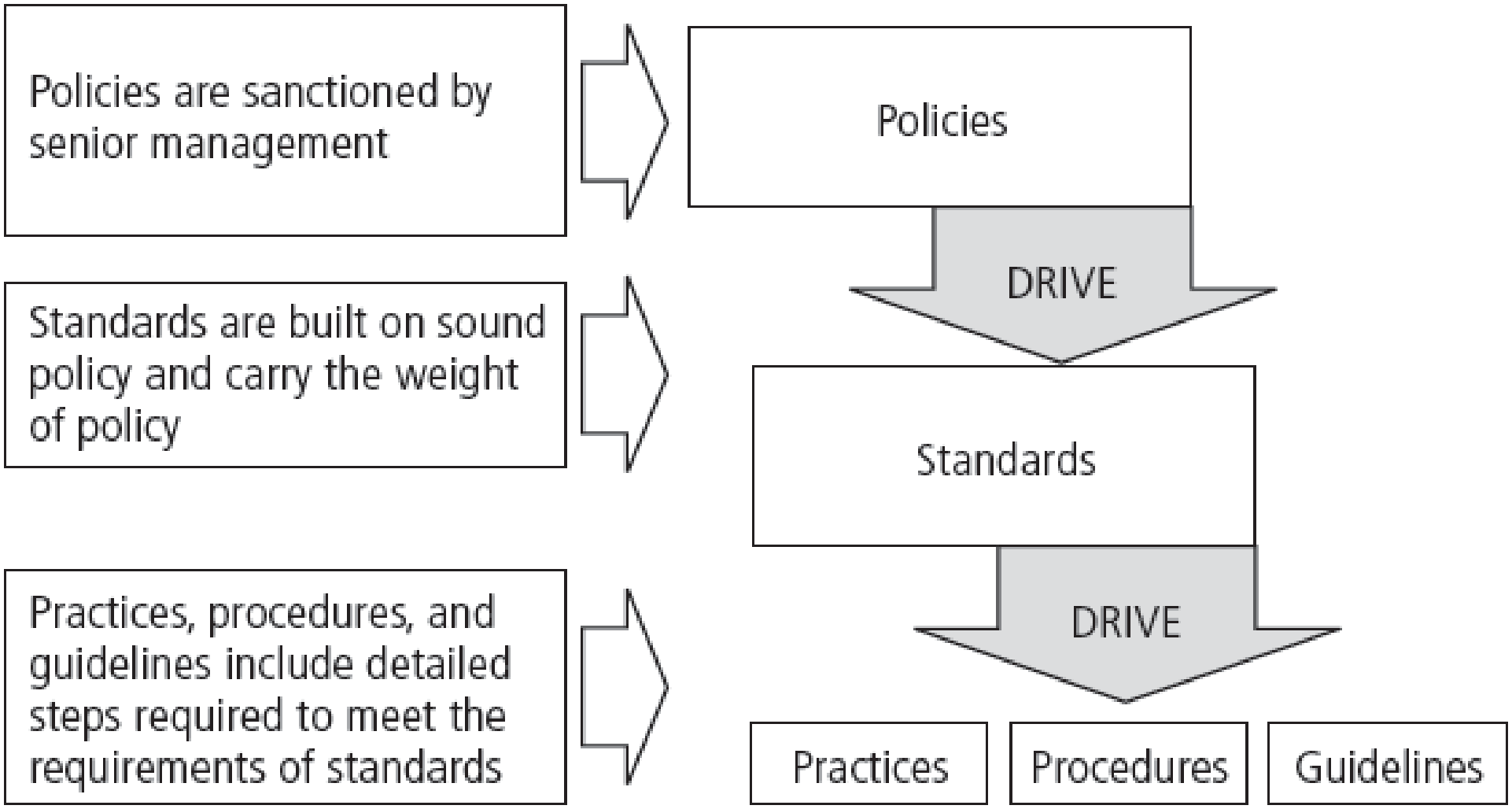
3. Chỉ dẫn

Chỉ dẫn là sự cần thiết, từng bước, hành động chi tiết hoá, yêu cầu phải thực hiện để hoàn thành một công việc

4. Hướng dẫn

Hướng dẫn thường là các phát biểu chung thiết kế để đạt được mục tiêu của chính sách bằng cách đưa ra nền tảng để thực hiện các chỉ dẫn

Mỗi quan hệ giữa các khái niệm



2. Phân loại chính sách

Chính sách chia thành 3 nhóm:

2.1. Toàn thể (mức 1): Dùng để tạo nên tầm nhìn chung và định hướng

2.2. Hướng đến chủ đề (mức 2): Đề cập đến các mục tiêu riêng biệt quan tâm

2.3. Hướng ứng dụng (mức 3): Tập trung trên các quyết định được áp dụng bởi người quản lý để điều khiển các ứng dụng riêng biệt

2. Phân loại chính sách

2.1. Toàn thể (mức 1):

Chủ đề

Vấn đề mà chính sách đề cập đến

Phạm vi chính sách quan tâm

Giới hạn

Giới hạn người có ảnh hưởng bởi chính sách
Giới hạn đối tượng điều chỉnh của chính sách

Trách nhiệm

Trách nhiệm các cá nhân

Sự tuân thủ hoặc những kết quả xấu
Hình thức xử phạt khi không tuân thủ

2. Phân loại chính sách

2.2. Hướng đến chủ đề (mức 2):

- Tập trung đến vấn đề liên quan và quan tâm hiện tại
- Thay đổi theo thời gian, sự thay đổi công nghệ, các nhân tố khác

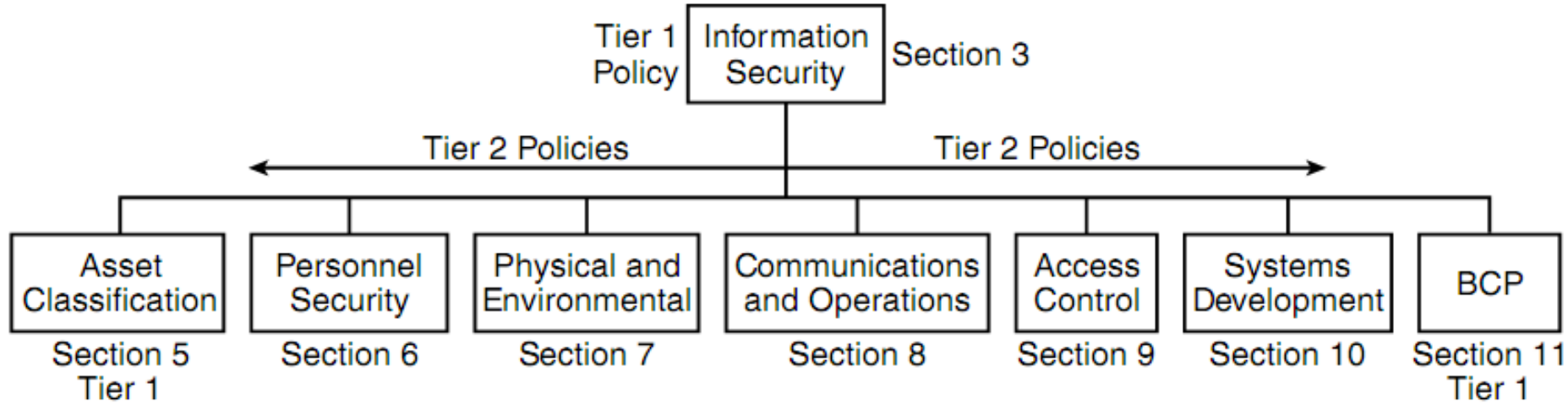


FIGURE 4.5 Topic-Specific Policies by Section

2. Phân loại chính sách

2.3. Mức ứng dụng (mức 3):

Chính sách mức 3 không có mô hình chặt chẽ như mức 1, 2. Nhưng cần chú ý một số điểm:

- Hiểu được nhiệm vụ, mục tiêu toàn cục của công ty
- Hiểu được nhiệm vụ của chương trình, hệ thống
- Thiết lập các yêu cầu hỗ trợ cả hai mục tiêu

3. Một số chính sách tiêu biểu

3.1 Chính sách phân lớp tài sản

3.2 Chính sách quản lý tài liệu

3.3 Chính sách điều khiển truy xuất

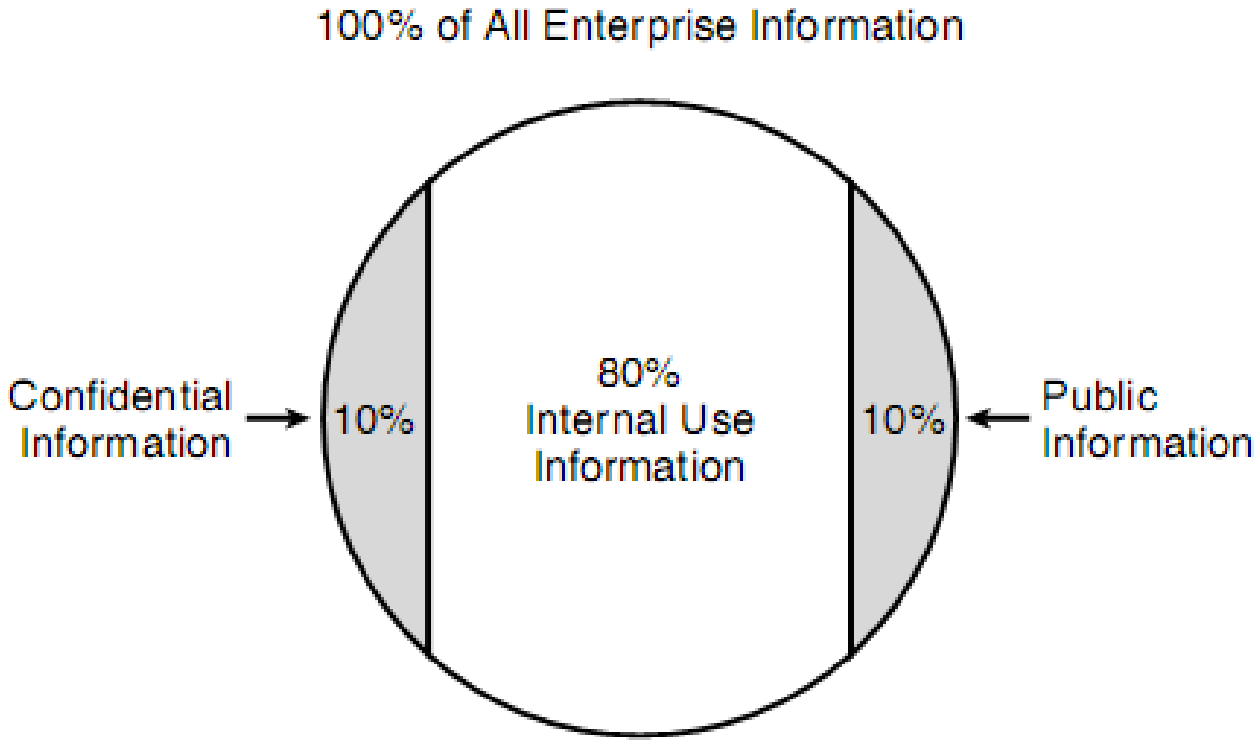
3.4 Chính sách công việc liên tục

3.5 Chính sách an ninh của một doanh nghiệp cụ thể

3.1 Chính sách phân lớp tài sản

i. Đảm bảo cho các tài sản được phân lớp đúng theo giá trị

ii.Cơ sở cho các chính sách đảm bảo trên các phân lớp



3.1 Chính sách phân lớp tài sản

Ví dụ về phân lớp thông tin

- *Top secret – tối mật*
- *Confidential – mật*
- *Restricted – giới hạn*
- *Internal Use – sử dụng nội bộ*
- *Public – công khai*

3.1 Chính sách phân lớp tài sản

Ví dụ về phân lớp thông tin

- *Top secret – tối mật: màu đỏ*
- *Confidential – mật: màu vàng*
- *Restricted – giới hạn: màu cam*
- *Internal Use – sử dụng nội bộ: màu xanh*
- *Public – công khai: màu trắng*

3.2 Chính sách quản lý tài liệu

- Kết hợp với chính sách về phân lớp tài sản để đề xuất các múc bảo vệ phù hợp
- Thực hiện trên các giai đoạn của tài liệu
  + Lưu trữ
  + Xử lý
  + Hủy
- Phân rõ trách nhiệm của các nhóm
  + Chủ sở hữu
  + Người bảo vệ
  + Người sử dụng

3.3 Chính sách điều khiển truy xuất

1. Cấp phép tài khoản

- Kiểm tra người dùng đăng ký tài khoản
- Cung cấp truy xuất đầu tiên với hệ thống

2. Quản lý quyền ưu tiên truy xuất

- Đảm bảo kiểm tra các ưu tiên theo thời gian với người dùng
- Đảm bảo sự tồn tại người dùng thực tế

3.3 Chính sách điều khiển truy xuất

3. Quản lý xác thực tài khoản

- Mật khẩu thay đổi theo tiêu chuẩn công nghiệp, 30 ngày
- Thời gian thay đổi mật khẩu thể hiện sự cần thiết bảo mật của thông tin trong hệ thống
- Mật khẩu phải được lựa chọn tốt: ít nhất có 8 ký tự, không sử dụng các ký tự trong từ điển, và có ký tự đặc biệt
- Hỗ trợ đăng nhập sai 3 lần trước khi khóa tài khoản

3.4 Chính sách công việc liên tục

- Đảm bảo công việc hoạt động trong các tình huống
- Bao gồm cả kế hoạch phục hồi sự cố
- Có tác dụng trong tình huống khẩn cấp
  + Khó kiểm tra
  + Khó thuyết phục người quản lý
  + Bảo hiểm chỉ giải quyết về mặt kinh tế

3.4 Chính sách công việc liên tục

Có nhiều yếu tố ảnh hưởng đến hoạt động

Thảm họa tự nhiên: lũ lụt, động đất, cháy, lốc, bão

+ Tai nạn
+ Cạnh tranh, tấn công đối thủ
+ Nang lượng không được cung cấp
+ Các dịch vụ: kết nối, vận chuyển, bảo vệ không hoạt động
+ Thảm họa về môi trường
+ Tấn công của hacker

3.4 Chính sách công việc liên tục

Các bước tiến hành

+ Xác định các tài nguyên

+ Xác định các đe dọa

+ Xác định các nguy cơ

+ Xác định ảnh hưởng đến hệ thống

+ Xác định các dịch vụ và hệ thống cần được khôi phục ngay

+ Xác định tài nguyên để hồi phục hệ thống

3.4 Chính sách công việc liên tục

Các bước tiến hành

+ Thành lập hội đồng

+ Xây dựng hệ thống câu hỏi xác định tác động công việc

+ Tiến hành thu thập thông tin

+ Xác định các đối tượng, tiến trình cần quan tâm

+ Xây dưng kế hoạch

+ Kiểm tra kế hoạch

+ Duy trì kế hoạch

3.5 Chính sách an ninh cho doanh nghiệp(EISP)

- Là tập hợp tất cả các chiến lược, phạm vi để đảm bảo an ninh cho tổ chức
- Tài liệu soạn thảo thường được soạn thảo bởi CIO của tổ chức
- Nó đáp ứng yêu cầu là đăng ký trách nhiệm tới từng bộ phận, thành phần trong hệ thống
- Sử dụng các biện pháp sử phạt đối với những vi phạm

3.5 Chính sách an ninh cho doanh nghiệp(EISP)

Các thành phần trong EISP bao gồm:

- Tổng quan về triết lý của công ty về bảo mật
- Thông tin về cơ cấu tổ chức bảo mật thông tin và từng cá nhân thực hiện vai trò bảo mật thông tin
- Trách nhiệm về an ninh được chia sẻ bởi tất cả các thành viên của tổ chức (nhân viên, nhà thầu, tư vấn, đối tác và khách truy cập)
- Trách nhiệm được gán cho mỗi thành viên trong tổ chức

3.5 Chính sách an ninh cho doanh nghiệp

Các thành phần của của một chính sách bao gồm:

1. Lời tuyến bố chính sách

a. Phạm vi và khả năng áp dụng

b. Định nghĩa về công nghệ được giải quyết

c. Trách nhiệm

2. Quyền truy cập và sử dụng thiết bị được ủy quyền

a. Người dùng truy cập

b. Sử dụng hợp pháp và có trách nhiệm

c. Bảo vệ quyền riêng tư

3. Nghiêm cấm sử dụng thiết bị

a. Sử dụng hoặc sử dụng sai mục đích

b. Tài liệu xúc phạm hoặc quấy rối

c. Bản quyền, được cấp phép hoặc tài sản trí tuệ khác

4. Quản lý hệ thống

a. Quản lý tài liệu lưu trữ

b. Giám sát nhà tuyển dụng

c. Bảo vệ chống vi-rút

d. Bảo mật vật lý

e. Mã hóa

3.5 Chính sách an ninh cho doanh nghiệp

Các thành phần của của một chính sách bao gồm:

5. Vi phạm chính sách

a. Thủ tục báo cáo vi phạm

b. Hình phạt đối với vi phạm

6. Xem xét và sửa đổi chính sách

a. Đánh giá theo lịch trình các thủ tục chính sách để sửa đổi

b. Tuyên bố từ chối trách nhiệm pháp lý

7. Giới hạn trách nhiệm pháp lý

a. Báo cáo trách nhiệm pháp lý

b. Các tuyên bố từ chối trách nhiệm khác khi cần

4. Dòng tiêu chuẩn ISO 27000

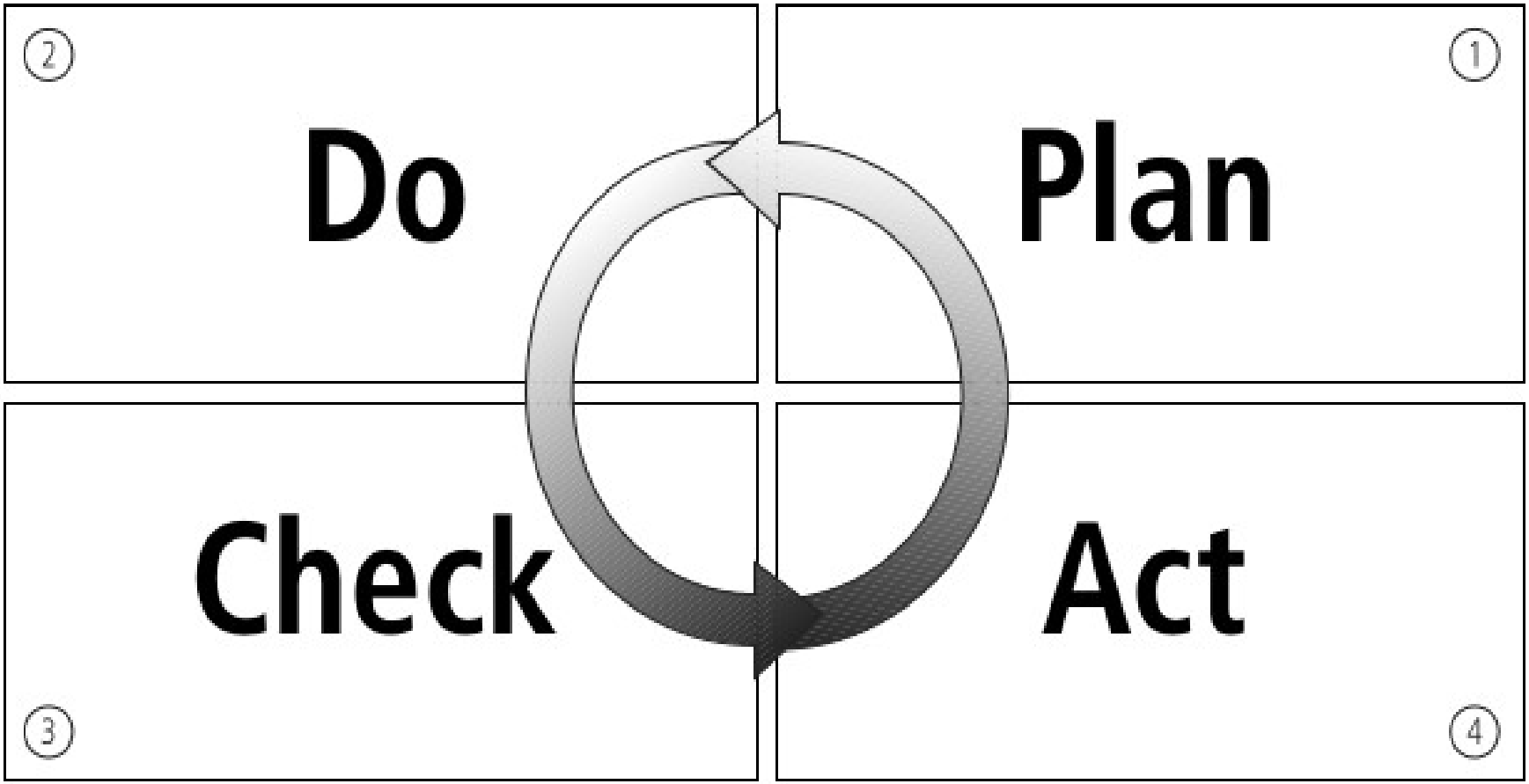
Định nghĩa: là tiêu chuẩn quốc tế về thông tin hoặc quản lý an ninh

- Tiêu chuẩn vạch ra phương pháp để thực hiện đánh giá độc lập hệ thống quản lý an ninh thông tin và chứng nhận cho hệ thống đó

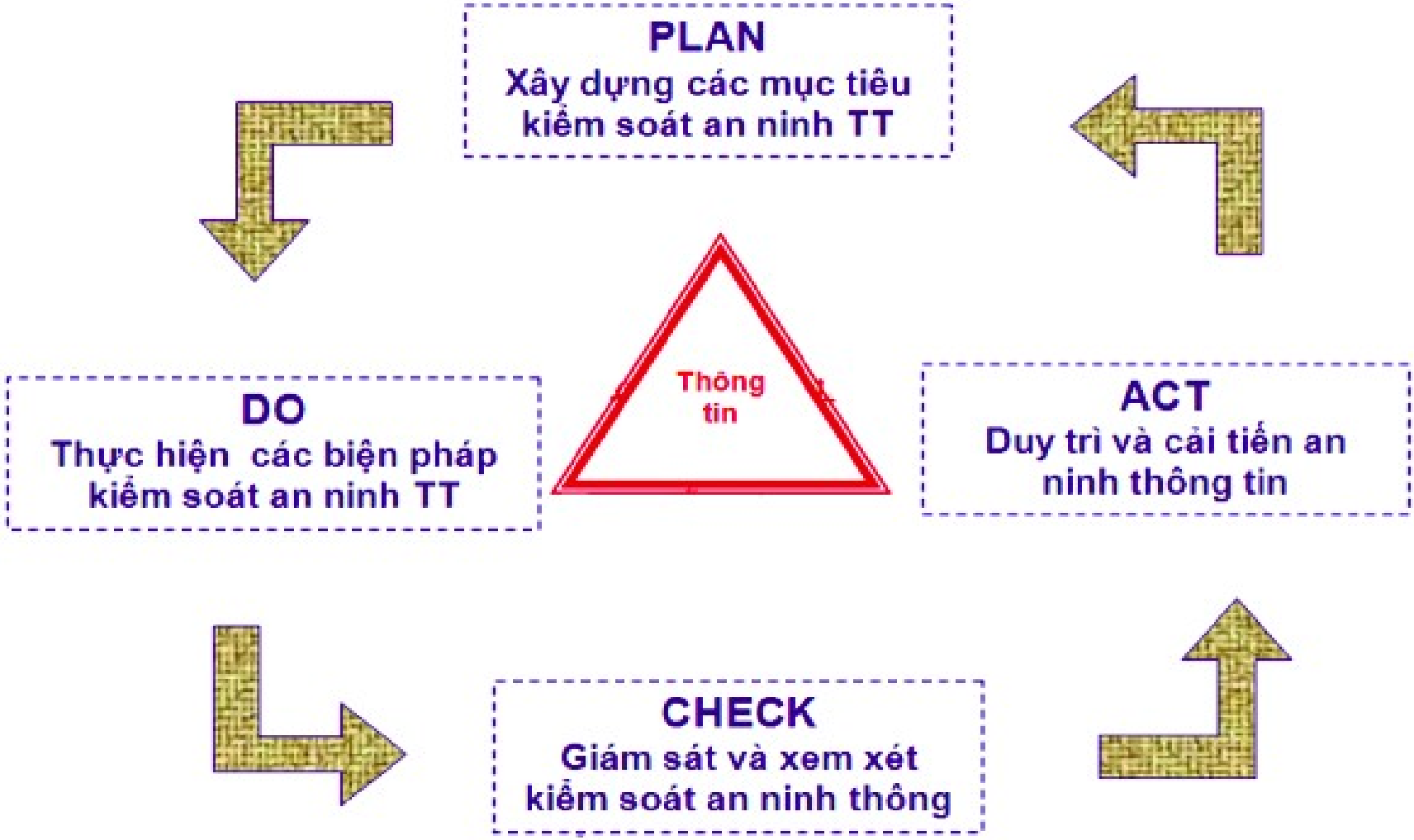
Mục đích: là đưa ra các khuyến nghị về quản lý bảo mật thông tin

- Cung cấp một cơ sở chung để phát triển an ninh của tổ chức

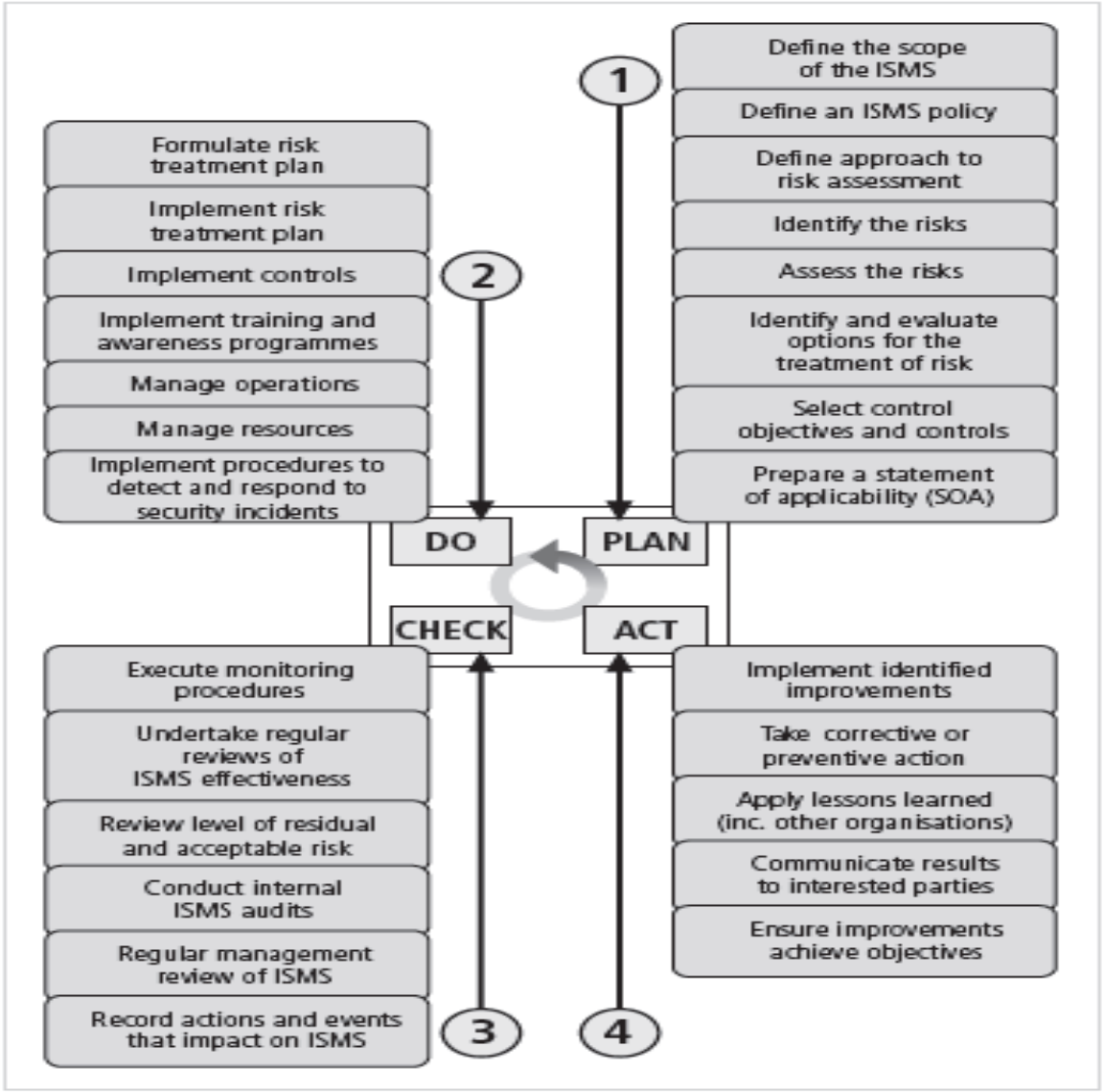
ISO/IEC 27001: 2005 Plan-Do-Check-Act Cycle



ISO/IEC 27001: 2005 Plan-Do-Check-Act Cycle



ISO/IEC 27001: 2005 Plan-Do-Check-Act Cycle



Courtesy of Gamma Secure Systems

ISO/IEC 27001: 2005 Plan-Do-Check-Act Cycle

Plan	
1	Define the scope of the ISMS
2	Define an ISMS policy
3	Define the approach to risk assessment
4	Identify the risks
5	Assess the risks
6	Identify and evaluate options for the treatment of risk
7	Select control objectives and controls
8	Prepare a statement of applicability (SOA)

ISO/IEC 27001: 2005 Plan-Do-Check-Act Cycle

Do	
9	Formulate a risk treatment plan
10	Implement the risk treatment plan
11	Implement controls
12	Implement training and awareness programs
13	Manage operations
14	Manage resources
15	Implement procedures to detect and respond to security incidents

ISO/IEC 27001: 2005 Plan-Do-Check-Act Cycle

Check	
15	Execute monitoring procedures
16	Undertake regular reviews of ISMS effectiveness
17	Review the level of residual and acceptable risk
18	Conduct internal ISMS audits
19	Undertake regular management review of the ISMS
20	Record actions and events that impact an ISMS

ISO/IEC 27001: 2005 Plan-Do-Check-Act Cycle

Act	
21	Implement identified improvements
22	Take corrective or preventive action
23	Apply lessons learned
24	Communicate results to interested parties
25	Ensure improvements achieve objectives

5. Thảo luân và bài tập

What is the ISO 27000 series of standards? Which individual standards make up the Series?

What is contingency planning? How is it different from routine management planning?

What are the components of contingency planning?

HỎI VÀ ĐÁP