HỆ THỐNG QUẢN LÝ AN NINH THÔNG TIN

ISO/IEC 27001:2022

ISMS

By Royal Charter

Nội dung

- An ninh thông tin là gì ?
- Bộ tiêu chuẩn ISO 27000
- Nội dung ISO 27001:2022

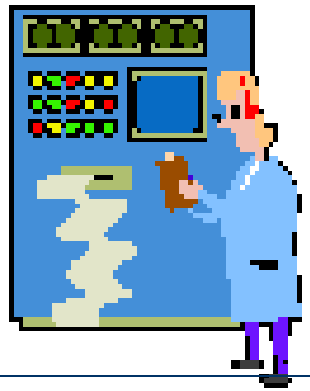
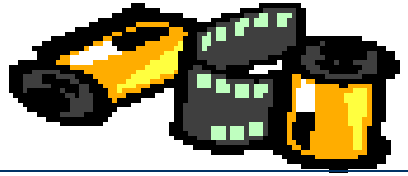
Thông tin là gì?

- **Định nghĩa theo ISO/IEC 27000:2022**
  - Thông tin là tài sản
  - Giống như bất kỳ tài sản kinh doanh khác
  - Nó có giá trị đối với tổ chức do đó phải được bảo vệ
- **Thông tin có thể ở nhiều dạng:**
  - dữ liệu được lưu trữ dưới dạng điện tử
  - dữ liệu đã được in ấn
  - kiến thức
  - trình chiếu
  - nói
  - dữ liệu mềm và dữ liệu cứng
- **Dù thông tin ở dạng nào, hay lưu giữ và chia xẻ bằng phương tiện gì thì nó luôn luôn cần được bảo vệ thích đáng.**

Information Nature





An ninh thông tin là gì?

Confidentiality

Đảm bảo chỉ những người được ủy quyền mới truy cập được thông tin

Availability

Đảm bảo những người được ủy quyền truy cập được thông tin và tài sản kèm theo khi có yêu cầu

Integrity

Đảm bảo độ chính xác và đầy đủ của thông tin và phương pháp xử lý

Có thể bao gồm thêm: authenticity, accountability, non-repudiation, và reliability (2.62)

bsi.

Quản lý

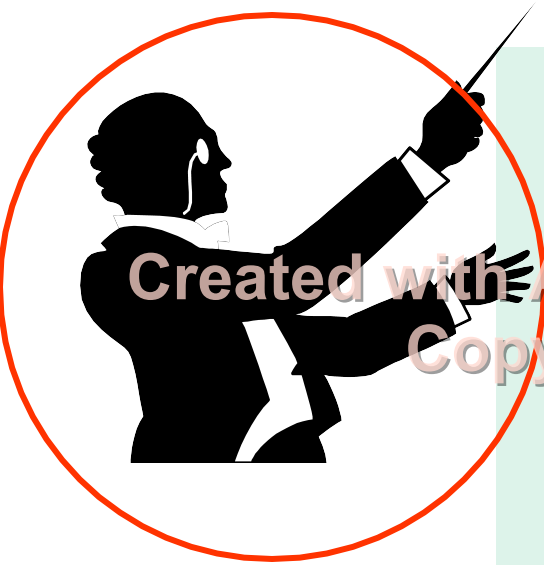
Các hoạt động có phối hợp để định hướng và kiểm soát một tổ chức

Hệ thống quản lý

Tập hợp các yếu tố có liên quan hoặc tương tác của tổ chức để thiết lập chính sách mục tiêu và các quá trình để đạt được các mục tiêu đó.

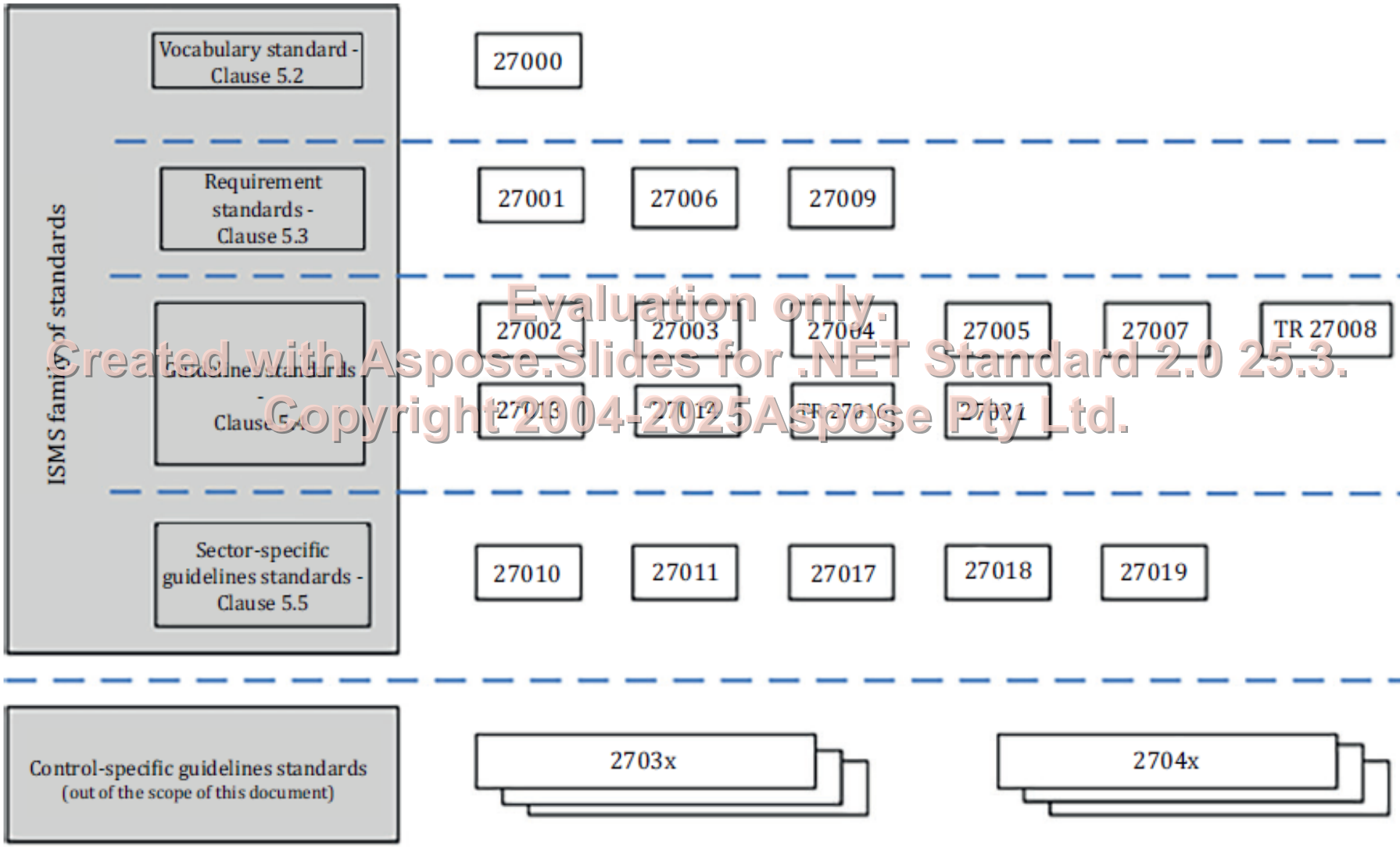
bsi.

HỆ THỐNG QUẢN LÝ AN TOÀN THÔNG TIN



Tập hợp các yếu tố có liên quan và tương tác thiết lập chính sách, mục tiêu về an ninh thông tin của một tổ chức và các quá trình để đạt được các mục tiêu đó

The ISO/IEC 27000 series



Giới thiệu

ISO/IEC 27001:2022

Information technology — Security techniques — Information security management systems — Requirements

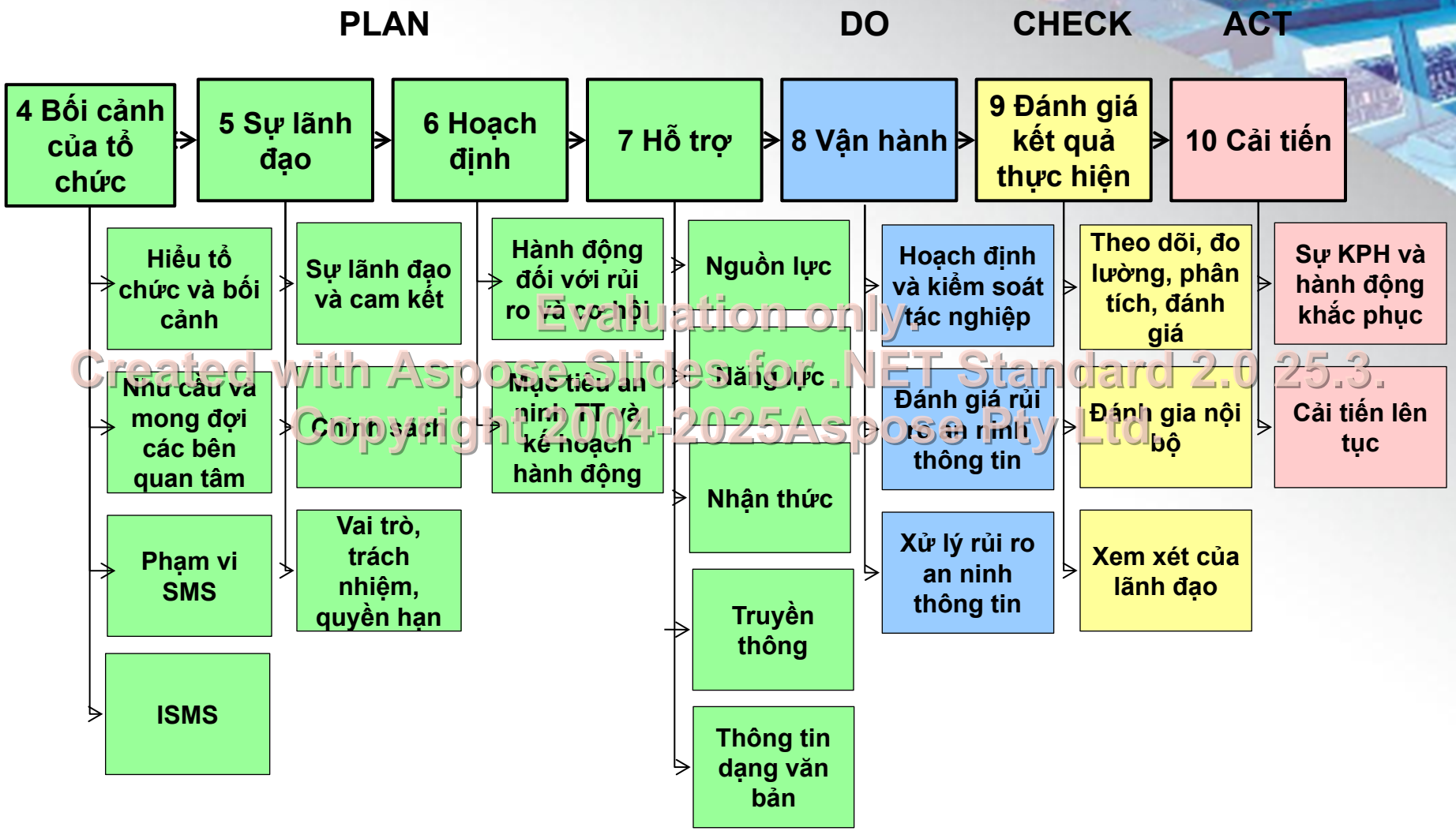
Mục đích

- Cụ thể các yêu cầu về thiết lập, thực hiện, vận hành, theo dõi, xem xét, duy trì và cải tiến ISMS trong điều kiện rủi ro kinh doanh của tổ chức .
- Hệ thống ISMS được thiết kế để đảm bảo chọn được các biện pháp kiểm soát an ninh thích hợp và cân đối để bảo vệ tài sản thông tin và tạo lòng tin cho các bên liên quan.

Phạm vi áp dụng

- **Mọi tổ chức, bất kể loại hình, quy mô hay tính chất kinh doanh**
- **Ngoại lệ :**
  - Không ảnh hưởng đến năng lực của tổ chức và/hoặc trách nhiệm cung cấp an ninh thông tin
  - Chứng minh được và cần bằng chứng rằng rủi ro kèm theo được chấp nhận bởi những người liên quan .
  - Không có ngoại lệ trong điều khoản 4, 5, 6, 7, 8, 9,10.

Cấu trúc ISO/IEC 27001:2013



4. Bối cảnh của tổ chức

4.1 Hiểu về tổ chức và bối cảnh

Xác định các vấn đề có liên quan đến việc thiết lập bối cảnh bên ngoài và nội bộ của tổ chức

4.2 Hiểu nhu cầu và mong đợi của các bên quan tâm

xác định:

a) các bên quan tâm có liên quan đến hệ thống quản lý an ninh thông tin; và

b) các yêu cầu của các bên quan tâm có liên quan đến an ninh thông tin

c) yêu cầu nào trong số này sẽ được giải quyết thông qua hệ thống quản lí ATTT

4. Bối cảnh của tổ chức

4.3 Xác định phạm vi của hệ thống quản lý an ninh thông tin

Xác định ranh giới và khả năng áp dụng của hệ thống quản lý an ninh thông tin để thiết lập phạm vi hệ thống

Xem xét:

a) các vấn đề bên ngoài và nội bộ nêu trong 4.1;

b) các yêu cầu nêu trong 4.2;

c) Sự tương tác và phụ thuộc giữa các hoạt động được thực hiện bởi tổ chức, và những hoạt động được thực hiện bởi các tổ chức khác

Phạm vi dưới dạng thông tin dạng văn bản

4. Bối cảnh của tổ chức

4.4 Hệ thống quản lý an ninh thông tin

Thiết lập, thực hiện, duy trì và cải tiến liên tục hệ thống quản lý an ninh thông tin phù hợp với các yêu cầu của tiêu chuẩn:

Các bước:

- xác định tài sản thông tin và các yêu cầu bảo mật thông tin liên quan;
- đánh giá và xử lý rủi ro bảo mật thông tin;
- lựa chọn và thực hiện các kiểm soát có liên quan để quản lý các rủi ro không thể chấp nhận;
- giám sát, duy trì và nâng cao hiệu quả của các kiểm soát liên quan đến tài sản thông tin.

5. Sự lãnh đạo/Leadership

5.1 Sự Lãnh đạo và cam kết

- Sự lãnh đạo và cam kết đối với ISMS
- Chính sách an ninh thông tin và các mục tiêu
- Hội nhập của các yêu cầu ISMS vào các quá trình
- Nguồn lực cần thiết
- Truyền thông tầm quan trọng của quản lý an ninh thông tin
- Hệ thống quản lý an ninh thông tin đạt được kết quả dự định
- Mọi người đóng góp vào hiệu lực của ISMS
- Cải tiến liên tục
- Vai trò quản lý khác có liên quan

5. Sự lãnh đạo/Leadership

5.2 Chính sách

Thiết lập chính sách an ninh thông tin phù hợp với mục đích tổ chức; bao gồm các mục tiêu ATTT hoặc cung cấp khuôn khổ cho việc thiết lập các chỉ tiêu ATTT

5.3 **Vai trò tổ chức, trách nhiệm và quyền hạn**

- trách nhiệm và quyền hạn đối với vai trò liên quan đến an ninh thông tin được phân công và truyền đạt.
- phân công trách nhiệm và thẩm quyền về HTQLANTT

6. Hoạch định/Planning

6.1 Các hành động đối với các rủi ro và cơ hội

6.1.1 Khái quát

- Hoạch định HTQLANTT
  - Xem xét các vấn đề được đề cập 4.1 và 4.2
  - Xác định rủi ro và cơ hội cần giải quyết
- Hoạch định:
  - Hành động để giải quyết các rủi ro và cơ hội;
  - Cách thức
    - tích hợp và thực hiện các hành động vào các quá trình của hệ thống quản lý an ninh thông tin
    - đánh giá hiệu lực các hành động

6. Hoạch định/Planning

6.1 **Các hành động đối với các rủi ro và cơ hội**

6.1.2 **Đánh giá rủi ro an ninh thông tin**:

Quá trình đánh giá rủi ro an ninh thông tin:

a/ chuẩn mực để thực hiện đánh giá rủi ro

- chuẩn mực để chấp nhận rủi ro
- chuẩn mực để thực hiện đánh giá rủi ro

b/ cung cấp các kết quả ổn định, đúng đắn và tương đương và có thể so sánh được

c/ xác định các rủi ro an ninh thông tin

- xác định các rủi ro liên quan với sự mất bí mật, tính toàn vẹn và tính sẵn sang
- xác định chủ sở hữu của rủi ro

6. Hoạch định/Planning

6.1 Các hành động đối với các rủi ro và cơ hội

6.1.2 Đánh giá rủi ro an ninh thông tin:

Quá trình đánh giá rủi ro an ninh thông tin:

d) phân tích các rủi ro an ninh thông tin

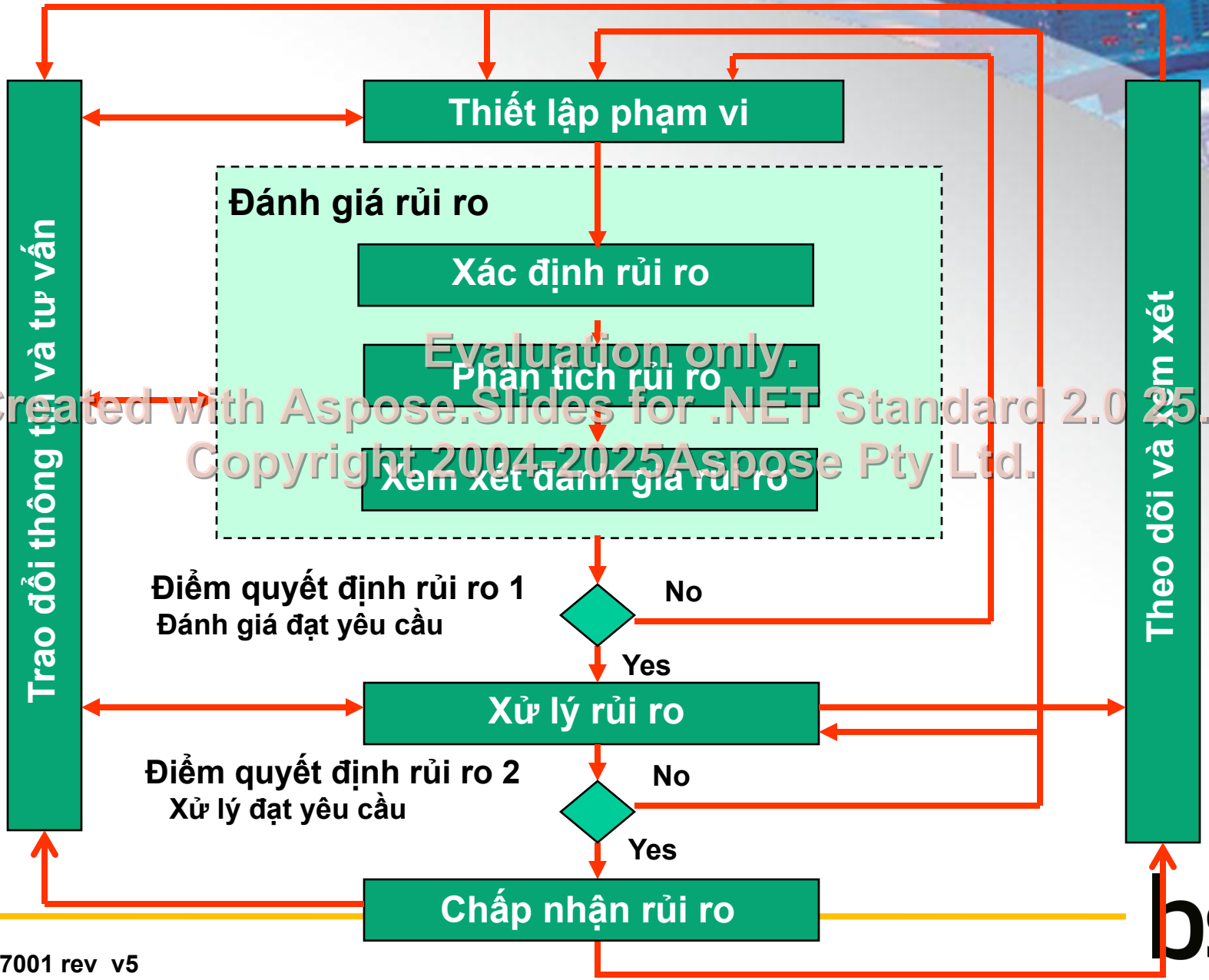
- đánh giá các hậu quả tiềm ẩn
- đánh giá khả năng xuất hiện của rủi ro
- xác định mức độ rủi ro;

e) đánh giá các rủi ro an ninh thông tin

- so sánh kết quả của phân tích rủi ro với các chuẩn mực rủi ro
- Ưu tiên các rủi ro được phân tích để xử lý

lưu thông tin dạng văn bản về quá trình đánh giá rủi ro

Quá trình Quản lý rủi ro an ninh thông tin



6. Hoạch định/Planning

6.1 Các hành động đối với các rủi ro và cơ hội

6.1.3 Xử lý rủi ro an ninh Thông tin

- chọn các cách xử lý ATTT phù hợp, có tính đến kết quả đánh giá rủi ro
- xác định tất cả các biện pháp kiểm soát cần thực hiện
- So sánh các biện pháp thực hiện trong 6.1.3b ở trên với Phụ lục A
- Statement of Applicability
- Xây dựng kế hoạch xử lý rủi ro
- phê duyệt kế hoạch xử lý rủi ro và chấp nhận các rủi ro dư

lưu giữ thông tin dạng văn bản về quá trình xử lý rủi ro

Tham khảo ISO 31000

bsi.

6. Hoạch định/Planning

6.2 Mục tiêu an ninh Thông tin

- nhất quán với chính sách an ninh thông tin;
- có thể đo lường được
- xét đến các yêu cầu an ninh thông tin, và kết quả đánh giá và xử lý rủi ro;
- được theo dõi
- được truyền đạt; và
- được cập nhật phù hợp

Thông tin dạng văn bản về các mục tiêu

6. Hoạch định/Planning

6.2 Mục tiêu an ninh Thông tin

Lập kế hoạch để đạt mục tiêu, tổ chức phải xác định:

- những gì sẽ được thực hiện;
- nguồn lực sẽ được yêu cầu;
- người chịu trách nhiệm;
- Thời điểm sẽ được hoàn thành; và
- kết quả sẽ được đánh giá như thế nào

7. Hỗ trợ/Support

7.1 Nguồn lực

- xác định và cung cấp các nguồn lực cần thiết cho việc thiết lập,thực hiện, duy trì và cải tiến liên tục của hệ thống quản lý an ninh thông tin

7.2 Năng lực

- xác định các năng lực cần thiết
- đảm bảo rang những người này có đủ năng lực căn cứ trên cơ sở được giáo dục, đào tạo hoặc có kinh nghiệm thích hợp
- hành động để có năng lực cần thiết, đánh giá hiệu lực hành động
- thông tin dạng văn bản về năng lực

7. Hỗ trợ/Support

7.3 Nhận thức

Có nhận thức về

- các chính sách an ninh thông tin;
- đóng góp vào hiệu lực của hệ thống quản lý an ninh thông tin, bao gồm cả lợi ích của kết quả thực hiện an ninh thông tin được cải thiện; và
- hệ lụy của việc không phù hợp với các yêu cầu hệ thống quản lý an ninh thông tin.

7. Hỗ trợ/Support

7.4 Trao đổi thông tin

xác định nhu cầu thông tin liên lạc nội bộ và bên ngoài liên quan đến hệ thống quản lí ATTT

a) Trao đổi thông tin gì;

b) Trao đổi thông tin khi nào;

c) Trao đổi thông tin với ai;

d) Làm thế nào để trao đổi thông tin

7. Hỗ trợ/Support

7.5 Thông tin dạng văn bản

7.5.1 Các loại thông tin:

- thông tin dạng văn bản theo yêu cầu của tiêu chuẩn
- thông tin dạng văn bản tổ chức xác định là cần thiết để hệ thống quản lý an ninh thông tin có hiệu lực

7.5.2 Tạo lập và cập nhật

Tổ chức phải đảm bảo

- nhận dạng và mô tả (tiêu đề, ngày, tác giả, số tham chiếu);
- định dạng (ngôn ngữ, phiên bản phần mềm, đồ họa) và phương tiện truyền thông (ví dụ như giấy, điện tử); và
- xem xét và phê duyệt về phù hợp và đầy đủ.

7. Hỗ trợ/Support

7.5.3 Kiểm soát thông tin dạng văn bản

- đảm bảo
  - có sẵn và phù hợp cho việc sử dụng, ở đâu, khi nào cần thiết;
  - bảo vệ đầy đủ (mất tính bảo mật, sử dụng không đúng cách, mất tính toàn vẹn).
- phân phối, truy cập, thu hồi và sử dụng;
- lưu trữ và bảo quản, bao gồm cả việc duy trì tính rõ ràng;
- kiểm soát các thay đổi (ví dụ như kiểm soát phiên bản); và
- lưu giữ và hủy bỏ.
- Xác định thích hợp, và kiểm soát Thông tin dạng văn bản có nguồn gốc bên ngoài cần thiết cho việc lập kế hoạch và hoạt động của hệ thống quản lý an ninh thông tin.

8. Vận hành/Operation

8.1 Lập kế hoạch và kiểm soát vận hành

- lập kế hoạch, thực hiện và kiểm soát các quá trình cần thiết đáp ứng 6.1, 6.2.
- lưu thông tin dạng văn bản
- kiểm soát thay đổi
- xác định và kiểm soát các quá trình thuê ngoài được

8.2 Đánh giá rủi ro an ninh Thông tin

- đánh giá rủi ro an ninh thông tin theo kế hoạch hoặc khi có thay đổi quan trọng
- thông tin dạng văn bản các kết quả đánh giá

8. Vận hành/Operation

8.3 Xử lý rủi ro an ninh thông tin

- kế hoạch xử lý rủi ro an ninh thông tin.
- thông tin dạng văn bản các kết quả xử lý rủi ro

9. Đánh giá kết quả thực hiện Performance evaluation

9.1 Giám sát, đo lường, phân tích và đánh giá

- những gì cần phải được giám sát và đo lường, bao gồm cả quá trình và biện pháp kiểm soát an ninh thông tin;
- phương pháp kiểm soát giám sát, đo lường, phân tích và đánh giá có thể áp dụng nhằm đảm bảo kết quả có thể lặp lại được và có thể so sánh được
- Thời điểm giám sát và đo lường
- Thời điểm kết quả từ giám sát và đo lường phải được phân tích và đánh giá
- người sẽ phân tích và đánh giá các kết quả này

Thông tin dạng văn bản

9. Đánh giá kết quả thực hiện
Performance evaluation

9.2 Đánh giá nội bộ

Đánh giá nội bộ theo kế hoạch

Mục đích: ISMS có:

a) phù hợp với

- yêu cầu riêng của tổ chức đối với hệ thống quản lý an ninh thông tin; và
- các yêu cầu của tiêu chuẩn này;

b) được thực hiện và duy trì có hiệu lực

9. Đánh giá kết quả thực hiện Performance evaluation

9.2 Đánh giá nội bộ

- lập kế hoạch, thiết lập, thực hiện và duy trì một chương trình đánh giá
- xác định các chuẩn mực đánh giá và phạm vi
- tính khách quan của auditor và tính khách quan của quá trình đánh giá
- kết quả của cuộc đánh giá được báo cáo tới cấp quản lý

Thông tin dạng văn bản

9. Đánh giá kết quả thực hiện Performance evaluation

9.3 Xem xét của lãnh đạo

- Xem xét hệ thống quản lý an ninh thông tin định kỳ có kế hoạch
- Đầu vào
  - tình trạng của các hành động từ xem xét của lãnh đạo trước đó;
  - thay đổi trong các vấn đề bên ngoài và nội bộ có liên quan
  - Những thay đổi về nhu cầu và mong đợi của các bên quan tâm có liên quan đến hệ thống quản lí ATTT
  - phản hồi về việc thực hiện an ninh thông tin,
  - ý kiến phản hồi từ các bên quan tâm;
  - Kết quả đánh giá rủi ro và tình trạng của kế hoạch xử lý rủi ro; và
  - cơ hội cải tiến liên tục
- Đầu ra
- các quyết định liên quan đến cơ hội cải tiến liên tục và bất kỳ nhu cầu thay đổi đối với hệ thống quản lý an ninh thông tin

10. Cải tiến/Improvement

10.1 Sự không phù hợp và hành động khắc phục

- Ứng phó với sự không phù hợp, tổ chức cần phải

  - Thực hiện hành động kiểm soát và sửa đổi

  - Xử lý hệ quả

- Đánh giá sự cần thiết phải hành động để loại bỏ nguyên nhân của sự không phù hợp, nhằm không để tái diễn hoặc xảy ra ở nơi khác

  - Soát xét sự không phù hợp

  - Xác định nguyên nhân của sự không phù hợp

  - Xác định nếu có sự không phù hợp tương tự tồn tại, hoặc khả năng có thể xảy ra

10. Cải tiến/Improvement

- Thực hiện mọi hoạt động cần thiết
- Soát xét tính hiệu lực của mọi hành động khắc phục đang được thực hiện
- Thực hiện các thay đổi đối với hệ thống quản lí ATTT

Thông tin dạng văn bản làm bằng chứng

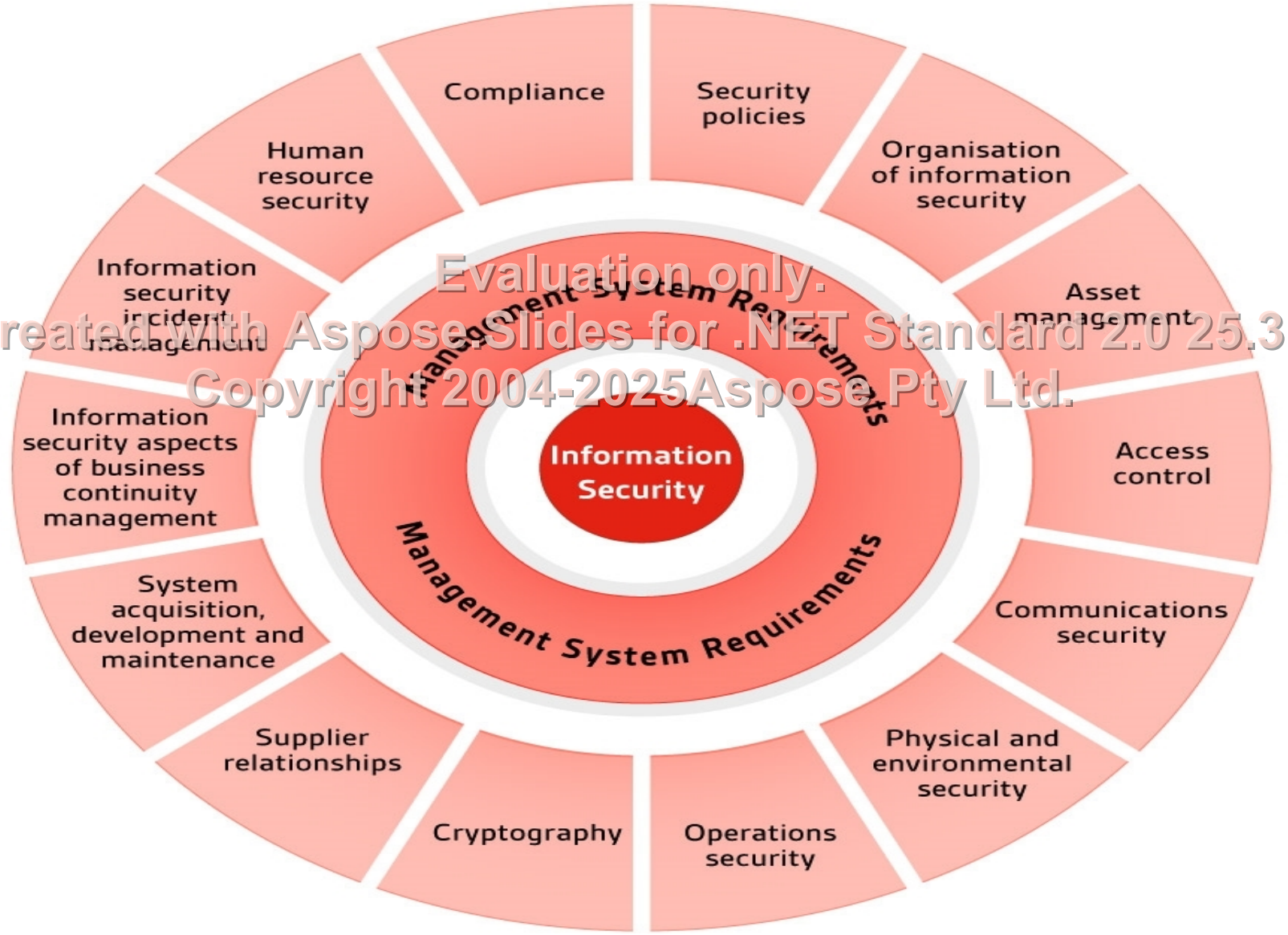
- Bản chất của sự không phù hợp và mọi hành động tiếp theo được thực hiện
- Các kết quả của bất kỳ hành động khắc phục nào.

Clauses, Categories, Controls

- 14 điều kiểm soát an ninh
- 35 chủng loại (categories) an ninh
- 114 kiểm soát

bsi.

Controls



14 lĩnh vực chủ yếu

1. **CHÍNH SÁCH AN NINH THÔNG TIN** – Cung cấp hướng dẫn và ý đồ quản lý để cải tiến an ninh thông tin.
2. **TỔ CHỨC AN NINH THÔNG TIN** – Tạo điều kiện kiểm soát an ninh thông tin trong tổ chức.
3. **QUẢN LÝ TÀI SẢN** – Thực hiện kiểm kê tài sản và bảo quản tài sản hiệu quả.
4. **KIỂM SOÁT TRUY CẬP** - Kiểm soát việc truy cập đến IS để đảm bảo tính bảo mật và sẵn có
5. **AN NINH TRUYỀN THÔNG**– Giảm thiểu rủi ro trong trao đổi thông tin
6. **AN NINH VẬT LÝ VÀ MÔI TRƯỜNG** – Phòng ngừa vi phạm, làm hỏng hoặc phá vỡ thiết bị công nghiệp và dữ liệu.
7. **AN NINH VẬN HÀNH**- Đảm bảo vận hành thích hợp và tin cậy các thiết bị sử lý thông tin.

14 Lĩnh vực chủ yếu

8. **MÃ HÓA**– Kiểm soát mã hóa thông tin đảm bảo bảo mật, toàn vẹn.
9. **QUAN HỆ VỚI NHÀ CUNG CẤP** – Đảm bảo an nnh thông tin giữa các bên đối tác
10. **THIẾT LẬP VÀ DUY TRÌ HỆ THỐNG THÔNG TIN** – Đảm bảo an ninh được kết hợp chặt chẽ vào hệ thống thông tin.
11. **QUẢN LÍ SỰ CỐ AN NINH THÔNG TIN** – Đảm bảocách tiếp cận nhất quán và hiệu quả đến việc kiểm soát sự cố an ninh thông tin.
12. **CÁC KHÍA CẠNH IS TRONG QUẢN LÝ TÍNH LIÊN TỤC KINH DOANH** – Giảm thiểu ảnh hưởng của sự gián đoạn kinh doanh và bảo vệ các quá trình quan trọng của tổ chức khỏi bị sai lỗi và thảm họa lớn.
13. **QUẢN LÝ NGUỒN NHÂN LỰC** – Đảm bảo an ninh nhân sự
14. **SỰ PHÙ HỢP** – Tránh vi phạm luật hình sự, dân sự, chế định hoặc hợp đồng và yêu cầu an ninh.

Q&A

- Any questions?