

CHƯƠNG 07

ISO 27000

ThS.Nguyễn Duy
duyn@uit.edu.vn

Nội dung

2

duyn@uit.edu.vn

- **Lịch sử hình thành ISO 27000**
- ISO 27001
- ISO 27002

Nội dung

3

duyn@uit.edu.vn

- ISO27000 – Overview and vocabulary
- ISO27001 – Audit requirements
- ISO27002 – Code of Practices (was ISO17799:2005)
- ISO27003 – Implementation Guidance
- ISO27004 – Measurement
- ISO27005 – Risk Management
- ISO27006 – Requirements for Bodies providing Audit and Certification of ISMSs

ISO 27001 & ISO 27002

4

duyn@uit.edu.vn

ISO 27001

- ISO 27001 formally specifies a management system that is intended to bring information security under explicit management control

ISO 27002

- ISO 27002 provides best practice recommendations on information security management for use by those responsible for initiating, implementing or maintaining Information Security Management Systems (ISMS)

Nội dung

5

duyn@uit.edu.vn

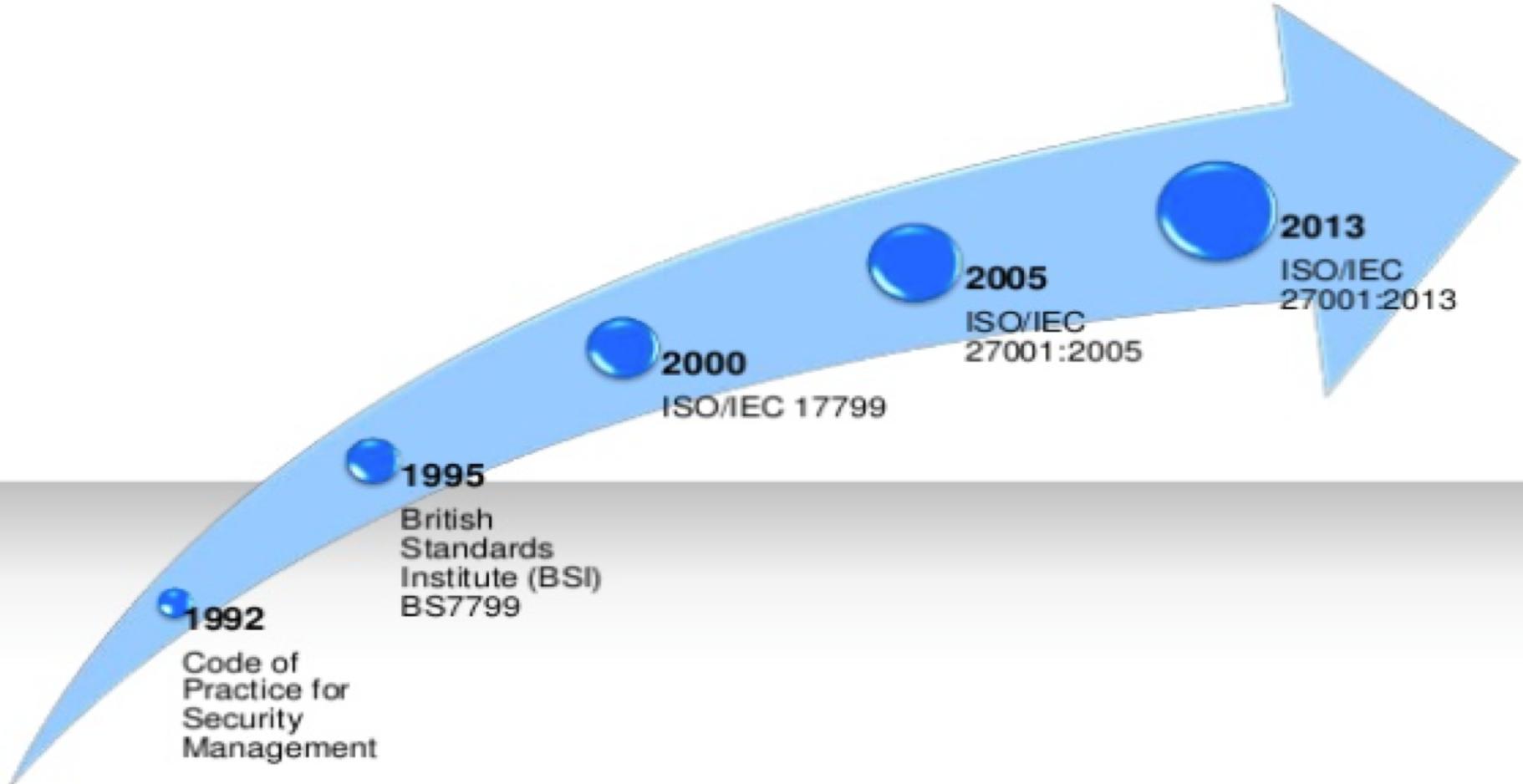
- Lịch sử hình thành ISO 27000
- **ISO 27001**
- ISO 27002

ISO 27001

Lịch sử hình thành

6

duyn@uit.edu.vn



ISO 27001

Tổng quan

7

duyn@uit.edu.vn

- Giúp xây dựng Hệ Thống Quản Lý Bảo Mật Thông Tin (Information Security Management System - ISMS)
- Cung cấp cách thức theo dõi và duy trì:
 - Tính bảo mật của thông tin
 - Tính toàn vẹn của thông tin
 - Tính sẵn sàng của thông tin

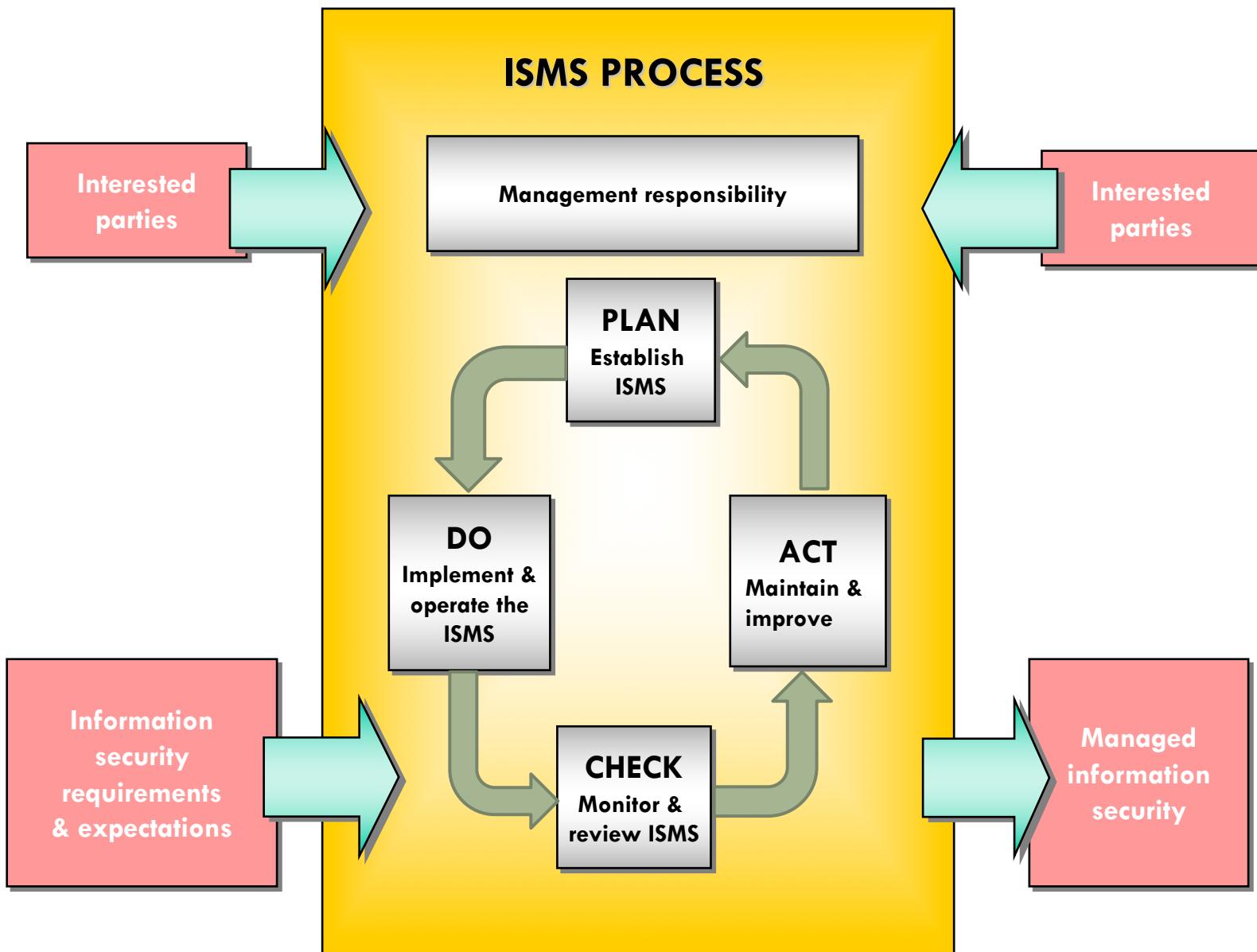
ISO 27001

Tổng quan

8

duyn@uit.edu.vn

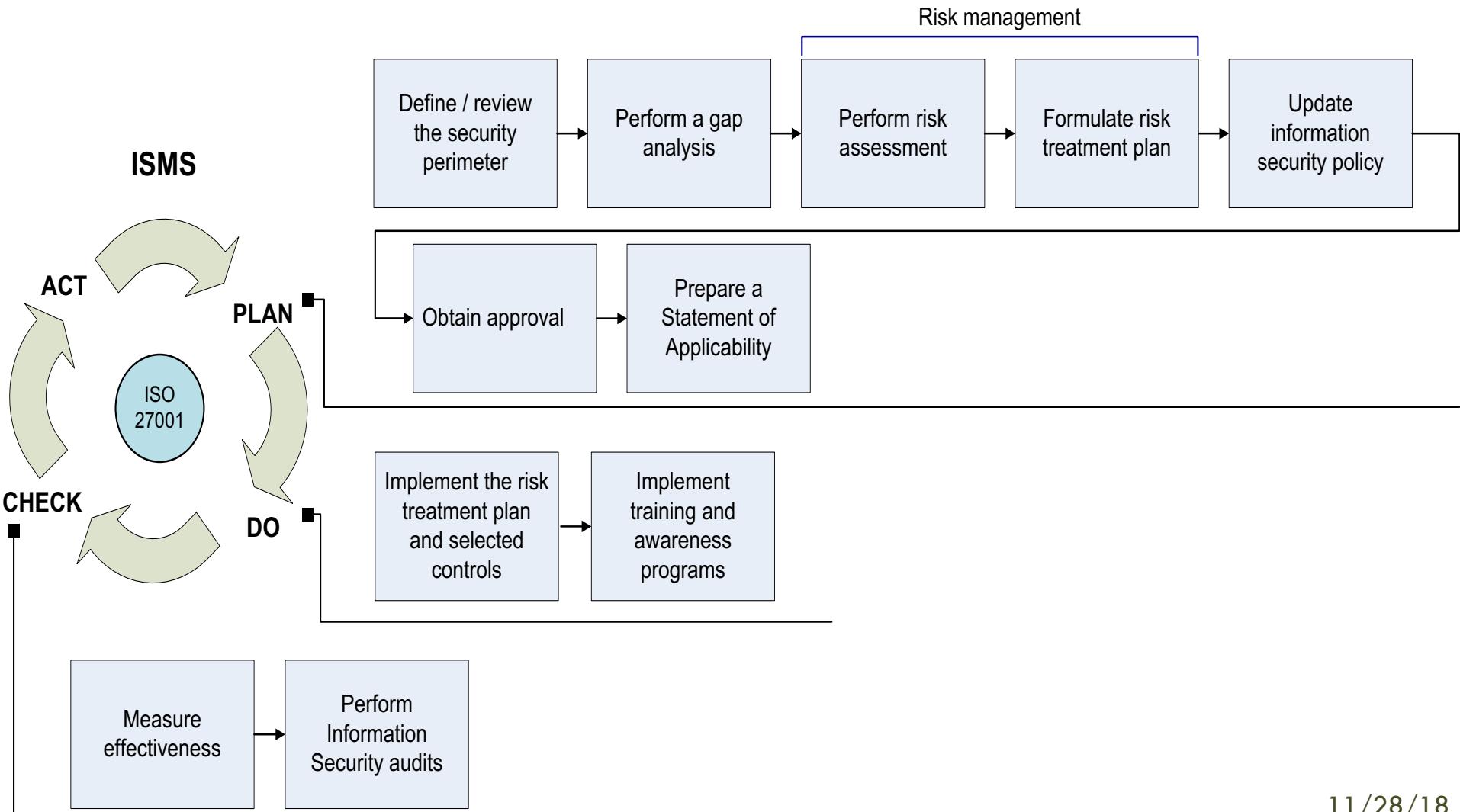
- Thiết kế và triển khai ISMS sẽ chịu ảnh hưởng bởi:
 - Mục đích bảo mật và mục đích kinh doanh
 - Những yêu cầu về quản lý rủi ro
 - Qui mô của tổ chức



ISO 27001 & Risk Management

10

duyn@uit.edu.vn

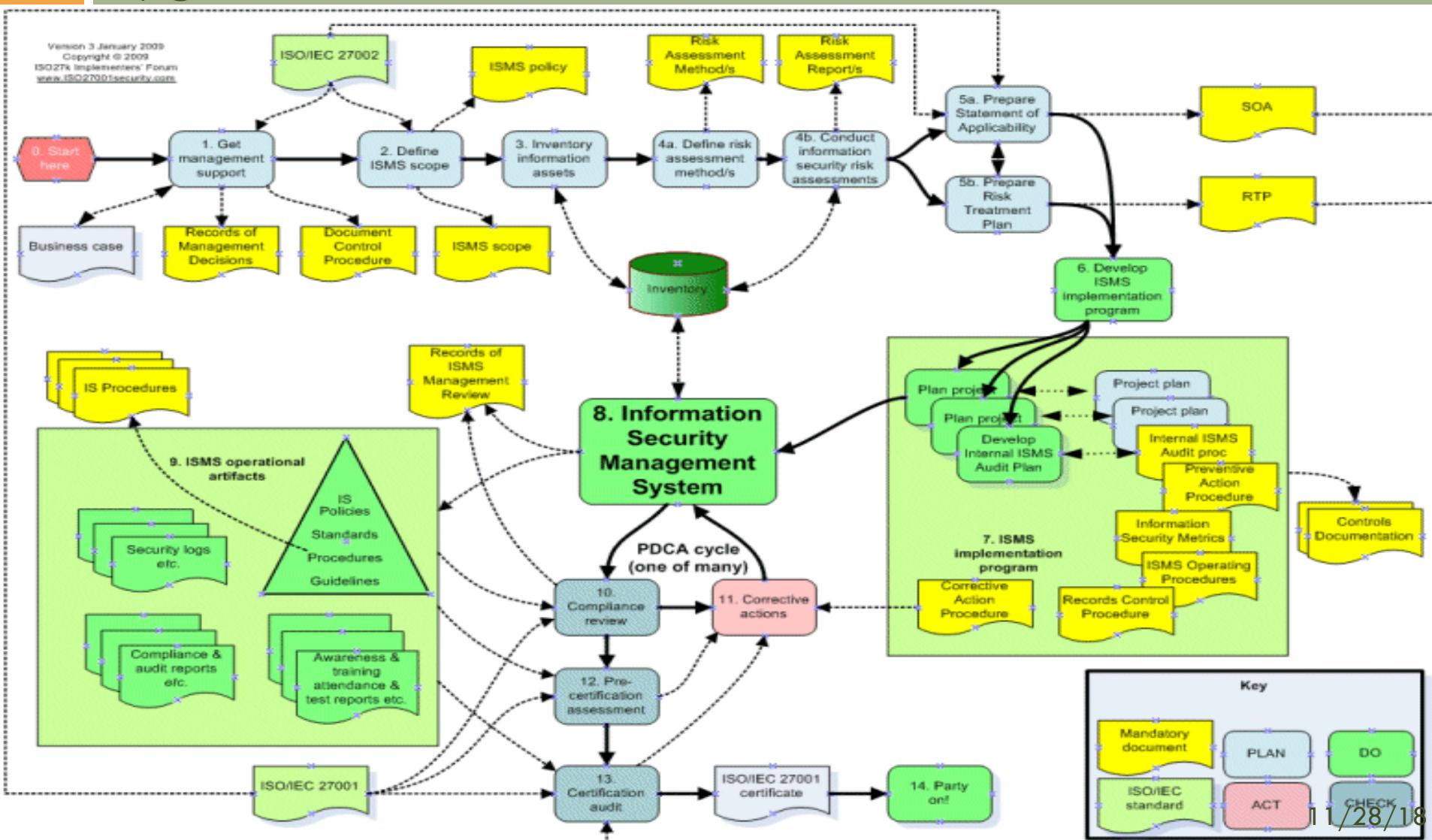


ISO 27001

Qui trình triển khai ISO27001

11

duyn@uit.edu.vn



Management Support (Sự hỗ trợ quản lý)

duyn@uit.edu.vn

- Định hướng rõ ràng của công ty về việc hỗ trợ trong xây dựng giải pháp an toàn thông tin
- Sự cam kết và hỗ trợ của tổ chức trong quá trình triển khai giải pháp an toàn thông tin:
 - Cung cấp tài nguyên
 - Ban hành chính sách

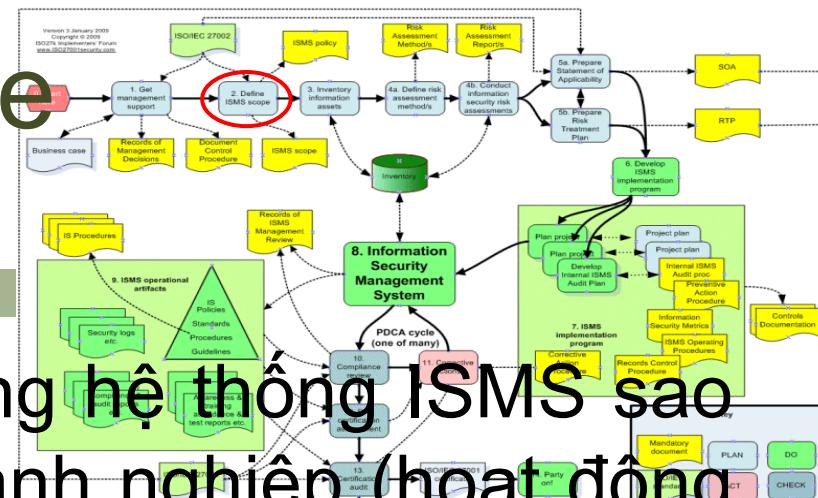


Defining ISMS scope (Định nghĩa ISMS)

13

duyn@uit.edu.vn

- Xác định phạm vi xây dựng hệ thống ISMS sao cho phù hợp nhất với doanh nghiệp (hoạt động kinh doanh, vị thế của doanh nghiệp, tài sản doanh nghiệp).
- Những gì không thực hiện được cần giải thích rõ ràng trong tài liệu Statement of Applicability (SOA)

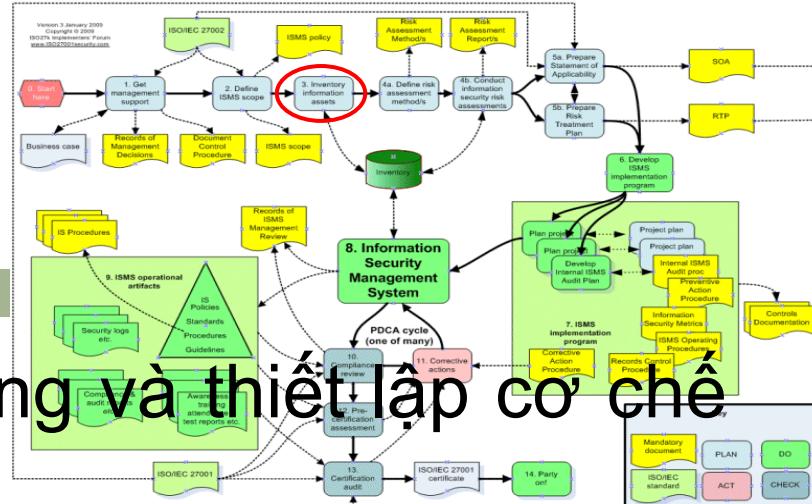


Inventory of Assets (Thống kê tài sản)

14

duyn@uit.edu.vn

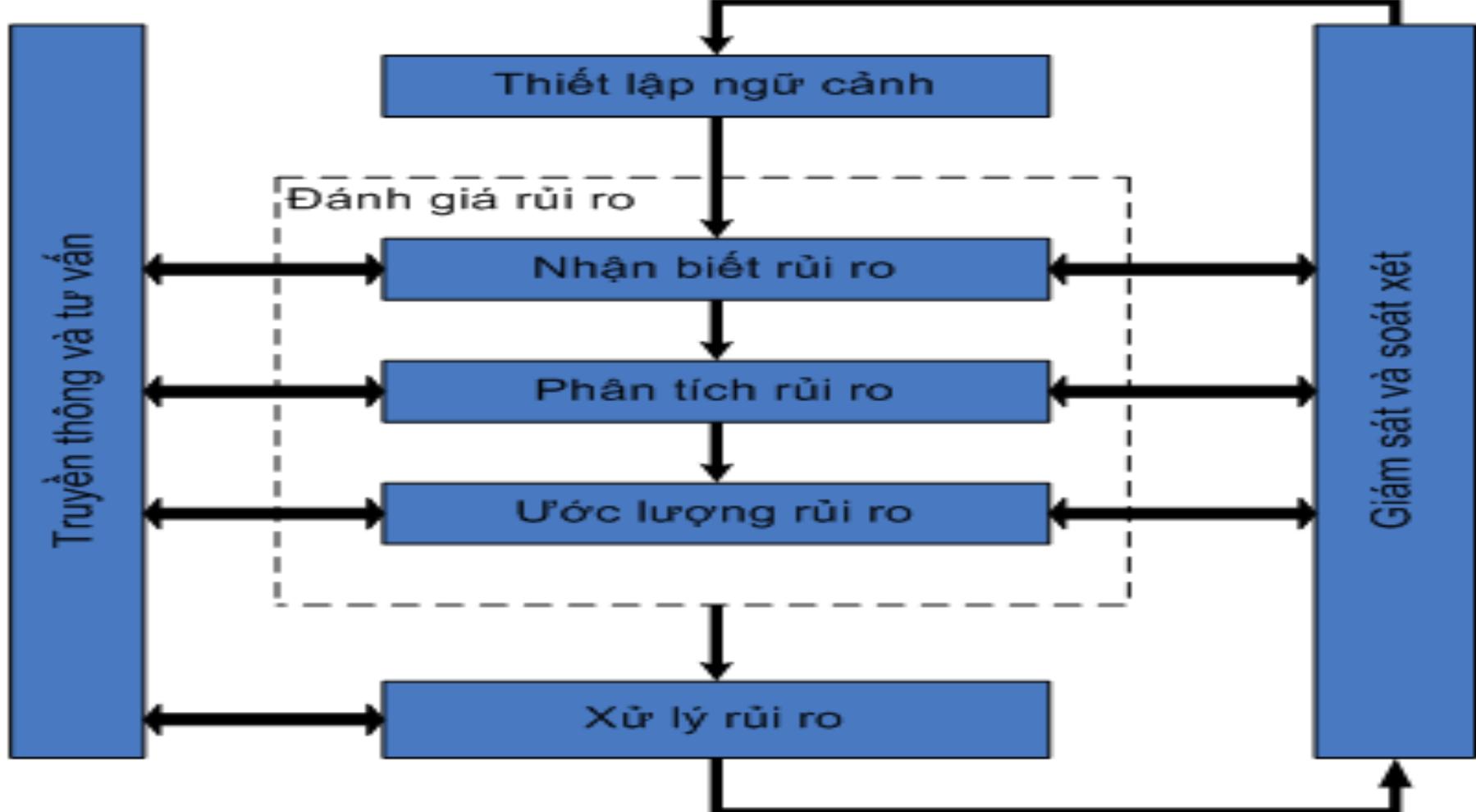
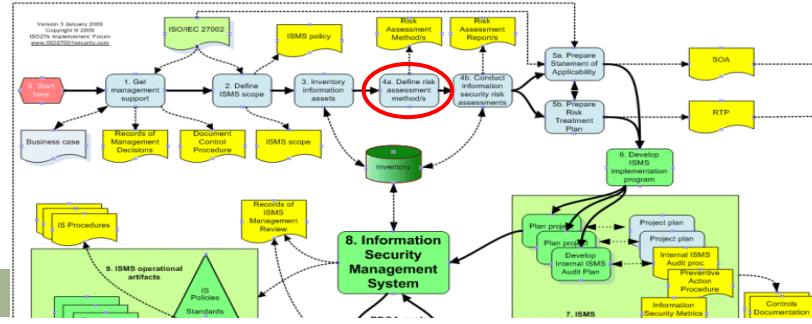
- Thống kê tài sản quan trọng và thiết lập cơ chế sử dụng, theo dõi chi tiết:
 - Physical (phần cứng)
 - Software (phần mềm)
 - People (con người)
 - Services (dịch vụ)
 - Intangibles (vô hình)



Risk Assessment (Đánh giá rủi ro)

15

duyn@uit.edu.vn

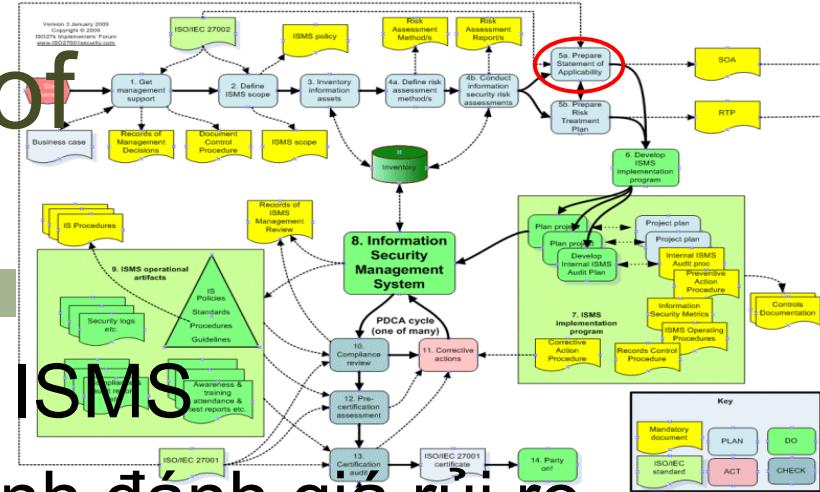


Prepare Statement of Applicability

16

duyn@uit.edu.vn

- SOA là tài liệu chính trong ISMS
- SOA là kết quả của quá trình đánh giá rủi ro
- SOA liệt kê mục tiêu quan trọng cần làm trong quá trình bảo mật thông tin
- SOA liệt kê những qui trình thực hiện cần thực hiện những mục tiêu
- SOA liệt kê những giải pháp cần xử phạt khi vi phạm chính sách

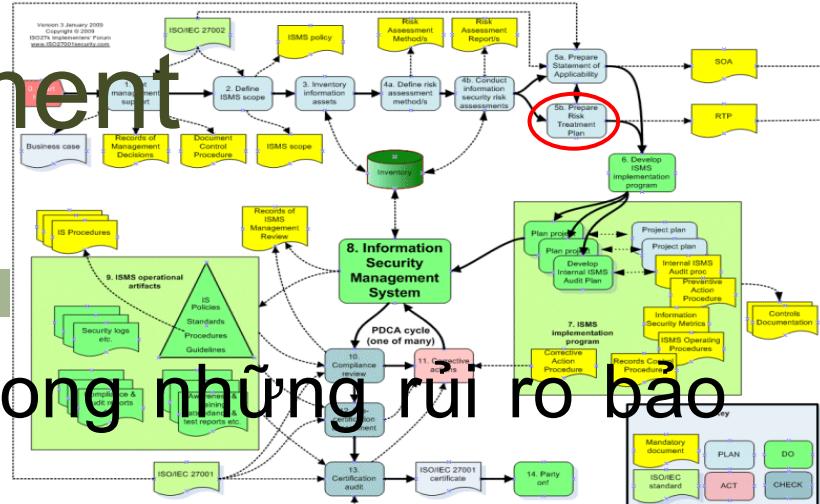


Prepare Risk Treatment Plan

17

duyn@uit.edu.vn

- Xác định thứ tự ưu tiên trong những rủi ro bảo mật.
- Phân tán trách nhiệm nhưng có sự quản lý một cách chặt chẽ.
- Chính sách ban hành toàn bộ công ty:
 - Người đứng đầu
 -
 - Người thấp nhất

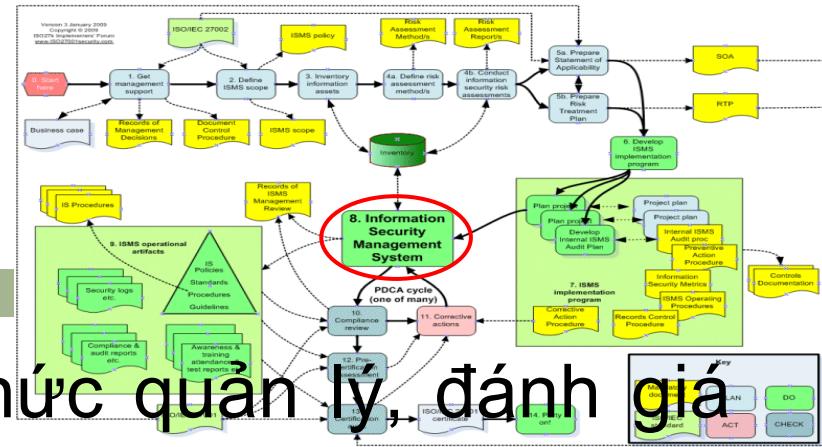


The ISMS

18

duyn@uit.edu.vn

- Mỗi quan hệ giữa cách thức quản lý, đánh giá rủi ro, xử lý rủi ro
- Tài liệu ISMS:
 - Chính sách và mục tiêu của ISMS
 - Phạm vi ISMS
 - Mô tả cách thức đánh giá rủi ro
 - Mô tả cách thức giảm thiểu, tránh rủi ro và kết quả
 - Sự ảnh hưởng của doanh nghiệp khi thực hiện ISMS

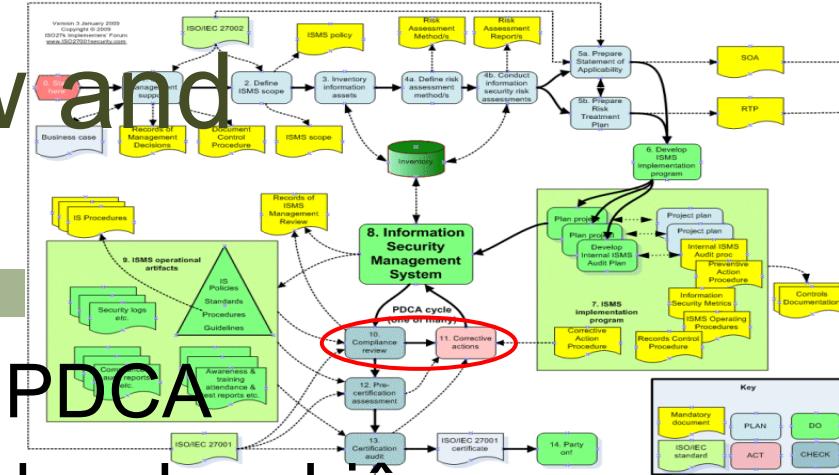


Compliance Review and Corrective Actions

19

duyn@uit.edu.vn

- Xem lại qui trình áp dụng PDCA
- Cải tiến cho phù hợp với doanh nghiệp

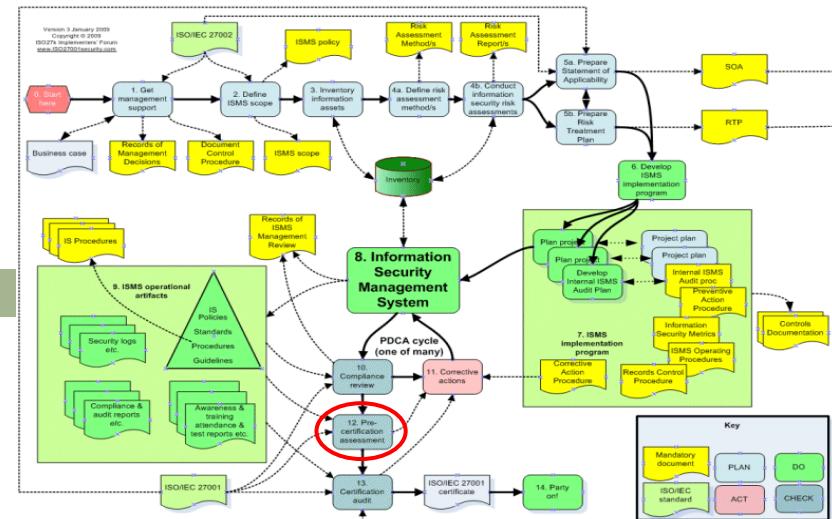


Pre-Certification Assessment

20

duyn@uit.edu.vn

➤ Đánh giá lợi ích



Nội dung

21

duyn@uit.edu.vn

- Lịch sử hình thành ISO 27000
- ISO 27001
- **ISO 27002**

ISO 27002

22

duyn@uit.edu.vn

- Có cái nhìn tổng quan về vấn đề ATTT
- ISO 27002 là chuẩn quốc tế về hướng dẫn thực hiện quản lý an toàn thông tin và đề cập đến mọi thành phần trong doanh nghiệp có ảnh hưởng đến ATTT





- 14 Control Areas
- 34 Control Objectives
- 114 Control Points

Organizing information security

- Xác định các mục tiêu an ninh thông tin đáp ứng yêu cầu của tổ chức.
- Thiết lập phạm vi của ISMS
- Đảm bảo đủ nguồn lực được cung cấp để phát triển, thực hiện, vận hành và duy trì ISMS.
- Phương pháp đánh giá hiệu quả khi triển khai ISMS.
- Phân rõ vai trò và trách nhiệm của từng bộ phận, từng cá nhân trong qui trình đảm bảo an ninh thông tin.

Asset management

26

duyn@uit.edu.vn

- Mục tiêu kiểm soát này là "để đạt được và duy trì mức độ bảo vệ thích hợp tài sản của tổ chức"
 - Thống kê tài sản
 - Chủ sở hữu tài sản
 - Mục tiêu sử dụng tài sản
 - Phân loại thông tin
 - Mức độ bảo mật cho từng trạng thái của dữ liệu

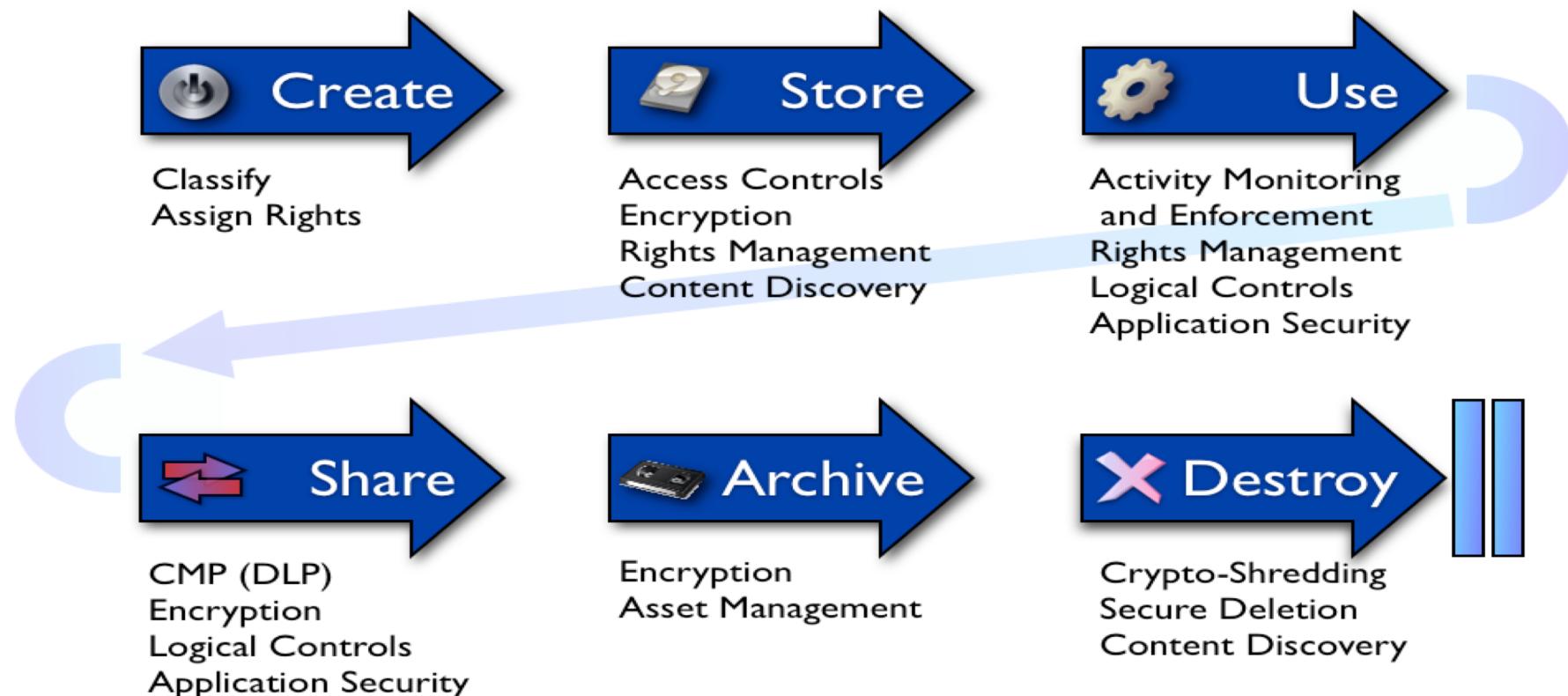
ISO 27002

Asset management

27

duyn@uit.edu.vn

Data Security Lifecycle



Human resources security

➤ Trước khi tuyển dụng:

- Đảm bảo rằng các nhân viên, nhà thầu và các bên thứ ba hiểu rõ trách nhiệm của mình và phù hợp với vai trò được giao, đồng thời giảm thiểu các rủi ro về việc đánh cắp, gian lận hoặc lạm dụng chức năng, quyền hạn
 - Điều khoản và điều kiện tuyển dụng
 - Vai trò và trách nhiệm
 - Sàng lọc

Human resources security

29

duyn@uit.edu.vn

➤ Trong quá trình làm việc:

➤ Đảm bảo rằng mọi nhân viên của tổ chức, nhà thầu và bên thứ ba nhận thức được các mối nguy cơ và các vấn đề liên quan tới an toàn thông tin, trách nhiệm và nghĩa vụ pháp lý của họ, và được trang bị các kiến thức, điều kiện cần thiết nhằm hỗ trợ chính sách an toàn thông tin của tổ chức trong quá trình làm việc, và giảm thiểu các rủi ro do con người gây ra

- Trách nhiệm ban quản lý
- **Nhận thức, giáo dục và đào tạo về an toàn thông tin**
- Xử lý kỷ luật

Human resources security

➤ Sau quá trình làm việc:

- Nhằm đảm bảo rằng các nhân viên của tổ chức, nhà thầu và các bên thứ ba nghỉ việc hoặc thay đổi vị trí một cách có tổ chức.
 - Trách nhiệm kết thúc hợp đồng
 - Bàn giao tài sản
 - **Hủy bỏ quyền truy cập**

Physical and environmental security

- Theo dõi và giới hạn việc truy cập để phát hiện, tránh và giảm thiểu tối đa các truy cập trái phép làm ảnh hưởng đến hệ thống.
- Danh sách những người được truy cập vào những khu vực an toàn phải được xem xét và phê duyệt và phê duyệt bởi người quản trị, bộ phận bảo mật thiết bị và có sự kiểm tra chéo của những người quản lý giữa các bộ phận đó.
- Cấm chụp ảnh hoặc ghi hình

Physical and environmental security

32

duyn@uit.edu.vn

- Ghi nhận đối tượng, thời gian và mục đích truy cập của từng đối tượng.
- Danh sách những người được truy cập vào những khu vực an toàn phải được xem xét và phê duyệt bởi người quản trị, bộ phận bảo mật thiết bị và có sự kiểm tra chéo của những người quản lý giữa các bộ phận đó.
- Cấm chụp ảnh hoặc ghi hình
- Sử dụng thẻ từ và thời gian truy cập để kiểm soát việc truy cập.

ISO 27002

Access control

33

duyn@uit.edu.vn

- Nhằm đảm bảo người dùng hợp lệ được truy cập và ngăn chặn những người dùng không hợp lệ truy cập trái phép đến hệ thống thông tin.
 - Vật lý
 - Mạng
 - Hệ điều hành
 - Ứng dụng

ISO 27002

Access control

34

duyn@uit.edu.vn

- Quản lý truy cập mạng:
 - Phân vùng mạng
 - Bảo vệ cổng cấu hình
 - Định danh thiết bị trong các mạng
 - Chính sách sử dụng các dịch vụ mạng
 - Xác thực người dùng cho các kết nối bên ngoài
 - Quản lý kết nối mạng
 - Quản lý định tuyến mạng
 - Log

ISO 27002

Access control

35

duyn@uit.edu.vn

- Quản lý truy cập hệ điều hành và ứng dụng:
 - Các thủ tục đăng nhập an toàn
 - Định danh và xác thực người dùng
 - Hệ thống quản lý mật khẩu
 - Thời gian giới hạn của phiên làm việc
 - Giới hạn thời gian kết nối
 - Log

ISO 27002

Systems acquisition, development and maintenance

36

duyn@uit.edu.vn

- Tính đúng đắn trong xử lý của các ứng dụng
 - Nhằm ngăn chặn các lỗi, mất mát, sửa đổi hoặc sử dụng trái phép thông tin trong các ứng dụng.
 - Kiểm tra tính hợp lệ của dữ liệu nhập vào
 - Kiểm soát việc xử lý nội bộ
 - Tính toàn vẹn thông điệp
 - Kiểm tra tính hợp lệ của dữ liệu đầu ra

➤ Quản lý CIA

- Nhằm bảo vệ tính bí mật, xác thực hoặc toàn vẹn của thông tin bằng các biện pháp mã hóa.
 - Chính sách sử dụng các biện pháp quản lý mã hóa
 - Quản lý khóa

ISO 27002

Systems acquisition, development and maintenance

38

duyn@uit.edu.vn

- Bảo đảm an toàn trong các quy trình hỗ trợ và phát triển
 - Các thủ tục quản lý thay đổi
 - Kiểm soát kỹ thuật các ứng dụng sau thay đổi của hệ thống điều hành.
 - Hạn chế thay đổi các gói phần mềm
 - Sự rò rỉ thông tin
 - Phát triển phần mềm thuê khoán

ISO 27002

Systems acquisition, development and maintenance

39

duyn@uit.edu.vn

- Quản lý các điểm yếu về kỹ thuật
 - Nhằm giảm thiểu các mối nguy hiểm xuất phát từ việc tin tặc khai thác các điểm yếu kỹ thuật đã được công bố

Business continuity management

- Chống lại các gián đoạn trong hoạt động nghiệp vụ và bảo vệ các quy trình hoạt động trọng yếu khỏi các ảnh hưởng do lỗi hệ thống thông tin hay các thảm họa và đảm bảo khả năng khôi phục các hoạt động bình thường đúng lúc.
- Đánh giá rủi ro và sự liên tục trong hoạt động của tổ chức
- Kiểm tra, bảo trì và đánh giá lại các kế hoạch đảm bảo sự liên tục trong hoạt động của tổ chức

ISO 27002

Compliance

41

duyn@uit.edu.vn

- Nhằm tránh sự vi phạm pháp luật, quy định, nghĩa vụ theo các hợp đồng đã ký kết, các yêu cầu về bảo đảm an toàn thông tin.
 - Xác định các điều luật hiện đang áp dụng được
 - Quyền sở hữu trí tuệ (IPR)
 - Bảo vệ các hồ sơ tổ chức
 - Bảo vệ dữ liệu và sự riêng tư của thông tin cá nhân
 - Ngăn ngừa việc lạm dụng phương tiện xử lý thông tin