CƠ SỞ AN TOÀN THÔNG TIN

Bài 11. Quản lý an toàn thông tin

1. Quản lý an toàn thông tin
2. Giới thiệu ISO 27001
3. Quản lý an toàn thông tin theo ISO 27001

Tài liệu tham khảo

1. Phạm Minh Thuấn, **Bài giảng Quản lý an toàn thông tin**, Học viện Kỹ thuật mật mã, 2016
2. Whitman, Mattord, **Principles of Information Security** (5e), Cengage Learning, 2014
3. ISO 27001:2005

1. Quản lý an toàn thông tin
2. Giới thiệu ISO 27001
3. Quản lý an toàn thông tin theo ISO 27001

An toàn Thông tin

80% là Quản lý

- Chính sách An toàn Thông tin
- Trách nhiệm An toàn Thông tin
- Phổ biến/Huấn luyện An toàn Thông tin
- Kế hoạch Kinh doanh Liên tục

20% là Công nghệ

- Hệ thống, Công cụ, Cấu trúc, v.v...

Định nghĩa

- **Quản lý** là sự tác động có mục đích của chủ thể quản lý đến một hệ thống nào đó nhằm biến đổi nó từ trạng thái này sang trạng thái khác.
- **Quản lý an toàn thông tin** là tác động lên hệ thống thông tin nhằm đưa hệ thống đó về trạng thái được đảm bảo tính bí mật, tính toàn vẹn và tính khả dụng.

Quản lý an toàn thông tin

❑Tác động lên hệ thống thông tin:

- Cài đặt phần mềm diệt mã độc
- Cài đặt, cấu hình tường lửa
- Phân quyền truy cập cho người dùng
- Thiết lập chính sách an toàn
- Đào tạo chuyên gia
- ....

Quản lý an toàn thông tin

❑Tác động lên hệ thống thông tin:

- Cần những biện pháp tác động nào?
- Tác
- Bac
- Kiểm chứng kết quả thế nào?
- ....

Áp dụng tiêu chuẩn về quản lý an toàn thông tin!

Tiêu chuẩn quản lý an toàn thông tin

- COBIT - Control Objectives for Information and Related Technology (Mục tiêu quản lý đối với công nghệ thông tin và công nghệ liên quan)
- ITIL – Information Technology Infrastructure Library (Thư viện hạ tầng công nghệ thông tin)
- ISO 27001 - Information Security Management Systems (ISMS)

Áp dụng tiêu chuẩn

Tìm hiểu các tiêu chí (các yêu cầu) của tiêu chuẩn

Áp dụng các biện pháp tác động chuẩn để đạt các tiêu chí

Thực hiện kiểm định hợp chuẩn bởi tổ chức có thẩm quyền

Công bố hợp chuẩn

Lợi ích của việc tuân thủ chuẩn

1

2

3

4

5

6

Cấp độ điều hành: Mang lại hiểu

Cấp độ thương mại: Các thành

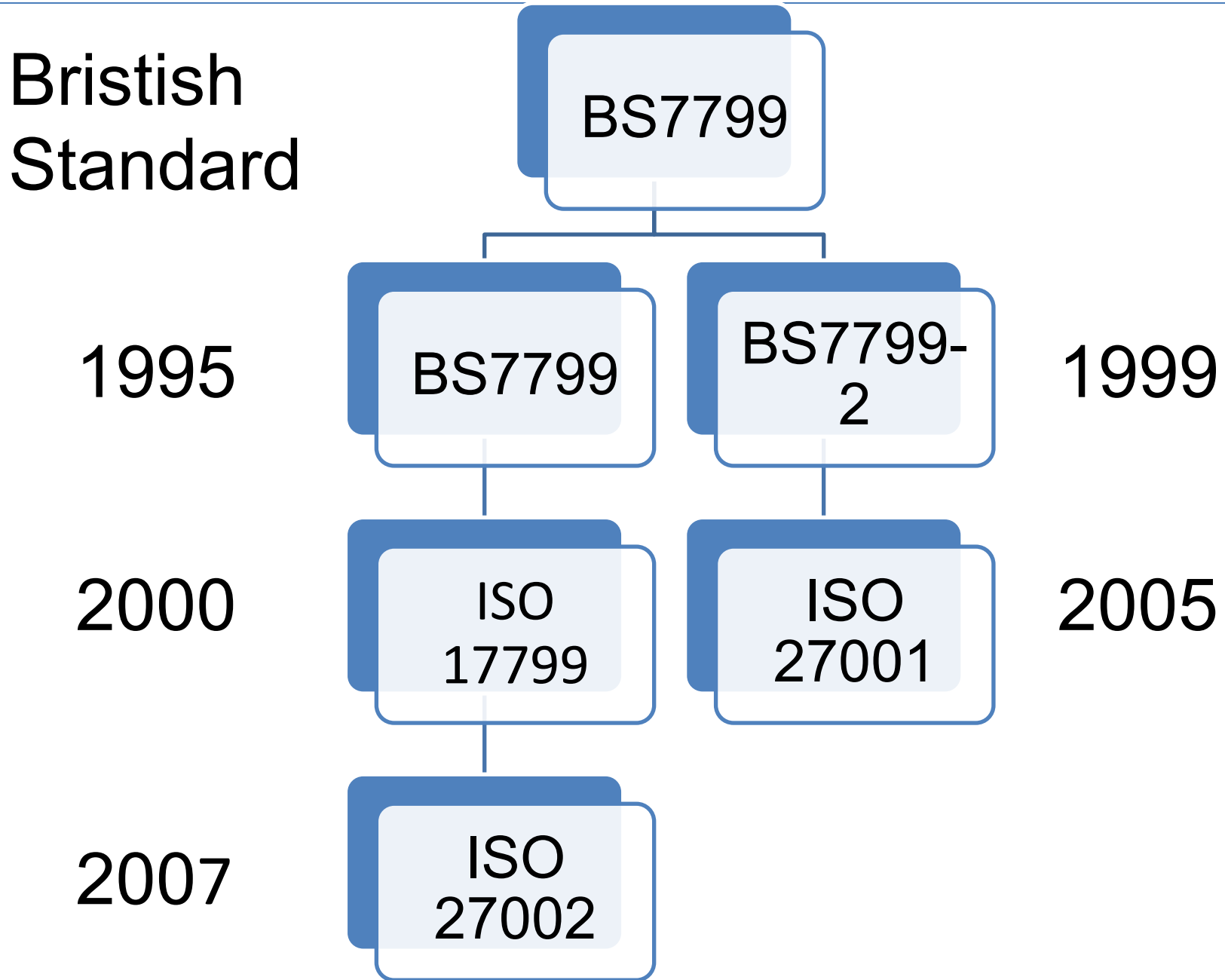
Cấp độ con người: Cải thiện nhận thức của nhân viên về các vấn đề an toàn thông tin và trách nhiệm của họ trong tổ chức

1 Quản lý an toàn thông tin

2 Giới thiệu ISO 27001

3 Quản lý an toàn thông tin theo ISO 27001

Lịch sử ISO 27001



Giới thiệu chung

- Đến nay, "27001" đại diện cho một bộ tiêu chuẩn 2700x
- ISO 27001 là một trong các tiêu chuẩn
- ISO 27001 là mục tiêu
- Các tiêu chuẩn khác giúp đạt được mục tiêu
- Hai nhóm tiêu chuẩn: tiêu chuẩn áp dụng, tiêu chuẩn kiểm chuẩn

Tiêu chuẩn áp dụng (1/2)

- ISO/IEC 27000 – ISMS Overview and Vocabulary;
- ISO/IEC 27001 – ISMS Requirements
- ISO/IEC 27002 – Code of Practice for Information Security Management
- ISO/IEC 27003 – ISMS Implementation Guidance;

Tiêu chuẩn áp dụng (2/2)

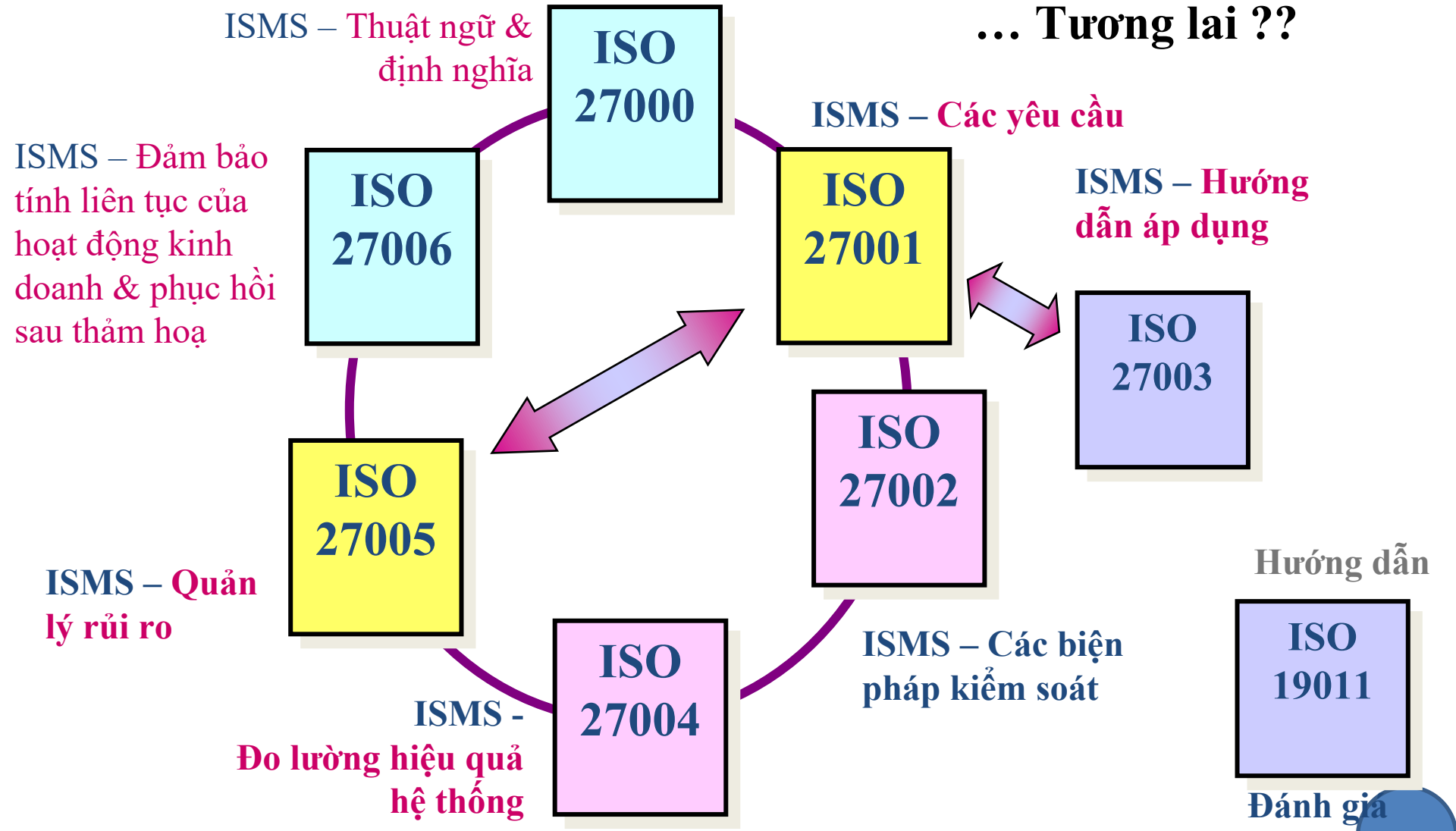
- ISO/IEC 27004 – Information Security Management Measurement & Metrics;
- ISO/IEC 27005 – Information Security Risk Management;
- ISO/IEC TR 27008 – Guidelines for Auditors on Information Security Controls;
- ISO/IEC 27031 – Information and Telecomunication Technology (ICT) Readiness for Business Continuity.

Tiêu chuẩn kiểm chuẩn

- ISO/IEC 17021 – Conformity Assessment: Requirements for bodies providing audit an stems;
- IS bodies pro Information Security Management Systems.

Phiên bản mới nhất
ISO 27001:2013

Bộ tiêu chuẩn ISO 27000

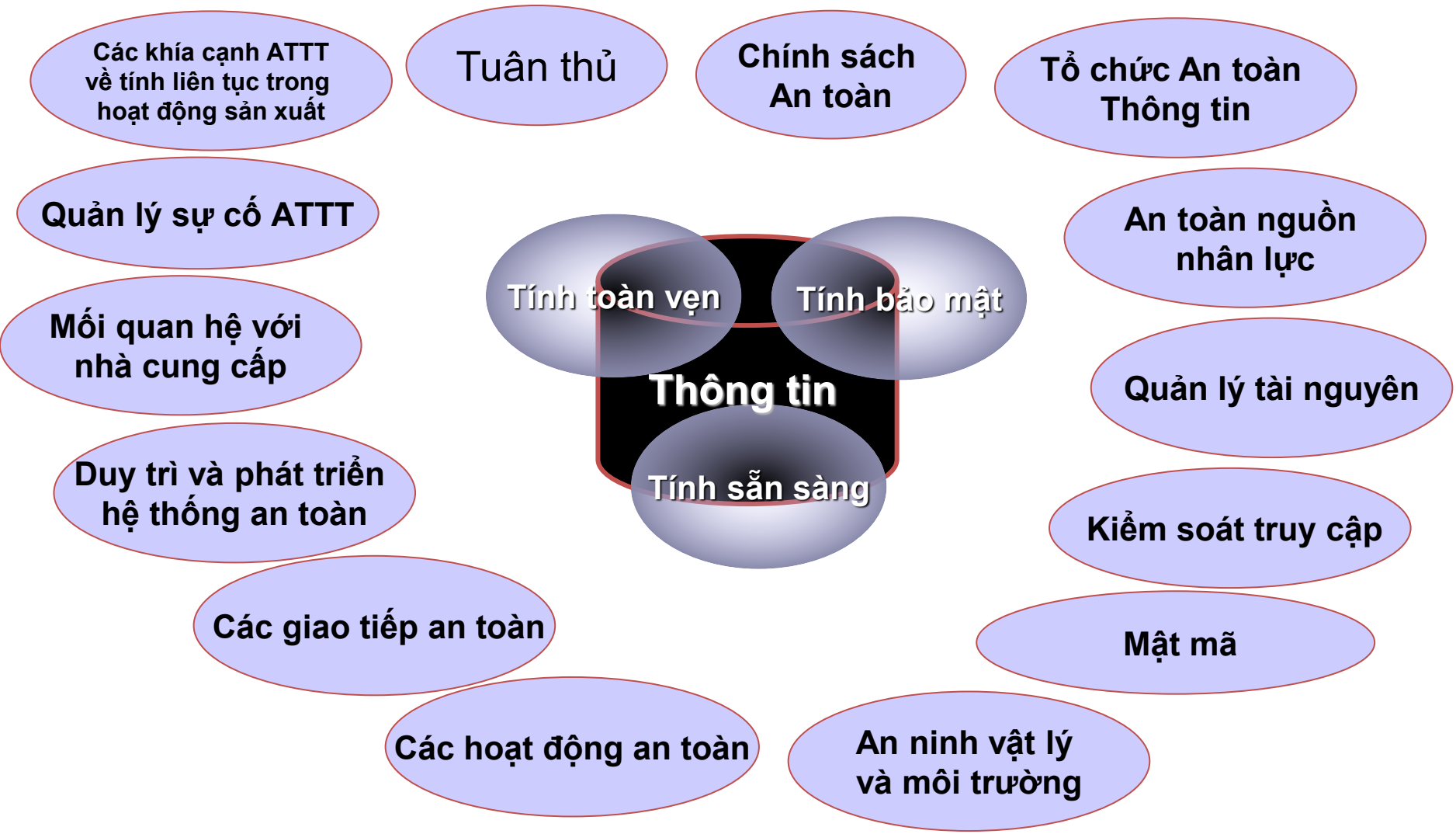


1. Quản lý an toàn thông tin
2. Giới thiệu ISO 27001
3. Quản lý an toàn thông tin theo ISO 27001

ISO 27001

- ISO 27001 cung cấp mô hình để xây dựng, thiết lập, vận hành, rà soát, bảo trì và cải tiến một Hệ thống quản lý an toàn thông tin
- ISMS = Information Security Management System
- Mô hình PDCA (Plan – Do – Check – Act)

Các kiểm soát (Phụ lục A)

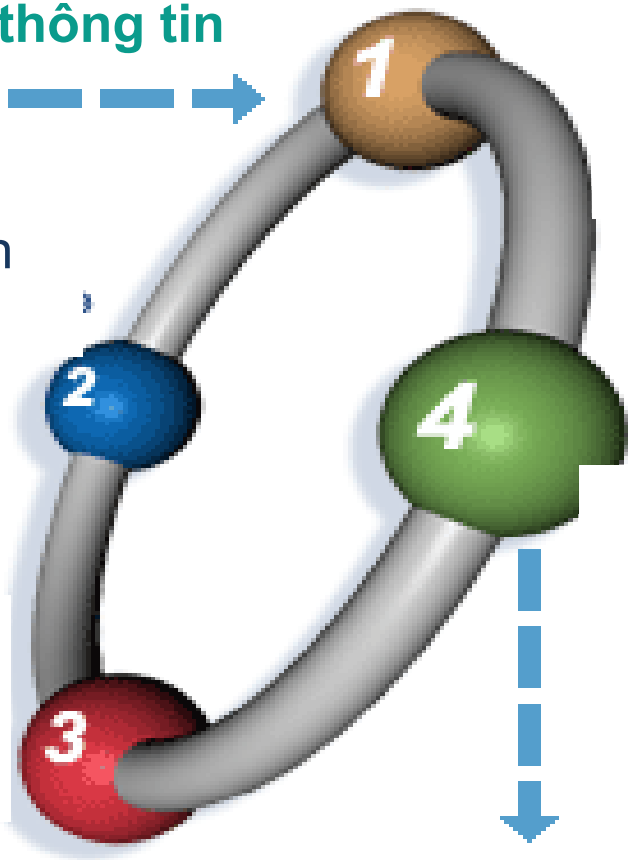


Mô hình PDCA

Các yêu cầu và mong muốn về an toàn thông tin

Lập kế hoạch
thiết lập ISMS

Thực hiện
triển khai và vận hành ISMS

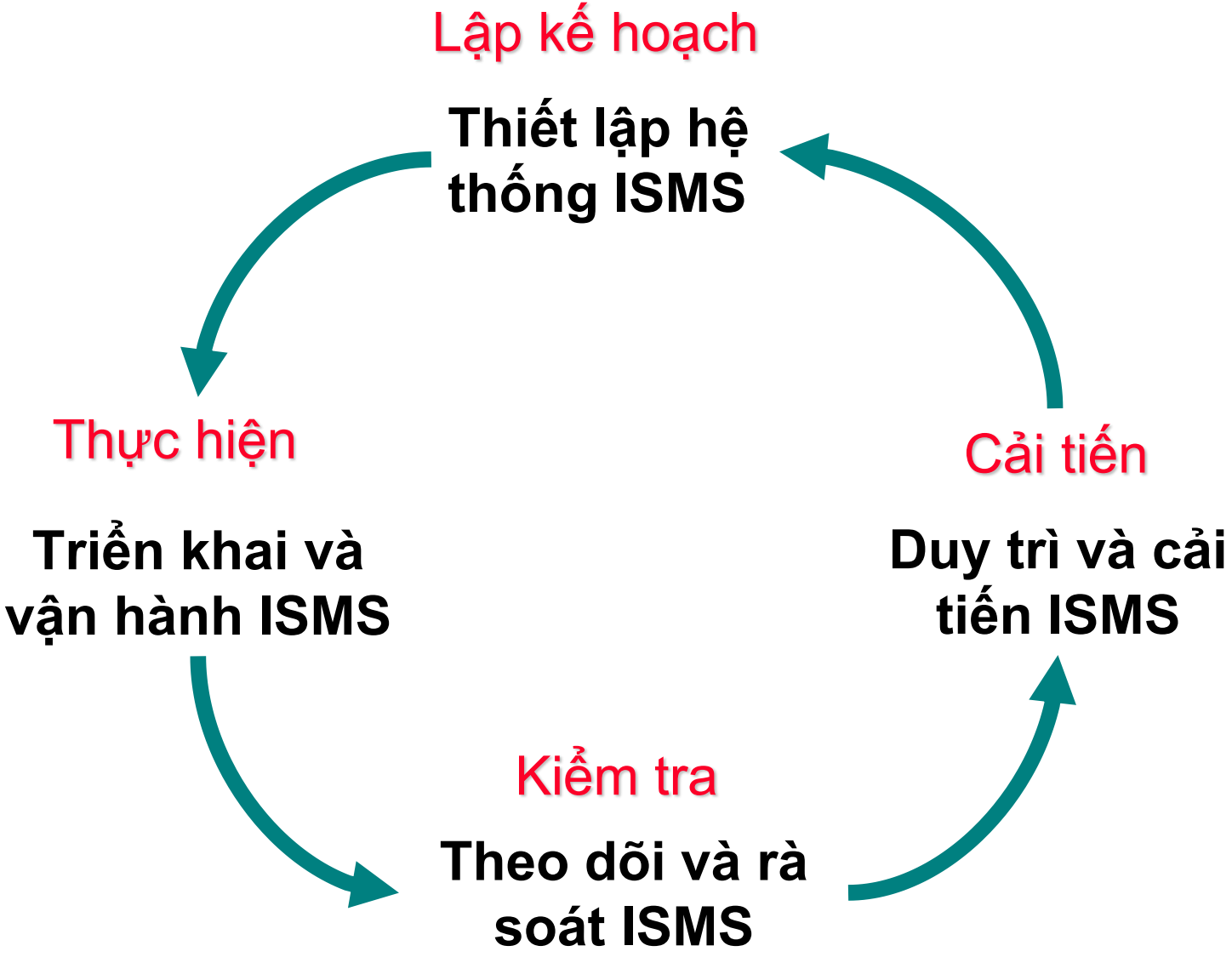


Cải tiến
duy trì và cải tiến ISMS

Kiểm tra
theo dõi và rà soát ISMS

an toàn thông tin được quản lý

Thực hiện các bước của mô hình PDCA



1/4. Lập kế hoạch

- **Thiết lập ISMS**

a) Xác định phạm vi của ISMS

b) Đề ra một chính sách ISMS

c) Xác định một phương pháp đánh giá rủi ro của tổ chức

d) Nhận diện các rủi ro

e) Phân tích và đánh giá các rủi ro

f) +++

2/4. Thực hiện

- **Triển khai và vận hành ISMS**

a) Thiết lập kế hoạch xử lý rủi ro

b) Thực hiện kế hoạch xử lý rủi ro

c) Thực hiện các công cụ kiểm soát được chọn để đáp ứng các mục tiêu kiểm soát

d) Quy định cách đo lường sự hiệu quả của các công cụ kiểm soát được chọn

e) +++

3/4. Theo dõi và rà soát

- **Theo dõi và rà soát ISMS**

a) Thực hiện các thủ tục theo dõi, soát xét và các công cụ kiểm soát khác

b) Rà soát định kỳ hiệu quả của ISMS

c) Đo lường hiệu quả của các công cụ kiểm soát

d) Xem xét định kỳ các đánh giá rủi ro

e) Định kỳ đánh giá nội bộ ISMS

f) +++

4/4. Cải tiến

- **Duy trì và cải tiến ISMS**

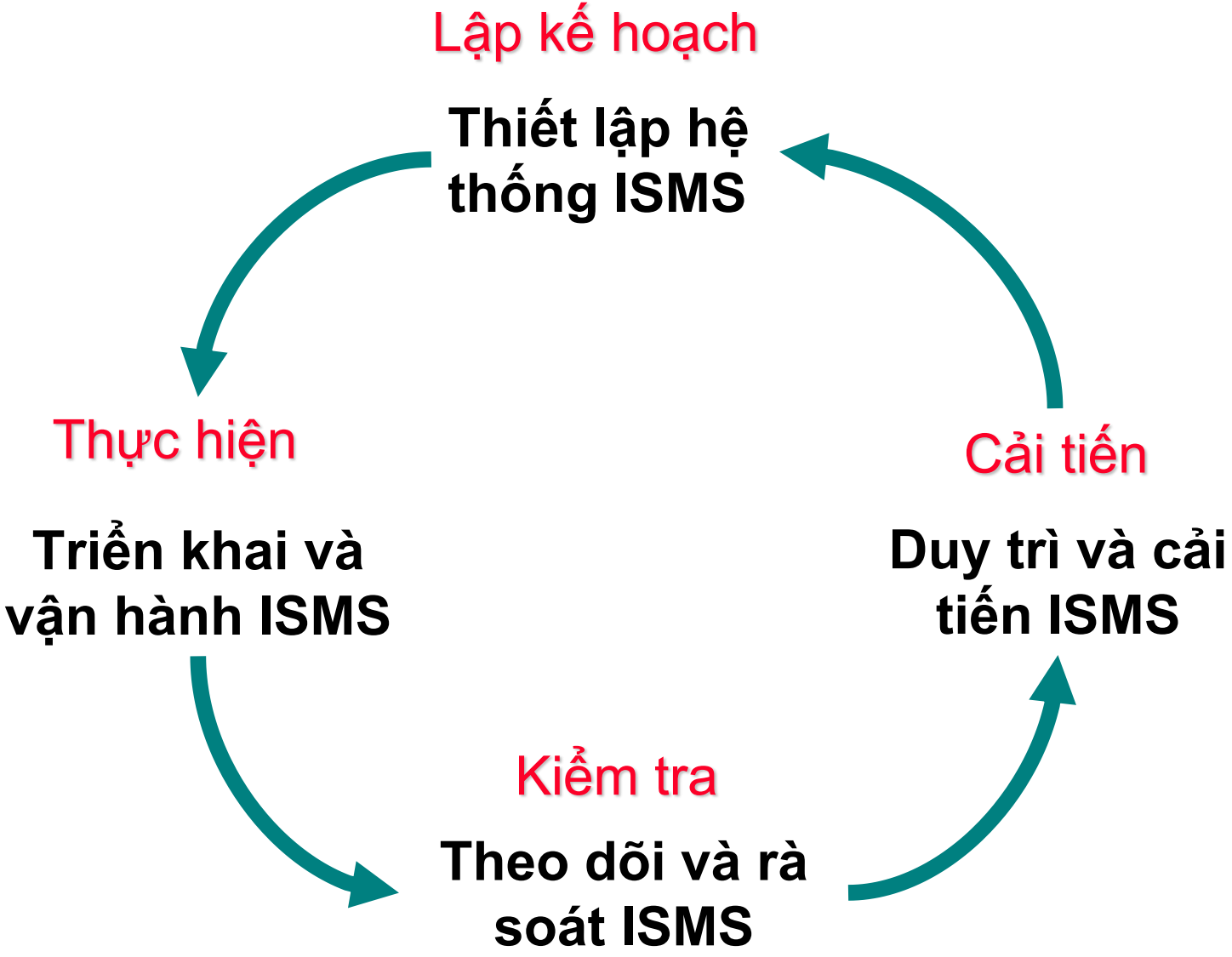
a) Thực hiện các cải tiến đã được xác định

b) Thực hiện các hành động khắc phục và phòng ngừa thích hợp

c) Thông tin về các hoạt động và cải tiến với tất cả các bên liên quan

d) Bảo đảm các cải tiến đạt được mục tiêu đề ra

Tiếp tục vòng lặp




Q&A