QUẢN LÝ AN TOÀN THÔNG TIN

BÀI 6:
MÔ HÌNH QUẢN LÝ AN TOÀN

Nội dung

- Mô hình kiểm soát truy cập
- Mô hình kiến trúc an toàn
- Mô hình quản lý bảo mật

Mục tiêu

- Mô tả được cốt lõi trong bản thiết kế , chương trình khung và mô hình quản lý ATTT, bao gồm những mô hình được công nhận tại Mỹ
- Giải thích được tại sao kiểm soát truy cập là một yếu tố thiết yếu của quản lý ATTT
- Có thể đề xuất mô hình quản lý ATTT và giải thích cách nó có thể được tùy chỉnh để đáp ứng nhu cầu của từng tổ chức cụ thể
- Mô tả các yếu tố cơ bản của các phương pháp quản lý ATTT chính

Bản thiết kế, khuôn mẫu và mô hình an toàn

Blue prints

- Bản kế hoạch
  - Để tạo và duy trì môi trường an toàn: phải thiết kế một kế hoạch bảo mật và sau đó triển khai một mô hình quản lý để thực hiện và duy trì kế hoạch đó.
- Bắt đầu bằng việc tạo hoặc xác nhận khung an toán thông tin.
  - Xây dựng kế hoạch chi tiết về an toàn thông tin.

Khung

- Là phác thảo của kế hoạch chi tiết kỹ lưỡng hơn. Đó là cơ sở cho việc thiết kế, lựa chọn và thực hiện tất cả các biện pháp kiểm soát an ninh tiếp theo.
- Để tạo ra một kế hoạch chi tiết về bảo mật, hầu hết các tổ chức dựa trên các mô hình và thực tiễn bảo mật đã được thiết lập.

Mô hình an toàn

- Mô hình an toàn
  - Là một bản thiết kế chung được cung cấp bởi một tổ chức dịch vụ.
  - Một số mô hình này là độc quyền và chỉ có sẵn với một khoản phí đáng kể; một số khác khác tương đối rẻ.
  - Ví dụ: ISO, NIST

- Mô hình bạn chọn thì phải linh hoạt, có thể mở rộng, mạnh mẽ và đủ chi tiết.

- Có một cách khác để tạo một kế hoạch chi tiết là xem xét các cách làm do các tổ chức khác thực hiện.

Mô hình kiểm soát truy cập

Mô hình kiểm soát truy cập

- Kiểm soát truy cập
  - Qui định việc tiếp nhận người dùng vào các khu vực đáng tin cậy của tổ chức, truy cập hợp lý vào **hệ thống thông tin** và **truy cập vật lý** vào cơ sở vật chất của tổ chức.
  - Kiểm soát truy cập là một cách để đảm bảo người dùng đúng như họ nói và chỉ có thể truy cập những gì họ được phép
- 4 yếu tố
  - Nhận dạng.
  - Xác thực.
  - Ủy quyền.
  - Trách nhiệm giải trình.

Mô hình kiểm soát truy cập

- Một số nguyên tắc chính:
  - **Least privilege**: thành viên của tổ chức chỉ có thể truy cập lượng thông tin tối thiểu trong khoảng thời gian tối thiểu cần thiết để thực hiện các nhiệm vụ được yêu cầu của họ.
  - **Need-to-know**: giới hạn quyền truy cập của người dùng vào thông tin cần thiết để thực hiện nhiệm vụ được giao hiện tại, và không chỉ vào loại dữ liệu cần thiết cho một chức năng công việc chung.
  - **Separation of duties**: yêu cầu các nhiệm vụ quan trọng phải được phân chia theo cách nhiều hơn một cá nhân chịu trách nhiệm về việc hoàn thành của họ.

Hạng mục kiểm soát truy cập

Hạng mục kiểm soát truy cập

- Preventative (Phòng ngừa)
- Deterrent (Răn đe)
- Detective (Phát hiện)
- Corrective (Khắc phục)
- Recovery (Khôi phục)
- Compensating (Bù trừ)

Phòng ngừa – Cảnh báo – Phát hiện

Phòng ngừa

- Firewalls / Anti-virus software
- Mã hóa
- Thẻ từ

Cảnh báo

- Biển cảnh báo
- Phân chia nhiệm vụ

Phát hiện

- Giám sát và ghi lại các sự kiện
- Không ảnh hưởng đến các sự kiện khác

Khắc phục – Khôi phục

Khắc phục

- Kiểm soát sau sự kiện để ngăn tái diễn
- Ví dụ: (Nếu được triển khai sau khi sự cố diễn ra)
  - Spam filter
  - Anti-virus on e-mail server
  - WPA Wi-Fi encryption

Khôi phục

- Khôi phục sau khi đã xảy ra sự cố

Compensating Controls

Kiểm soát được đưa ra để bù đắp cho sự thiếu sót, hỗ trợ chính sách an ninh.

Ví dụ:

- Giám sát hàng ngày
- Đánh giá hàng tháng về thông tin đăng nhập quản trị
- Sử dụng Web Application Firewall ngăn chặn lỗ hổng

Phân loại

Kĩ thuật (Technical)

Triển khai (Operational)

Quản lý (Management)

	Deterrent	Preventative	Detective	Corrective	Recovery	Compensating
Management	Policies	Registration procedures	Periodic violation report reviews	Employee or account termination	Disaster recovery plan	Separation of duties, job rotation
Operational	Warning signs	Gates, fences, and guards	Sentries, CCTVs	Fire suppression systems	Disaster recovery procedures	Defense in depth
Technical	Warning banners	Login systems, Kerberos	Log monitors and IDPSs	Forensics procedures	Data backups	Key logging and keystroke monitoring

Mô hình kiểm soát truy cập

Mô hình kiểm soát truy cập bắt buộc (MAC)

- Phân loại dữ liệu, người dùng dựa theo các lớp bảo mật.
- Lớp bảo mật có thể được phân loại theo:
  - Mức bảo mật (Classification level)
  - Lĩnh vực (Category)
- Các mức bảo mật cơ bản: TopSecret > Secret > Classify > Unclassified

Mô hình kiểm soát truy cập bắt buộc (MAC)

- Lĩnh vực:
  - Phân loại người dùng và dữ liệu theo lĩnh vực hoạt động của hệ thống, hoặc theo từng phòng ban trong một tổ chức.
  - Ví dụ: Một công ty có 3 phòng ban là: Phòng kinh doanh, phòng sản xuất và phòng phân phối. Như vậy thì các người dùng và dữ liệu trong công ty này có thể được phân loại theo lĩnh vực dựa theo 3 phòng ban này

Mô hình kiểm soát truy cập bắt buộc (MAC)

- Khi MAC được triển khai, chủ sở hữu dữ liệu bị hạn chế quyền truy cập/sử dụng tài nguyên.

- Nguyên tác: Không đọc lên – Không ghi xuống

Kiểm soát truy cập tùy ý (DAC)

- Chủ sở hữu của một đối tượng kiểm soát ai và những gì có thể truy cập vào nó.
- Ví dụ: Unix file

Kiểm soát truy cập không tùy ý

- Điều khiển dựa trên vai trò được gắn với vai trò mà một người dùng cụ thể thực hiện trong một tổ chức

- Điều khiển dựa trên nhiệm vụ bị ràng buộc với một nhiệm vụ hoặc trách nhiệm cụ thể.

Các hình thức kiểm soát truy cập khác

- Content-dependent access controls (Kiểm soát truy cập phụ thuộc vào nội dung)
- Constrained user interfaces (Giao diện người dùng bị ràng buộc)
- Temporal (time-based) isolation (dựa trên thời gian) - Trong một số trường hợp, quyền truy cập thông tin bị giới hạn bởi sự ràng buộc về thời gian trong ngày.

Mô hình kiến trúc bảo mật

Mô hình kiến trúc bảo mật

- Có thể giúp các tổ chức nhanh chóng thực hiện các cải tiến thông qua sự thích ứng
- Liên quan đến:
  - Phần cứng và phần mềm máy tính
  - Chính sách và thực hành
  - Tính bảo mật của thông tin
  - Tính toàn vẹn của thông tin

Mô hình kiến trúc an toàn

- Để chứng nhận bảo mật máy tính
- Quy trình CC đảm bảo rằng đặc điểm kỹ thuật, việc triển khai và đánh giá các sản phẩm bảo mật máy tính được thực hiện một cách nghiêm ngặt và tiêu chuẩn.

Tiêu chuẩn chung

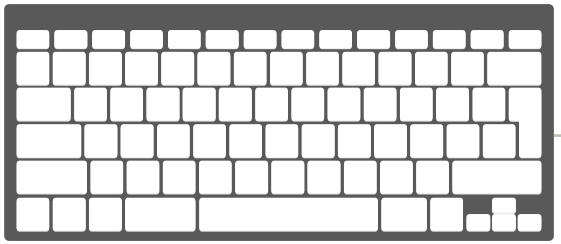
TIÊU CHUẨN CHUNG

Mục tiêu đánh giá (ToE)	Hệ thống đang được đánh giá
Hồ sơ bảo vệ (PP)	Đặc điểm kỹ thuật do người dùng tạo cho các yêu cầu bảo mật
Mục tiêu bảo mật (ST)	Tài liệu mô tả thuộc tính bảo mật của ToE
Các yêu cầu chức năng bảo mật (SFRs)	Danh mục các chức năng bảo mật của sản phẩm
Mức độ đảm bảo đánh giá (EAL)	Đánh giá hoặc xếp loại của ToE sau khi đánh giá

Mô hình kiến trúc an toàn

- Mô hình bảo mật Bell-LaPadula(BLP)
- Mô hình toàn vẹn Biba
- Mô hình toàn vẹn của Clark-Wilson
- Mô hình kiểm soát truy cập Graham-Denning
- Mô hình Harrison-Ruzzo-Ullman
- Mô hình Brewer-Nash (Bức tường Trung Quốc)

Các mô hình bảo mật



Mô hình bảo mật Bell-LaPadula

- Mô hình tham chiếu đảm bảo tính bí mật của hệ thống bằng cách sử dụng MAC, phân loại dữ liệu và độ an toàn.
- Qui tắc Đọc xuống – Ghi lên.

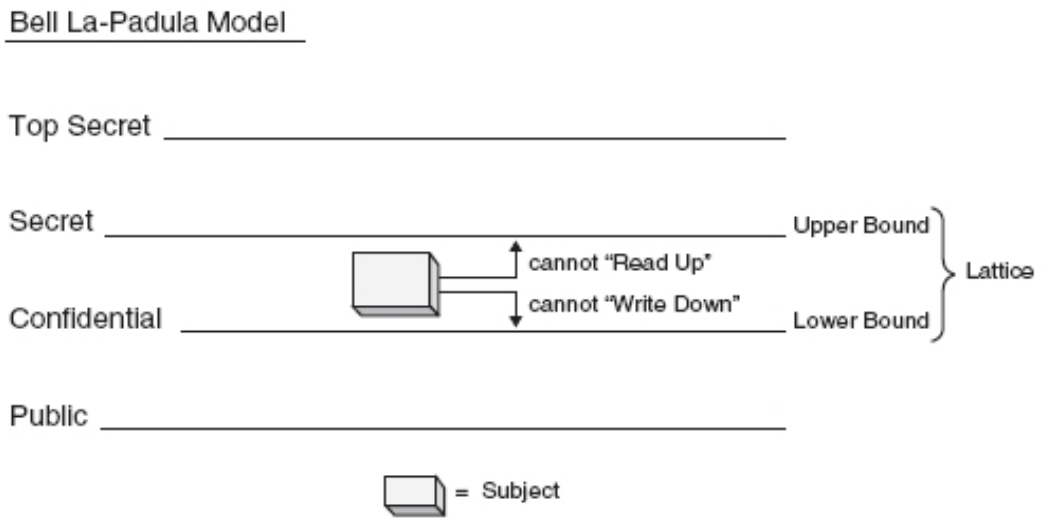


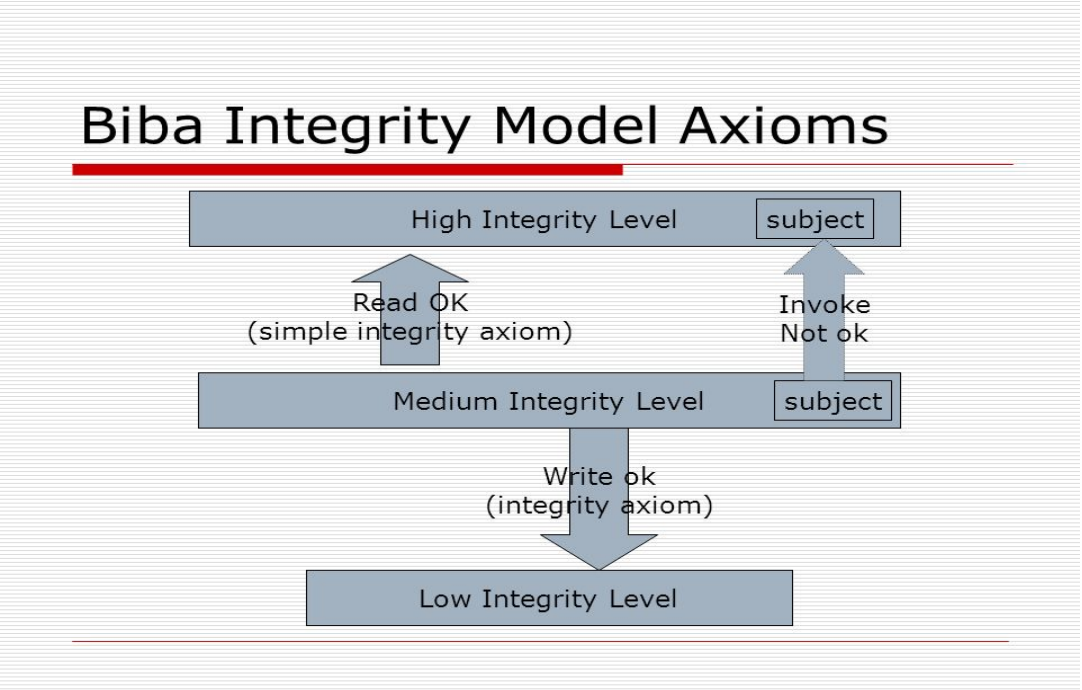
Figure 5-14 In the Bell-LaPadula model, each subject has a lattice of rights.

Mô hình toàn vẹn Biba

- Mục tiêu của mô hình BIBA là duy trì tính toàn vẹn của dữ liệu.
- Dữ liệu và chủ thể được sắp xếp theo mức độ toàn vẹn của chúng
- Đảm bảo không có thông tin nào từ một chủ thể có thể được chuyển cho một đối tượng ở mức độ bảo mật cao hơn.

- Đọc lên –

Ghi xuống



Mô hình Clark-Wilson

- Mô hình này cũng nhắm đến việc duy trì tính toàn vẹn của dữ liệu. Trong mô hình này, dữ liệu được chia thành 2 loại:
  - Có ràng buộc: chủ thể cần đáp ứng đủ điều kiện mới có thể truy cập.
  - Không ràng buộc: mọi chủ thể có thể truy cập mà không cần điều kiện gì.

- Dựa trên các nguyên tắc kiểm soát thay đổi hơn ở mức toàn vẹn, được thiết kế cho môi trường thương mại.

Mô hình kiểm soát truy cập Graham-Denning

- Có 3 phần:
  - Tập các đối tượng
  - Tập các chủ thể (quá trình và domain)
  - Tập các luật

- Quyền bảo vệ:
  - Tạo hoặc xóa đối tượng, Tọa hoặc xóa chủ thể.
  - Quyền đọc , quyền truy cập, xóa quyền, chuyển quyền.

Mô hình Harrison - Ruzzo - Ullman

- Xác định một phương pháp cho phép các thay đổi đối với quyền truy cập và việc thêm bớt các chủ thể và đối tượng.
  - Vì các hệ thống thay đổi theo thời gian nên trạng thái bảo vệ của chúng cần thay đổi.
- Dựa trên ma trận kiểm soát truy cập.

- Bao gồm một tập hợp các quyền chung và một tập hợp các lệnh cụ thể.

- Mô hình Harrison-Ruzzo-Ullman (HRU) xác định một phương pháp cho phép thay đổi quyền truy cập và thêm và bớt các chủ thể và đối tượng, một quá trình mà mô hình BLP không làm.
- Mô hình HRU được định nghĩa như sau:
  - Tập chủ thể S
  - Tập đối tượng O
  - Tập quyền truy cập R
  - Ma trận truy cập M | M = (Mso) sÎS, oÎO | Mso Î R
- HRU được xây dựng trên ma trận kiểm soát truy cập và bao gồm một tập hợp các quyền chung và một tập hợp các lệnh cụ thể. Gồm:
  - Tạo chủ đề/ tạo đối tượng
  - Nhập ngay X vào
  - Xóa ngay X khỏi
  - Hủy chủ đề / hủy đối tượng
- Bằng cách thực hiện tập hợp các quyền và lệnh này và giới hạn các lệnh trong một thao tác duy nhất, có thể xác định xem và khi nào một chủ thể cụ thể có thể có được một quyền cụ thể đối với một đối tượng.

Mô hình Brewer-Nash (Chinese Wall)

- Người dùng chỉ có thể truy cập dữ liệu mà không xung đột với dữ liệu mà họ truy cập trước đó.

- Mô hình này thường được các công ty tư vấn và kế toán sử dụng

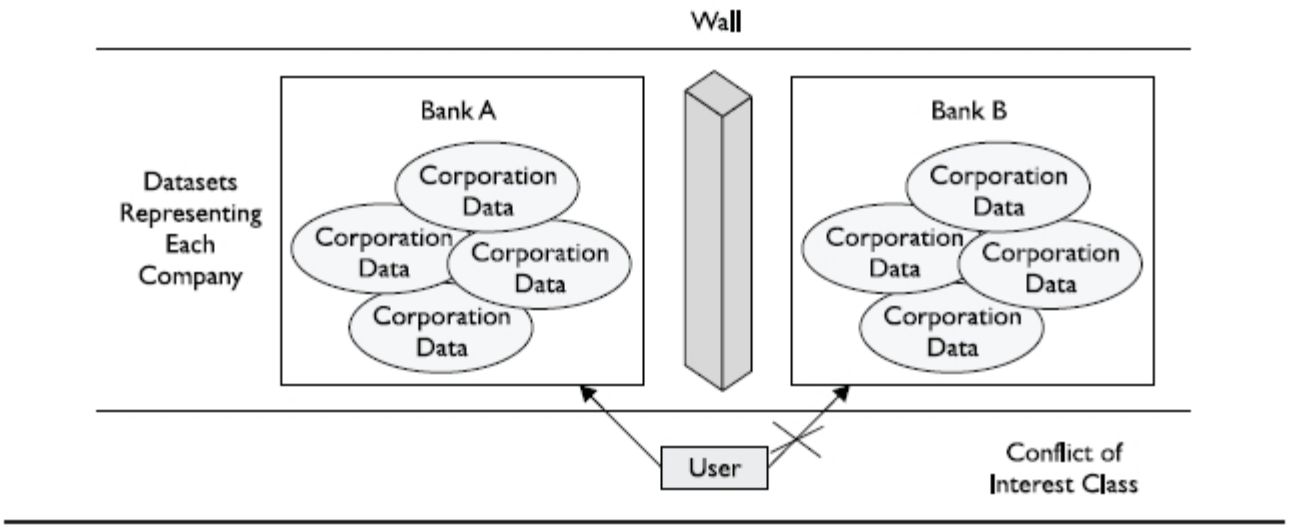


Figure 5-15 The Chinese Wall model provides dynamic access controls.

Mô hình quản lý an toàn

Một mô hình quản lý ATTT

- Là 1 bản thiết kế chung được cung cấp bởi 1 tổ chức dịch vụ.
- Có thể sử dụng các mô hình bảo mật như một phác thảo cho một thiết kế toàn diện của toàn bộ chương trình bảo mật đã được lên kế hoạch của một tổ chức hoặc làm điểm khởi đầu cho một phiên bản tùy chỉnh đầy đủ hơn.
- Không phải mô hình nào cũng là miễn phí.

MÔ HÌNH QUẢN LÝ ATTT

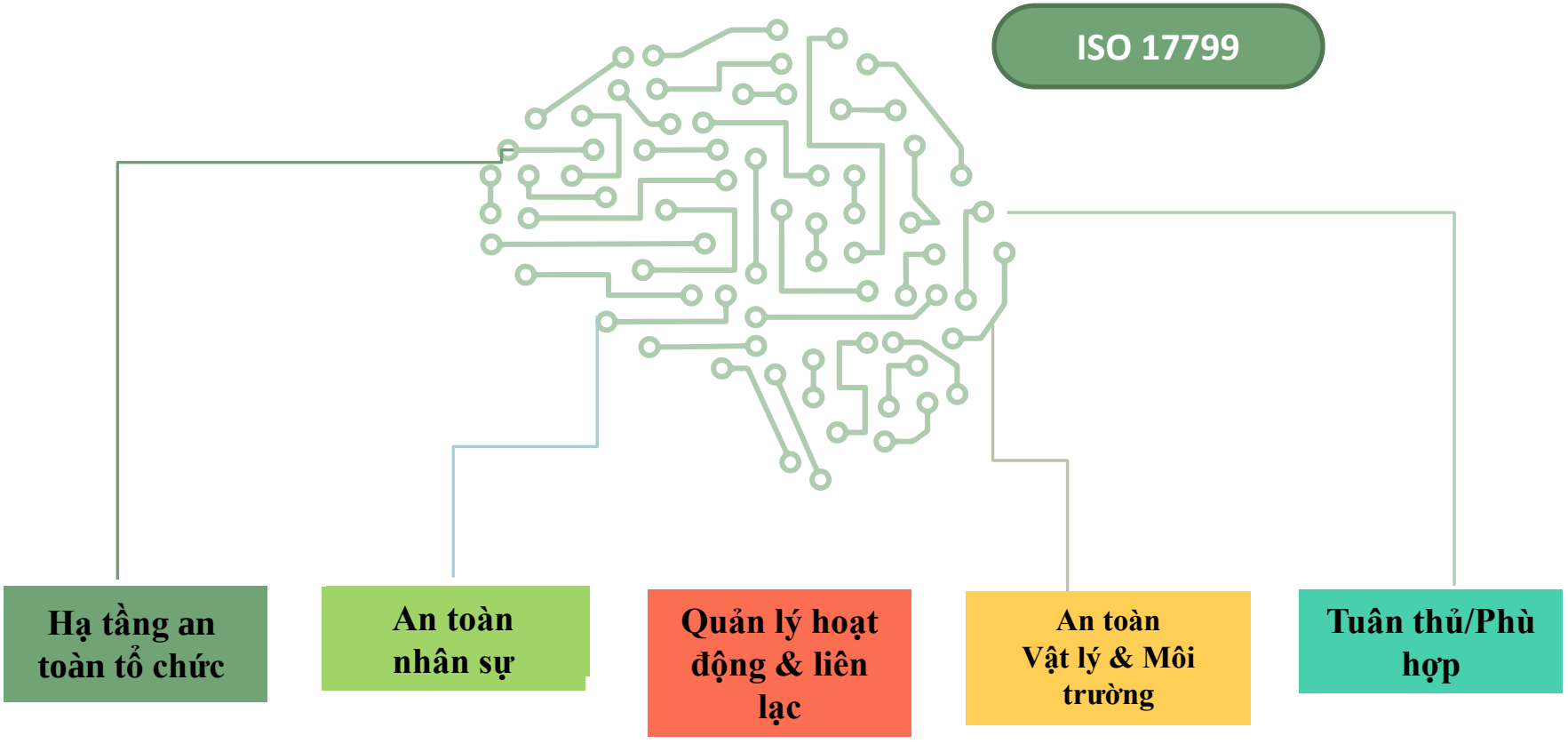
ISO/IEC

ISO 17799

Mô hình này này được dùng làm chuẩn quốc tế bởi ISO và IEC dưới tên ISO/IEC 17799 vào năm 2000 như là khung cho an toàn thông tin

MÔ HÌNH QUẢN LÝ ATTT

ISO/IEC



The ISO 27000 Series

- Information Technology – Code of Practice for Information Security Management
  - Một trong những mô hình quản lý an toàn thông tin được tham khảo rộng rãi
  - Được xuất bản với tên gọi British Standard và sau đó là ISO/IEC 17799
  - Vào năm 2007, nó được đổi tên thành ISO 27002.

- Thiết lập các hướng dẫn để bắt đầu, thực hiện, duy trì và cải tiến quản lý an ninh thông tin.
- Khi tiêu chuẩn lần đầu tiên ra mắt, một số quốc gia (bao gồm Hoa Kỳ, Đức và Nhật Bản) đã từ chối áp dụng nó.

The ISO 27000 Series

- “ISO / IEC 27001: 2005: Hệ thống quản lý an toàn thông tin” cung cấp chi tiết triển khai chu trình Kế hoạch - Thực hiện - Kiểm tra - Hành động (Plan - Do - Check - Act)

ISO / IEC 27001: 2005

- Plan
  - Xác định phạm vi của ISMS
  - Xác định chính sách ISMS
  - Xác định cách tiếp cận để đánh giá rủi ro
  - Xác định rủi ro
  - Đánh giá rủi ro
  - Xác định và đánh giá các lựa chọn để giải quyết rủi ro

ISO / IEC 27001: 2005

- Do
  - Lập kế hoạch xử lý rủi ro
  - Thực hiện kế hoạch xử lý rủi ro
  - Triển khai các biện pháp kiểm soát
  - Thực hiện các chương trình đào tạo và nâng cao nhận thức
  - Quản lý hoạt động, tài nguyên
  - Xác định và đánh giá các lựa chọn để giải quyết rủi ro
  - Thực hiện các thủ tục để phát hiện và ứng phó với sự cố an ninh

ISO / IEC 27001: 2005

- Check
  - Thực hiện các thủ tục giám sát
  - Thực hiện đánh giá thường xuyên về hiệu quả của ISMS
  - Tiến hành đánh giá ISMS nội bộ
  - Thực hiện đánh giá quản lý thường xuyên của ISMS
  - Ghi lại các hành động và sự kiện ảnh hưởng đến ISMS

ISO / IEC 27001: 2005

- Act
  - Thực hiện các cải tiến đã xác định
  - Thực hiện hành động khắc phục hoặc phòng ngừa
  - Áp dụng bài học kinh nghiệm
  - Đảm bảo các cải tiến đạt được các mục tiêu

Mô hình quản lí ATTT
Đánh giá tuân thủ ISO 27002 bởi SANS

Chính sách bảo mật

Tổ chức An ninh Thông tin

Quản lý tài sản

Nhân sự An ninh

An ninh Vật lý và Môi trường

Quản lý Truyền thông và Hoạt động

Kiểm soát truy cập

Mua lại, Phát triển và Bảo trì Hệ thống Thông tin

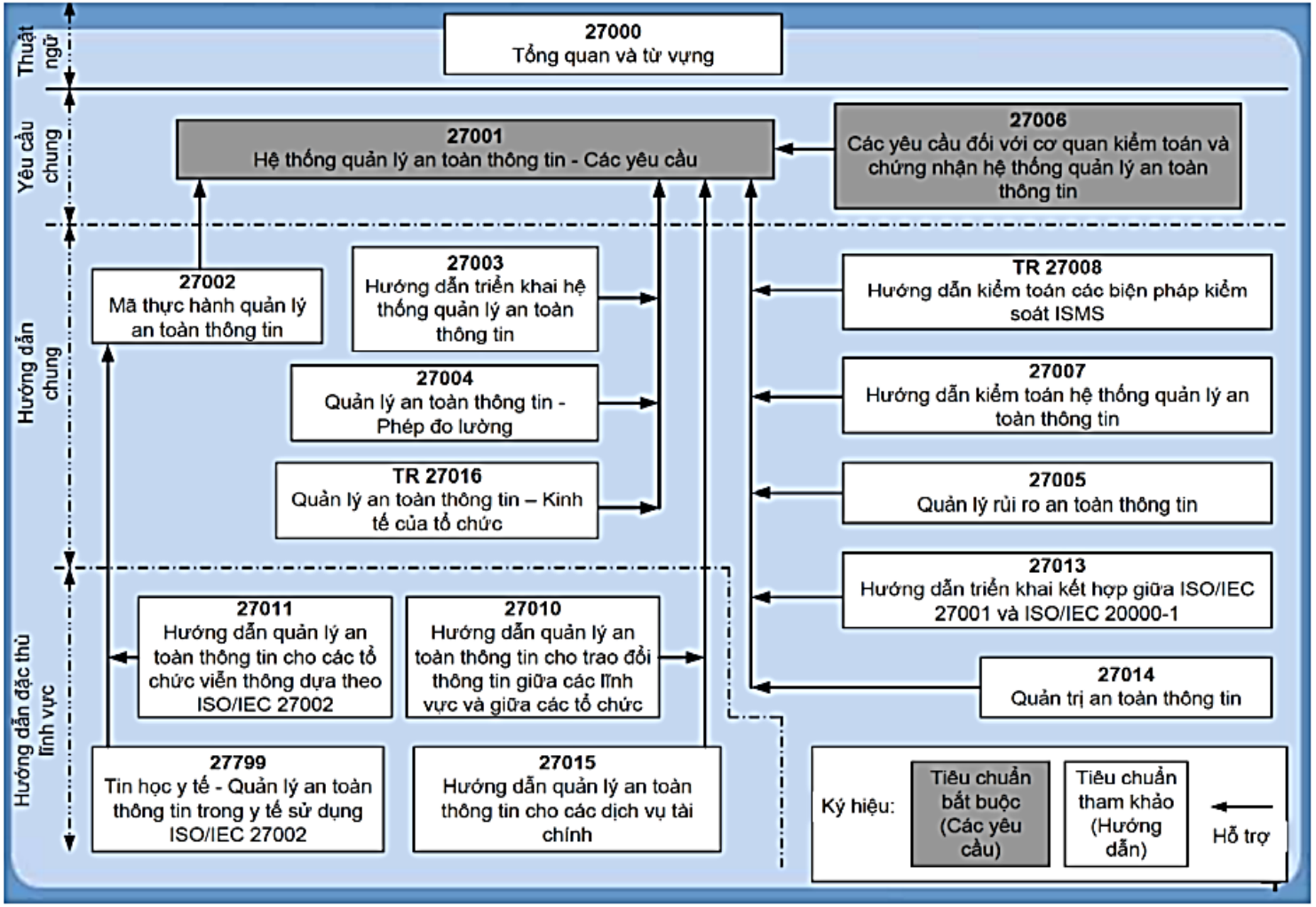
Quản lý sự cố an toàn thông tin

Quản lý kinh doanh liên tục

Tuân thủ

MÔ HÌNH QUẢN LÝ ATTT

ISO/IEC



Hình 3-1. Bộ tiêu chuẩn ISO 27000

NIST **Security Models**

- Cách tiếp cận khác về xây dựng và phát triển khung an toàn hiện có, được mô tả trong các văn bản có từ trung tâm tài nguyên an toàn máy tính (csrc.nist.gov) với bộ tài liệu NIST 800.
- Bộ tài liệu NIST 800 là một tập hợp các tài liệu mô tả chính sách, thủ tục và hướng dẫn bảo mật máy tính của chính phủ liên bang Hoa Kỳ-NIST (Viện Tiêu chuẩn và Công nghệ Quốc gia).

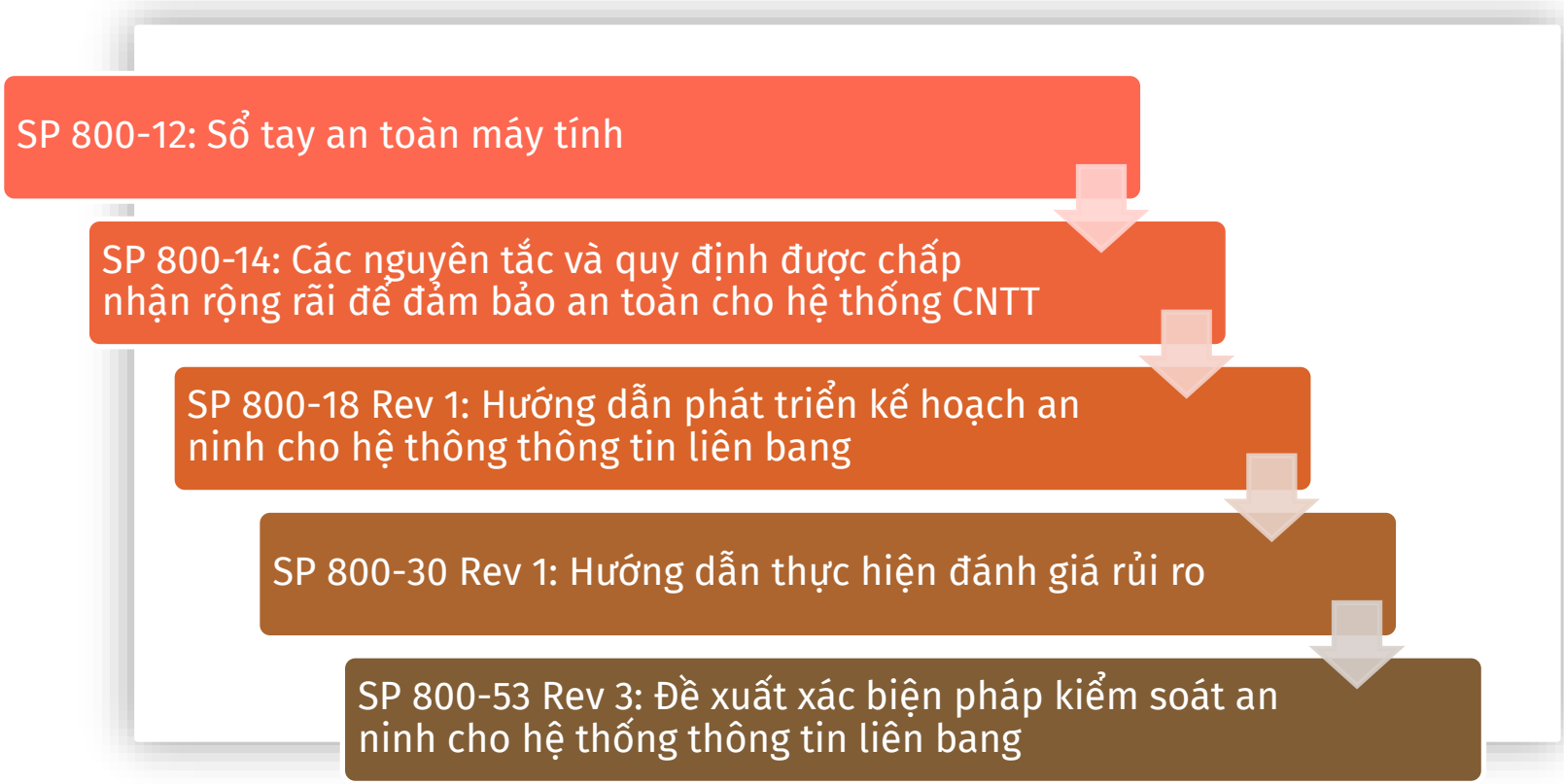
Tiêu chuẩn về bảo mật và ATTT của NIST

- Ưu điểm nổi bật:
  - Công khai, miễn phí.
  - Đã tồn tại trong một khoảng thời gian.
  - Đã được sử dụng rộng rãi và được đánh giá bởi các chính phủ và chuyên gia.

- Có 3 loại: SP, FIPS, NISTIR

- Ví dụ: SP 800-12, SP 800-14, SP 800-18, SP 800-30

Một số tài liệu NIST tiêu biểu



MÔ HÌNH QUẢN LÝ ATTT

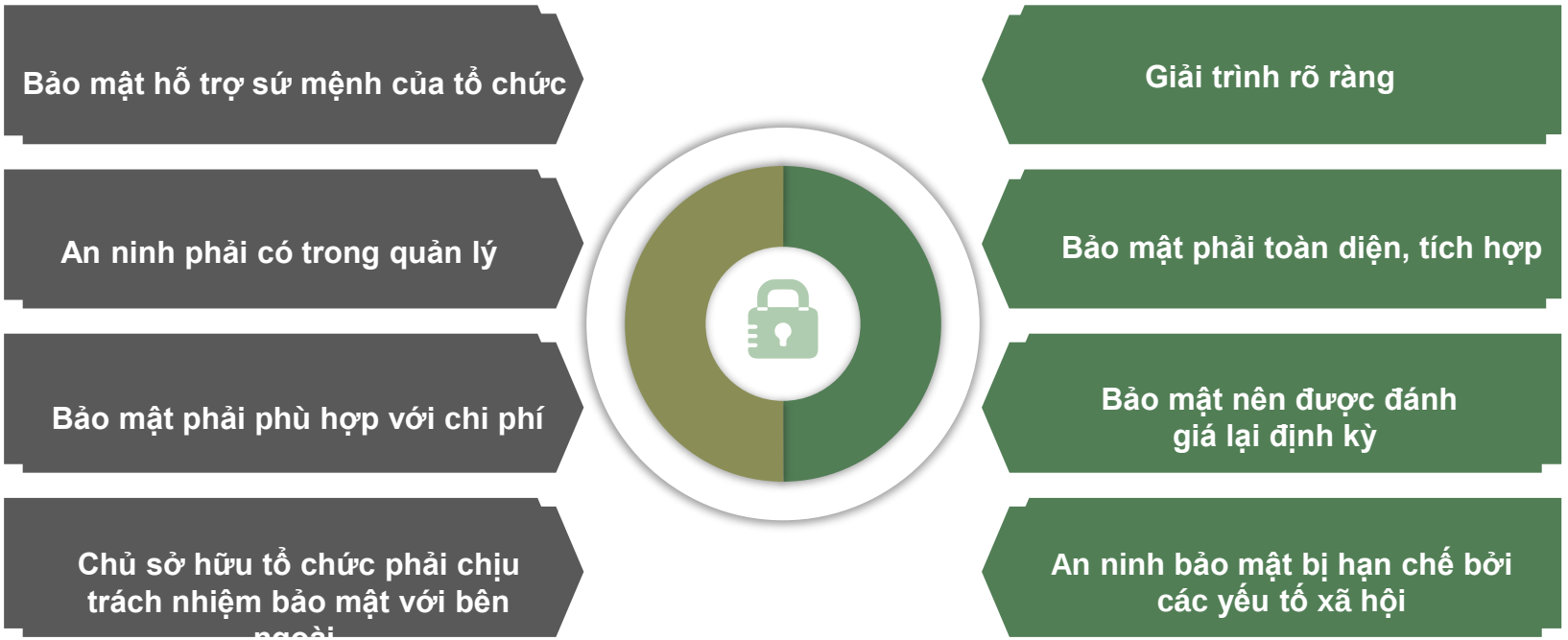
NIST Special Publication 800-12: Sổ tay bảo mật máy tính

SP 800-12 dựa trên Nguyên tắc của OECD về Bảo mật Hệ thống Thông tin, đã được Hoa Kỳ tán thành. Nó cung cấp:

- Trách nhiệm giải trình
- Nhận thức
- Đạo đức
- Tương xứng
- Tích hợp
- Kịp thời
- Đánh giá lại
- Hợp pháp

MÔ HÌNH QUẢN LÝ ATTT

NIST Special Publication 800-14: Các nguyên tắc và thực tiễn thường được chấp nhận cho bảo mật hệ thống thông tin



Kiểm soát thông tin và công nghệ liên quan (COBIT)

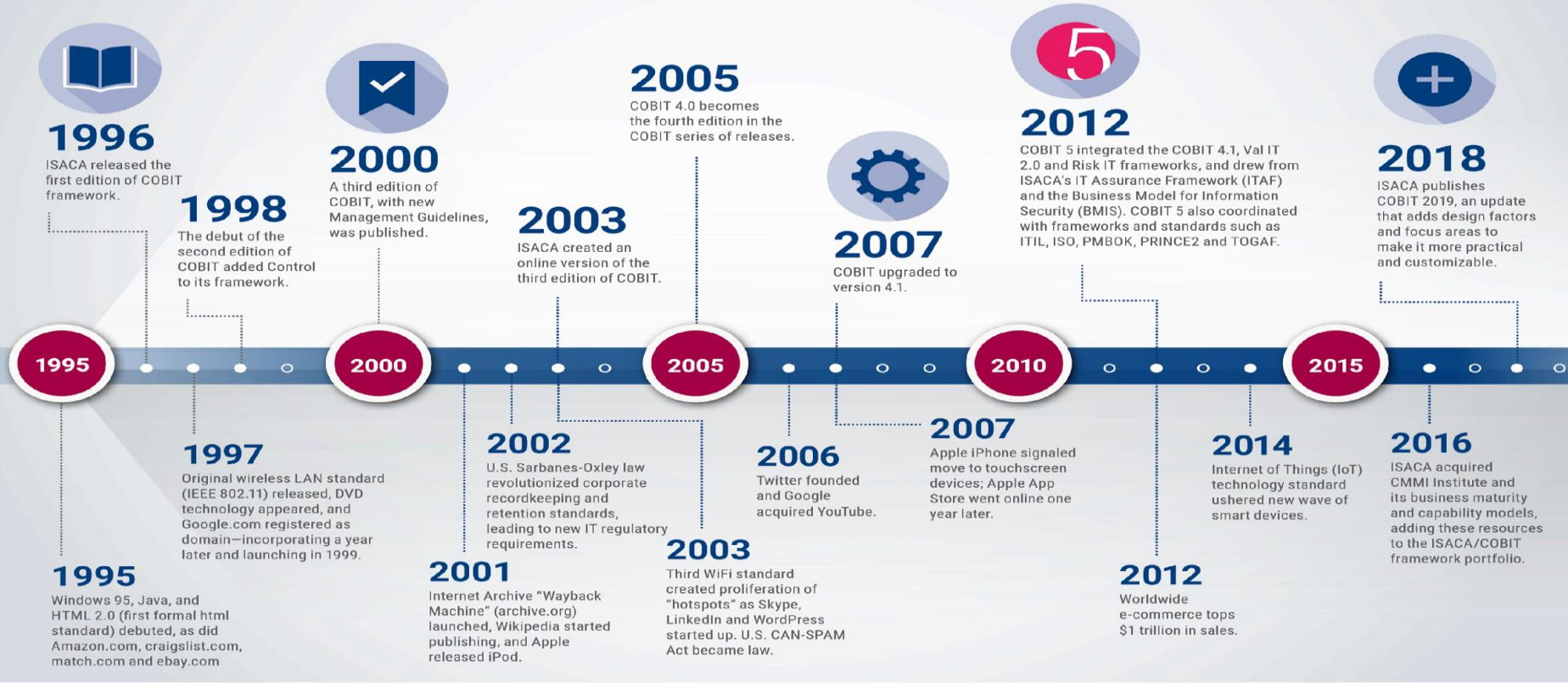
- Control Objectives for Information and Related Technology (COBIT)
  - Cung cấp lời khuyên về thực thi kiểm soát và mục tiêu kiểm soát cho an toàn thông tin.
  - Được tạo ra bởi Hiệp hội kiểm soát và đánh giá hệ thống thông tin (ISACA) và Viện quản trị CNTT (ITGI) vào năm 1992.
- COBIT 5 cung cấp 5 nguyên tắc tập trung vào quản trị và quản lý CNTT trong một tổ chức:

1. Nhu cầu của các bên liên quan.
2. Bao quát Doanh nghiệp.
3. Áp dụng một khung tích hợp, duy nhất.
4. Kích hoạt phương pháp tiếp cận toàn diện.
5. Tách quản trị khỏi quản lý

A HISTORICAL TIMELINE

The COBIT® Framework

COBIT 2019

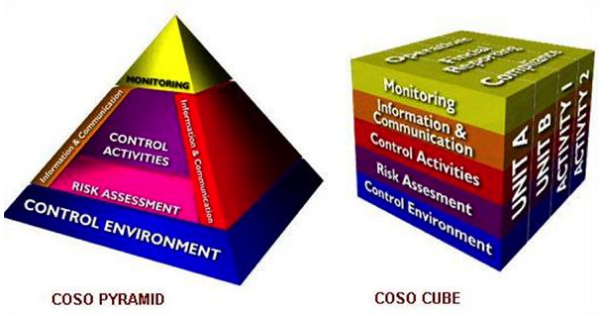


For more information, visit www.isaca.org/cobit

50 ISACA

COSO

- Một sáng kiến của khu vực tư nhân Hoa Kỳ.
- Mục tiêu chính là xác định các yếu tố gây ra gian lận trong báo cáo tài chính và đưa ra các biện pháp khuyến nghị để giảm thiểu tỉ lệ.
  Thiết lập một định nghĩa chung về kiểm soát nội bộ, tiêu chuẩn và tiêu chí mà các công ty và tổ chức có thể đánh giá hệ thống kiểm soát của họ.
- Giúp các tổ chức tuân thủ các quy định quan trọng như Sarbanes-Oxley.



COSO PYRAMID COSO CUBE

COSO

COSO PYRAMID

COSO CUBE

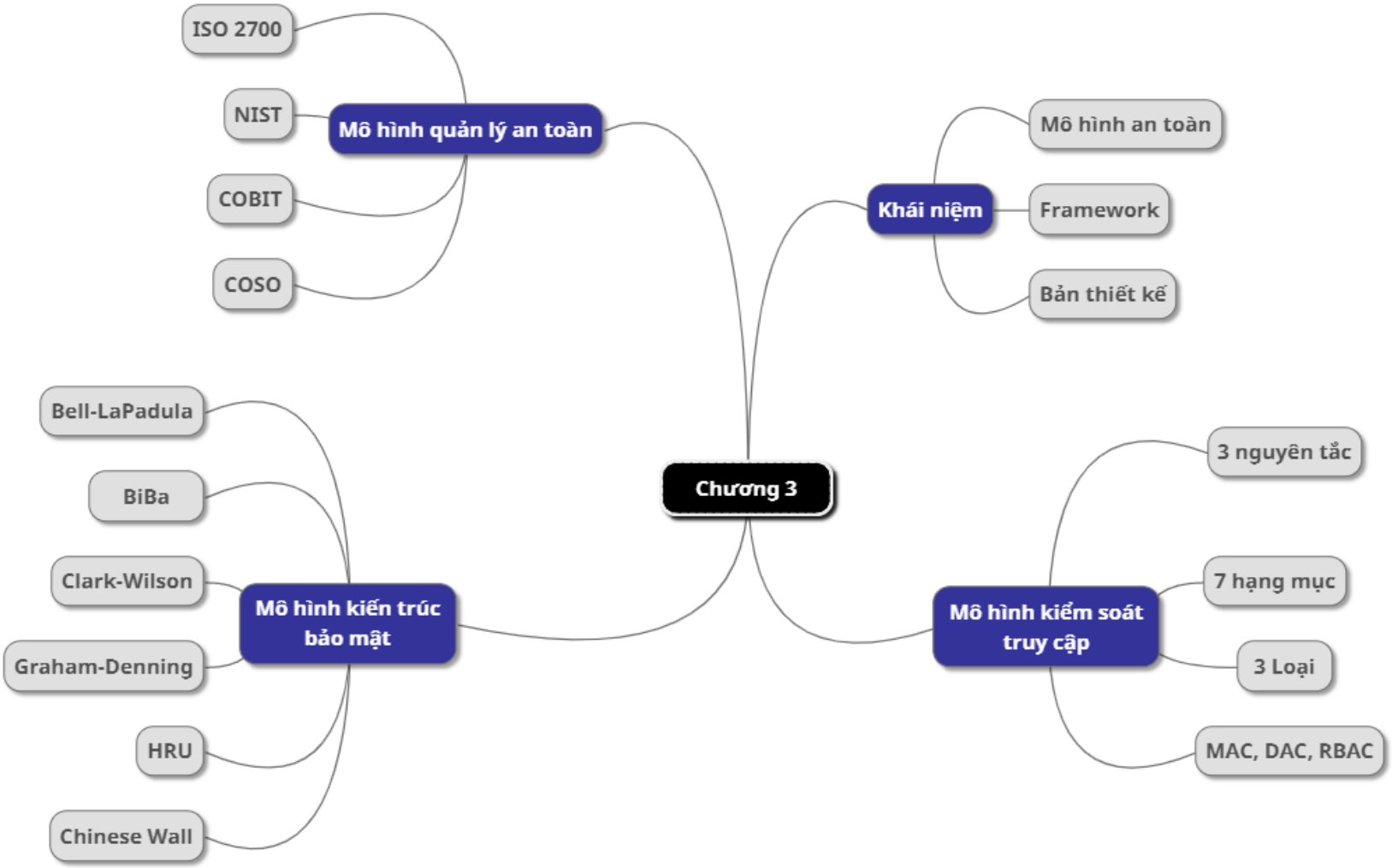
COSO Framework

- Xây dựng dựa trên năm thành phần có liên quan với nhau:
  - Kiểm soát môi trường
  - Đánh giá rủi ro
  - Kiểm soát hành vi
  - Thông tin và liên lạc
  - Giám sát

ITIL

- Là một tập hợp các phương pháp và thực hành quản lý sự phát triển và vận hành của cơ sở hạ tầng CNTT.
- Vì ITIL bao gồm mô tả chi tiết về nhiều hoạt động quan trọng liên quan đến CNTT, nên nó có thể được điều chỉnh cho phù hợp với nhiều tổ chức CNTT.

Tóm tắt


Chương 3
Khái niệm
Mô hình an toàn
Framework
Bản thiết kế
Mô hình quản lý an toàn
ISO 2700
NIST
COBIT
COSO
Mô hình kiến trúc bảo mật
Bell-LaPadula
BiBa
Clark-Wilson
Graham-Denning
HRU
Chinese Wall
Mô hình kiểm soát truy cập
3 nguyên tắc
7 hạng mục
3 Loại
MAC, DAC, RBAC