ĐỀ CƯƠNG ÔN TẬP MÔN QLATTT

# Phần 1: Lý thuyết

## Phân tích mối quan hệ giữa hiểm họa, điểm yếu và rủi ro.

* Hiểm họa là những nguyên nhân tiềm ẩn gây ra sự cố không mong muốn, kết quả có thể gây thiệt hại cho hệ thống, tổ chức
* Điểm yếu là những khiếm khuyết, nhược điểm của tài sản hay các biện pháp kiểm soát, có thể bị khai thác bởi một hay nhiều hiểm họa
* Rủi ro là những khả năng xấu có thể xảy ra đối với một hệ thống
* Mối quan hệ:
  + Nếu hiểm họa không xảy ra thì không có rủi ro
  + Nếu không có điểm yếu thì không có rủi ro
  + Rủi ro là kết quả của việc kết hợp hiểm họa và điểm yếu.
  + Rủi ro =f(tài sản, hiểm họa, điểm yếu)

## Việc xác định rủi ro có vai trò như thế nào trong Quản lý an toàn thông tin.

Việc xác định rủi ro có vai trò xác định được mức độ ảnh hưởng từ việc xác định mức độ tài sản thiệt hại qua đó xác định được mức độ ưu tiên. Vai trò:

* Giúp các tổ chức nhận biết, đánh giá các nguy cơ tiềm ẩn có thể gây ra tổn thất cho hệ thông thông tin của họ.
* Xác định các biện pháp an toàn phù hợp để hạn chế và loại bỏ các rủi ro.
* Giúp các tổ chức hiểu rõ hơn về môi trường hoạt động của mình
* Chuẩn bị kế hoạch ứng phó khi xảy ra sự cố ATTT

## Tầm quan trọng của Luật pháp trong quản lý ATTT.

* Răn đe, ngăn chặn các hành vi sai trái, xâm phạm quyền lợi chính đáng của các cá nhân, tổ chức khác.
* Làm cơ sở để xử phạt đối với những hành vi vi phạm.
* Đảm bảo tính hiệu quả trong quản lý
* Xây dựng hành lang pháp lý để bảo vệ quyền, lợi ích hợp pháp của cá nhân, tổ chức, xã hội và nhà nước trong lĩnh vực thông tin

## Lập kế hoạch là gì, vai trò của việc xây dựng KH cho chiến lược an toàn, nêu các thành phần cho kế hoạch chiến lược cấp tổ chức.

* Lập kế hoạch là quá trình xác định và chỉ rõ định hướng, mục tiêu dài hạn của một tổ chức và các bước cần thực hiện, việc phân bổ, thu thập nguồn lực cần thiết để theo đuổi và đạt được mục tiêu.
* Vai trò:
  + Là phương tiện chủ đạo để quản lý tài nguyên của tổ chức
  + Liệt kê 1 chuỗi các hành động để đạt được mục tiêu cụ thể trong 1 khoảng thời gian xác định, kiểm soát việc thực hiện các bước này
  + Cung cấp định hướng cho tương lai của tổ chức
* Thành phần:

1. Tóm tắt
2. Tuyên bố sứ mệnh, tầm nhìn, giá trị
3. Hồ sơ và lịch sử của tổ chức
4. Các vấn đề và thách thức chiến lược
5. Mục tiêu của tổ chức
6. Mục tiêu của đơn vị kinh doanh chính
7. Phụ lục (nếu có)

## Trình bày và so sánh 2 cách tiếp cận trong phân tích, triển khai ATTT.

* 2 cách tiếp cận là từ trên xuống và từ dưới lên

|  |  |
| --- | --- |
| **Từ trên xuống** | **Từ dưới lên** |
| - Bắt đầu từ quản lý cấp cao xuống  - Có sự hỗ trợ của quản lý cấp cao mạnh mẽ  - Chương trình được thiết kế để hỗ trợ toàn bộ tổ chức trong 1 nỗ lực toàn diện, tất cả các bên liên quan đều phải tham gia thực hiện an toàn và kết quả có rất ít lỗ hổng | - Bắt đầu như một nỗ lực cơ sở từ quản trị viên, kỹ thuật viên lên  -  - Hoạt động ngắn hạn vì thiếu |

## Khi lập kế hoạch an toàn, việc phân loại hệ thống dựa trên các tiêu chí nào; Khả năng tác động của từng tiêu chí được xem xét cụ thể như thế nào.

* Việc phân loại hệ thống dựa trên 3 tiêu chí: bí mật, toàn vẹn, sẵn sàng
* Khả năng tác động của từng tiêu chí:

|  |  |  |  |
| --- | --- | --- | --- |
|  | Thấp | Trung bình | Cao |
| Bí mật: các phương tiện bảo vệ quyền riêng tư cá nhân, thông tin độc quyền | có tác động bất lợi, hạn chế hoạt động của tổ chức, tài sản của tổ chức hoặc cá nhân | có thể ảnh hưởng xấu nghiêm trọng tới hoạt động của tổ chức, tài sản của tổ chức hoặc cá nhân | có thể gây ra tác động tiêu cực nghiêm trọng hoặc nghiêm trọng đối với hoạt động của tổ chức, tài sản của tổ chức hoặc cá nhân |
| Toàn vẹn: chống lại sự sửa đổi hay phá hủy thông tin không phù hợp: đảm bảo thông tin được xác thực và không bị từ chối | như trên | như trên | như trên |
| Sẵn sàng: đảm bảo việc truy cập và sử dụng thông tin kịp thời, đáng tin cậy | như trên | như trên | như trên |

## Mục tiêu chính của vòng đời phát triển hệ thống an toàn (SecSDLC) là gì; Trình bày giai đoạn thiết kế trong SecSDLC.

(Bổ sung) Thành công của kế hoạch ATTT có thể được nâng cao bằng cách sử dụng các quy trình phân tích và thiết kế hệ thống. Vòng đời phát triển hệ thống (SDLC) là một phương pháp luận để thiết kế và triển khai hệ thống thông tin trong một tổ chức. Quá trình phát triển hệ thống theo từng giai đoạn được mô tả bởi SDLC truyền thống có thể được điều chỉnh để hỗ trợ việc triển khai chuyên biệt của một dự án an toàn bằng cách sử dụng vòng đời phát triển hệ thống an toàn (SecSDLC)

Thành công được nâng cao sử dụng quy trình phân tích và vòng đời phát triển hệ thống an toàn (SDLC) nâng cao dự an là SecSDLC

* Mục tiêu của SecSDLC là hỗ trợ triển khai chuyên biệt một dự án an toàn
* Giai đoạn thiết kế trong SecSDLC có 2 giai đoạn chính là thiết kế logic và thiết kế vật lý.
  + Thiết kế logic: tạo các bản thiết kế an toàn và chính sách quan trọng được kiểm tra và thực hiện. Phát triển các kế hoạch dự phòng quan trọng để ứng phó sự cố.
  + Thiết kế vật lý: đánh giá các công nghệ an toàn phù hợp cần thiết để hỗ trợ bản thiết kế này, xây dựng các biện pháp thay thế và đưa ra 1 bản thiết kế cuối cùng, đánh giá tính khả thi của bản thiết kế.

Một số yếu tố thiết kế khác có thể được xây dựng:

* + Chính sách ATTT
  + Chương trình SETA: được thiết kế để giảm thiểu nhưng sai sót không đáng có của nhân viên.
  + Xây dựng các biện pháp kiểm soát: bao gồm: kiểm soát quản lý, kiểm soát hoạt động và kiểm soát kỹ thuật.
  + Tạo các tài liệu chuẩn bị trước: lập kế hoạch dự phòng.
  + An toàn vật lý

## Tại sao cần bảo trì đối với hệ thống quản lý an toàn thông tin.

* Cần bảo trì đối với hệ thống quản lý ATTT vì môi trường bên trong và hệ thống sẽ thay đổi thường xuyên. Nếu không theo dõi, kiểm tra, điều chỉnh, bảo trì thích hợp với những thay đổi này có thể phải bắt đầu lại chu trình quản lý ATTT lại từ đầu.

## Khái niệm, vai trò và phân loại chính sách ATTT.

* CSATTT là các hướng dẫn bằng văn bản do cấp quản lý cung cấp nhằm thông báo cho nhân viên và những người khác tại nơi làm việc về hành vi thích hợp liên quan đến việc sử dụng thông tin và tài sản thông tin một cách thích hợp và an toàn.
* Vai trò
  + Một chương trình ATTT chất lượng bắt đầu và kết thúc với chính sách.
  + Là nền tảng thiết yếu của một chương trình ATTT hiệu quả.
  + Có vị trí trung tâm đối với tất cả các vấn đề trong lĩnh vực ATTT.
  + Được thiết kế để tạo ra một môi trường làm việc năng suất và hiệu quả, không có những phiền nhiễu không cần thiết và các hành động không phù hợp.
  + Được phát triển và thực hiện một cách thích hợp cho phép chương trình ATTT hoạt động gần như liên tục tại tổ chức.
  + Là phương tiện kiểm soát ít tốn kém nhất, nhưng thường khó thực hiện nhất.
  + Là tài liệu tham khảo quan trọng:
    - Đối với đánh giá nội bộ
    - Để giải quyết các tranh chấp pháp lý về trách nhiệm giải trình của ban quản lý
    - Các văn bản chính sách có thể hoạt động như một tuyên bố rõ ràng về ý định của ban quản lý
  + Có thể là một trong số rất ít các biện pháp kiểm soát hoặc biện pháp bảo vệ một số thông tin nhất định.
* Phân loại

Ba loại CSATTT (NIST SP 800-14):

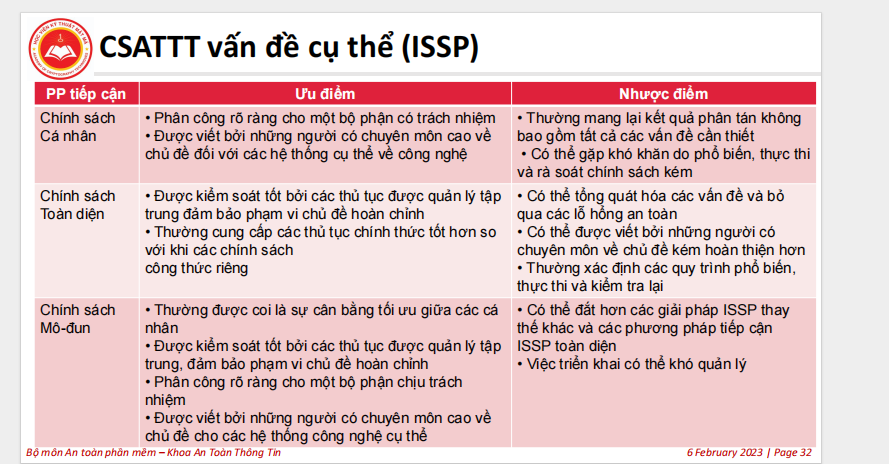
* CSATTT doanh nghiệp (Enterprise information security policy - EISP), đặt ra định hướng chiến lược, phạm vi và tư tưởng cho tất cả các nỗ lực an toàn; EISP phải dựa trên và hỗ trợ các tuyên bố về tầm nhìn và sứ mệnh của tổ chức.
* CSATTT vấn đề cụ thể (Issue-specific security policies - ISSP), cung cấp hướng dẫn cho tất cả các thành viên của tổ chức về việc sử dụng CNTT.
* CSATTT hệ thống cụ thể (System-specific security policies - SysSP), hướng dẫn việc quản lý và các thông số kỹ thuật của các công nghệ và hệ thống cụ thể.

## Phân biệt các khái niệm: chính sách, tiêu chuẩn, thủ tục.

* Chính sách: Tuyên bố về quan điểm của tổ chức nhằm tác động và xác định các quyết định và hành động, sử dụng để kiểm soát mọi người và sự phát triển của các thủ tục.
* Thủ tục: Hướng dẫn từng bước được thiết kế để hỗ trợ mọi người tuân theo tiêu chuẩn, chính sách, hướng dẫn.
* Tiêu chuẩn: Tuyên bố chi tiết về những việc phải làm để tuân thủ chính sách, đôi khi được xem như các quy tắc chi phối việc tuân thủ chính sách.

=> Các chính sách xác định những gì bạn có thể làm và không nên làm, trong khi các tài liệu khác tập trung vào cách làm.

## Liệt kê và mô tả ba cách tiếp cận để xây dựng CS cho vấn đề cụ thể. Theo bạn, cái nào là phù hợp nhất để sử dụng cho một tổ chức nhỏ và tại sao; Nếu tổ chức mục tiêu lớn hơn rất nhiều, thì cách tiếp cận nào sẽ phù hợp hơn và tại sao.



Ba cách tiếp cận để xây dựng CS cho vấn đề cụ thể (ISSP):

• Chính sách cá nhân: tạo một số tài liệu ISSP, mỗi tài liệu phù hợp với một vấn đề cụ thể.

• Chính sách toàn diện: tạo một tài liệu ISSP toàn diện duy nhất bao gồm tất cả các vấn đề.

• Chính sách mô-đun: Tạo một tài liệu ISSP mô-đun thống nhất việc tạo và quản lý chính sách trong khi vẫn duy trì các yêu cầu của từng vấn đề cụ thể.

* Chính sách toàn diện phù hợp cho tổ chức nhỏ; Chính sách cá nhân phù hợp cho tổ chức lớn; Chính sách mô-đun phù hợp cho tổ chức vừa

## Tại sao muốn quản lí chính sách và chuẩn an toàn thông tin thành công thì phải xác định được các lớp người dùng chính sách; Làm thế nào để đạt được sự đồng thuận của tất cả người dùng trong tổ chức.

Xác định lớp người dùng cơ sở giúp xác định rõ vai trò, quyền hạn và trách nhiệm của từng nhóm người dùng trong tổ chức đối với thông tin, hệ thống thông tin (mỗi nhóm người dùng có nhu cầu và quyền hạn riêng).

Để đạt được sự đồng thuận của người dùng trong tổ chức thì:

* Tạo ra chính sách và quy trình rõ ràng.
* Tạo các buổi đào tạo, nâng cao nhận thức ATTT cho người dùng => để giải thích về chính sách và chuẩn ATTT.
* Thiết lập việc kiểm tra và đánh giá việc tuân thủ từ phía người dùng.
* Lấy ý kiến đóng góp từ các bên ảnh hưởng, người dùng trong tổ chức => sửa đổi tài liệu phù hợp.

## Nêu các nguyên tắc phát triển chính sách và chuẩn; Trình bày nguyên tắc Trách nhiệm, phòng thử chiều sâu or (đánh giá lại, đặc quyền tối thiểu).

Những nguyên tắc phát triển CS và chuẩn:

* Trách nhiệm
* Nhận thức
* Đạo đức
* Đa ngành, đa lĩnh vực
* Tỉ lệ (Proportionality)
* Tích hợp
* Phòng thủ chiều sâu
* Kịp thời
* Đánh giá lại
* Dân chủ
* Kiểm soát nội bộ
* Đối thủ (Adversary)
* Đặc quyền tối thiểu
* Phân chia nhiệm vụ
* Tính đơn giản
* AT lấy chính sách làm trung tâm

Nguyên tắc trách nhiệm:

* Cần phải rõ ràng
* Đảm bảo mọi người hiểu về trách nhiệm của mình trước hành động mà họ thực hiện khi sử dụng tài nguyên của tổ chức

Nguyên tắc Phòng thủ chiều sâu:

* Áp dụng các lớp kiểm soát và bảo vệ với khả năng phòng ngừa, phát hiện và ứng phó sẽ làm tăng tính AT
* Cơ chế AT được phân tầng để điểm yếu của một cơ chế bảo vệ được hai hay nhiều cơ chế khác ngăn chặn

Nguyên tắc Đánh giá lại:

* Sự AT nên được đánh giá định kì vì rủi ro thay đổi hàng ngày
* Cũng cần đánh giá lại chuẩn ít nhất 1 lần/năm để đảm bảo chúng vẫn phù hợp

Nguyên tắc đặc quyền tối thiểu:

* các 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 nhiệm vụ của họ. Đặc quyền tối thiểu giả định một nhu cầu cần biết và ngụ ý quyền truy cập hạn chế vào cấp độ cần thiết cho các nhiệm vụ được giao. Ví dụ: nếu một tác vụ chỉ yêu cầu đọc dữ liệu, người dùng được cấp quyền truy cập chỉ đọc, không cho phép tạo, cập nhật hoặc xóa dữ liệu.

## Nêu các thành phần trong khung mẫu chính sách ATTT; Tại sao ko có phần khen thưởng, xử phạt ở đây.

Tên chính sách và thông tin định danh:

1. Mục đích
2. Tổng quan
3. Phạm vi
4. Chính sách
5. Vai trò trách nhiệm
6. Luật/hướng dẫn áp dụng
7. Tính hiệu lực
8. Thông tin và hỗ trợ
9. Phê chuẩn
10. Tài liệu tham khảo

* Không có phần khen thưởng, xử phạt ở đây vì…..

## Khái niệm và vai trò của QLRR; Trình bày ngắn gọn quy trình quản lý rủi ro; Tại sao 2 quy trình truyền thông và tư vấn rủi ro, giám sát và soát xét rủi ro cần thực hiện song song và xuyên suốt quá trình.

**Quản lý rủi ro** là quá trình tiếp cận rủi ro một cách khoa học và có hệ thống nhằm nhận diện, kiểm soát, phòng ngừa và giảm thiểu những tổn thất, mất mát, những ảnh hưởng bất lợi của rủi ro.

**Vai trò** của QLRR là để hạn chế tối đa các tác động của rủi ro cần có một phương pháp quản lý rủi ro trong HTTT một cách hiệu quả.

**Quy trình quản lý rủi ro**:

* Thiết lập bối cảnh.
* Đánh giá rủi ro.
* Xử lý rủi ro.
* Chấp nhận rủi ro.
* Truyền thông và tư vấn rủi ro ATTT.
* Giám sát và soát xét rủi ro ATTT.

Tại sao 2 quy trình …?

## Tại sao và khi nào cần tiến hành khảo sát và phân tích rủi ro; Trình bày các phương pháp phân tích rủi ro.

Tại sao và khi nào cần tiến hành khảo sát và phân tích rủi ro????

**Phương pháp phân tích rủi ro**:

* Định tính: xác định hệ quả, xác suất và mức độ rủi ro bằng các mức như “cao”, “trung bình” và “thấp”, có thể kết hợp hệ quả và xác suất, và đánh giá mức độ rủi ro theo các tiêu chí định tính.
* Bán định lượng: sử dụng thang chia bằng số đối với hệ quả và xác suất kết hợp chúng để đưa ra một mức rủi ro bằng cách sử dụng công thức. Thang đo có thể là tuyến tính hoặc theo logarit, hay có mối quan hệ khác nào đó, công thức được sử dụng cũng có thể khác nhau.
* Định lượng: ước tính giá trị thực tế đối với hệ quả và xác suất của chúng, và đưa ra giá trị về mức rủi ro theo các đơn vị cụ thể được xác định khi xây dựng bối cảnh.

## Mục đích của giai đoạn nhận diện rủi ro là gì; Nêu các phương pháp nhận diện rủi ro; Cho ví dụ minh họa về phương pháp thiết lập bảng kê trong nhận diện rủi ro.

Mục đích của giai đoạn nhận diện rủi ro:

+ Là quá trình tìm kiếm, thừa nhận và ghi lại các rủi ro

+ Bao gồm:

* Nhận biết về tài sản: để xác định danh mục các tài sản của tổ chức cần bảo vệ bao gồm TT, HTTT.
* Nhận biết về mối đe dọa: để xác định các mối đe dọa đối với mỗi tài sản.
* Nhận biết về điểm yếu: để xác định các điểm yếu có thể tồn tại đối với mỗi tài sản.

=> Kết quả: danh mục các mối đe dọa và điểm yếu đối với các tài sản được xác định

Phương pháp nhận diện rủi ro:

* Thiết lập bảng kê
* Phân tích tài chính
* Phương pháp lưu đồ
* Phân tích công nghệ
* Kiểm tra hiện trường
* Tham khảo các chuyên gia khác trong tổ chức
* Phương pháp thông qua tư vấn
* Phương pháp phân tích hợp đồng
* Nghiên cứu các số liệu tổn thất trong quá khứ
* Nhận diện những mối nguy tiềm năng

Ví dụ minh họa về phương pháp thiết lập bảng kê trong nhận diện rủi ro: ????

## Khái niệm và mục đích của Ước lượng rủi ro là gì; Trình bày các phương pháp giúp xác định ước lượng rủi ro.

\* Khái niệm và mục đích của Ước lượng rủi ro:

Ước lượng rủi ro là quá trình đánh giá rủi ro như những đe dọa và cơ hội tiềm năng:

Ước lượng rủi ro đưa ra:

+ Xác suất rủi ro: cho biết rủi ro có xảy ra hay không

+ Tác động của rủi ro: Khi xảy ra có lớn hay không, lớn bao nhiêu, tác động tích cực hay tiêu cực

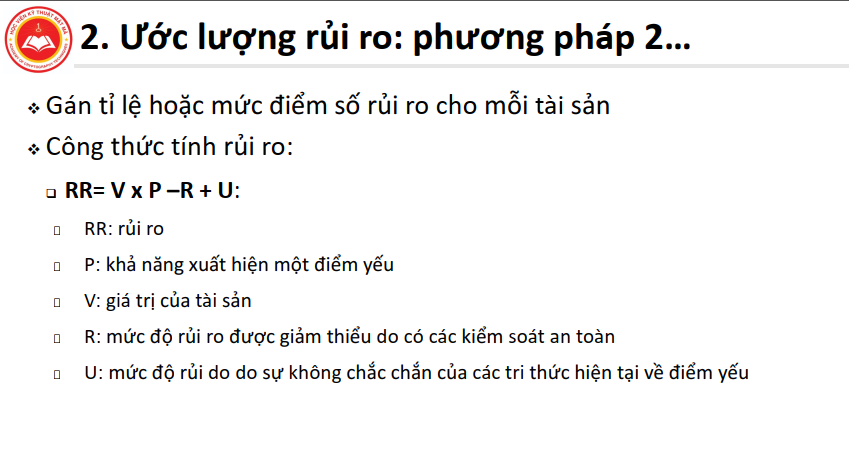
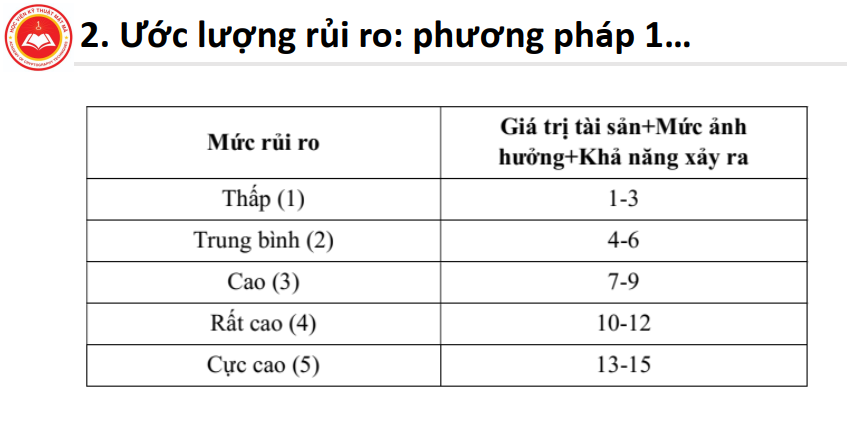
=> Mục đích để đưa ra các quyết định phù hợp đối với các rủi ro

Rủi ro được tính giá trị bằng công thức: Mức rủi ro = f(hệ quả rủi ro, khả năng xảy ra)

Rủi ro được xếp hạng ưu tiên từ cao đến thấp theo các giá trị mức rủi ro tính toán được

Tùy theo tổ chức và đặc thù từng quá trình/dự án, chủ quá trình/trưởng dự án sẽ xác định những rủi ro nào cần đưa vào kiểm soát theo mức ưu tiên.

\* Các phương pháp giúp xác định ước lượng rủi ro:



## Sau khi xác định ước lượng rủi ro cho từng tài sản, tổ chức cần làm gì để đáp ứng mục tiêu đề ra.



## Mục tiêu, Nguyên tắc và các thành phần của COSO, COBIT 5

**Mục tiêu COSO**: xác định các yếu tố gây ra báo cáo tài chính gian lận và đưa ra các khuyến nghị để giảm tỷ lệ mắc phải.

**Thành phần của COSO:**

* Kiểm soát môi trường.
* Đánh giá rủi ro.
* Kiểm soát hoạt động.
* Thông tin và truyền thông.
* Giám sát.

**Nguyên tắc của COSO**:

**Nguyên tắc 1**: Đơn vị thể hiện được cam kết về tính chính trực và giá trị đạo đức.

**Nguyên tắc 2**: HĐQT chứng minh được sự độc lập với nhà quản lý và thực thi việc giám sát sự phát triển và hoạt động của KSNB.

**Nguyên tắc 3:** Nhà quản lý dưới sự giám sát của HĐQT cần thiết lập cơ cấu tổ chức, quy trình báo cáo, phân định trách nhiệm và quyền hạn nhằm đạt được mục tiêu của đơn vị.

**Nguyên tắc 4:** Đơn vị phải thể hiện sự cam kết về việc sử dụng nhân viên có năng lực thông qua tuyển dụng, duy trì và phát triển nguồn nhân lực phù hợp với mục tiêu của đơn vị.

**Nguyên tắc 5:** Đơn vị cần yêu cầu các cá nhân chịu trách nhiệm báo cáo về trách nhiệm của họ trong việc đáp ứng các mục tiêu của tổ chức.

**Nguyên tắc 6:** Đơn vị phải thiết lập mục tiêu rõ ràng và đầy đủ để xác định và đánh giá các rủi ro phát sinh trong việc đạt được mục tiêu của đơn vị.

**Nguyên tắc 7:** Đơn vị phải nhận diện rủi ro trong việc đạt được mục tiêu của đơn vị, tiến hành phân tích rủi ro để xác định rủi ro cần được quản lý như thế nào.

**Nguyên tắc 8:** Đơn vị cần xem xét các loại gian lận tiềm tàng khi đánh giá rủi ro đối với việc đạt mục tiêu của đơn vị.

**Nguyên tắc 9:** Đơn vị cần xác định và đánh giá những thay đổi của môi trường ảnh hưởng đến KSNB.

**Nguyên tắc 10:** Đơn vị phải lựa chọn và phát triển các hoạt động kiểm soát để góp phần hạn chế các rủi ro giúp đạt mục tiêu trong giới hạn chấp nhận được.

**Nguyên tắc 11:** Đơn vị lựa chọn và phát triển các hoạt động kiểm soát chung với công nghệ hiện đại để hỗ trợ cho việc đạt được các mục tiêu.

**Nguyên tắc 12:** Đơn vị tổ chức triển khai hoạt động kiểm soát thông qua nội dung các chính sách đã được thiết lập và triển khai chính sách thành các hành động cụ thể.

**Nguyên tắc 13:** Đơn vị thu thập, truyền đạt và sử dụng thông tin thích hợp, có chất lượng để hỗ trợ những bộ phận khác của KSNB.

**Nguyên tắc 14**: Đơn vị cần truyền đạt trong nội bộ những thông tin cần thiết, bao gồm cả mục tiêu và trách nhiệm đối với KSNB, nhằm hỗ trợ cho chức năng kiểm soát.

**Nguyên tắc 15:** Đơn vị cần truyền đạt cho các đối tượng bên ngoài đơn vị về các vấn đề ảnh hưởng đến KSNB.

**Nguyên tắc 16:** Đơn vị phải lựa chọn, triển khai và thực hiện việc đánh giá liên tục hoặc định kỳ để biết chắc rằng liệu những thành phần nào của KSNB có hiện hữu và đang hoạt động.

**Nguyên tắc 17:** Đơn vị phải đánh giá và thông báo những yếu kém của KSNB một cách kịp thời cho các đối tượng có trách nhiệm bao gồm nhà quản lý và HĐQT để có những biện pháp khắc phục.

**Mục tiêu COBIT**: Cung cấp một khuôn khổ cụ thể cho quản lý doanh nghiệp, quản lý CNTT, cung cấp cho kiểm soát viên quy trình và kiểm soát để phát triển CNTT trong tổ chức.

**COBIT được xây dựng với ba thành phần cơ bản:**

* IT Resource: nguồn tài nguyên CNTT.
* Business Requirements: yêu cầu nghiệp vụ.
* IT Processes: quy trình CNTT.

**Nguyên tắc COBIT 5**:

* Đáp ứng nhu cầu các bên liên quan.
* Bao phủ toàn bộ hoạt động của tổ chức.
* Áp dụng duy nhất một khuôn khổ đơn thích hợp.
* Tạo một giải pháp tiếp cận toàn diện.
* Phân tách quản trị từ quản lý.

## Tại sao cần triển khai ISMS trong tổ chức; Phân biệt ISO/IEC 27001 vs 27002

Hệ thống QLATTT (ISMS) sẽ giúp tổ chức thực hiện kiểm soát và định hướng cho các hoạt động đảm bảo ATTT. Việc hệ thống vận hành tốt sẽ giúp công tác đảm bảo ATTT tại tổ chức được duy trình liên tục, được xem xét đánh giá định kỳ và không ngừng cải tiến để đối phó với các rủi ro mới phát sinh. Các hoạt động đảm bảo ATTT trong tổ chức sẽ mang tính hệ thống, giảm sự phụ thuộc vào cán bộ thực thi và luôn được xem xét, đánh giá để nâng cao hiệu quả

* Tăng khả năng phục hồi sau tấn công: ISMS cả thiện khả năng chuẩn bị, ứng phó phục hồi sau bất kỳ cuộc tấn công mạng nào
* Quản lý tất cả dữ liệu của bạn ở một nơi: Là khung quản lý trung tâm cho thông tin của tổ chức, ISMS cho phép bạn quản lý mọi thứ ở một nơi

|  |  |
| --- | --- |
| Code practice (“Hướng dẫn thực hiện”) | Certification Standard (“Tiêu chuẩn chứng nhận”) |
| Reference (Tham chiếu) | Requirement (Yêu cầu) |
| Should do (Nên làm) | Shall (Phải làm) |
| Non-auditable (Không kiểm tra được) | Auditable (Có thể kiểm tra) |
| Không có tiêu chuẩn về chứng chỉ/chứng nhận | Có chứng chỉ/chứng nhận |

* Mục đích: ISO 27001 là tiêu chuẩn chứng nhận, trong khi ISO 27002 cung cấp các biện pháp kiểm soát tốt nhất. Nói các khác, các tổ chức có thể được chứng nhận theo ISO 27001 nhưng không được chứng nhận theo ISO 27002

## Trình bày quá trình chứng nhận đạt chuẩn; Các yếu tố quan trọng của việc áp dụng thành công chuẩn là gì.

**Quá trình chứng nhận đạt chuẩn**:

* Tiếp xúc ban đầu.
* Nộp đơn.
* Đánh giá giai đoạn 1.
* Đánh giá giai đoạn 2.
* Cấp chứng chỉ.
* Giám sát.
* Tái chứng nhận.

**10 yếu tố quan trọng của việc áp dụng chuẩn:**

* Chính sách và mục tiêu ATTT và các hoạt động phản ánh mục tiêu kinh doanh.
* Một cách tiếp cận và khuôn khổ của việc áp dụng, duy trì, theo dõi và cải tiến hoàn toàn thống nhất với văn hoá của tổ chức.
* Sự hỗ trợ đáng kể và cam kết từ mọi cấp lãnh đạo.
* Hiểu biết thấu đáo các yêu cầu ATTT, đánh giá rủi ro và kiểm soát rủi ro.
* Tuyên truyền một cách hiệu quả về ATTT đến tất cả các cấp quản lý, nhân viên và các bên để có nhận thức.
* Phân phát hướng dẫn về tiêu chuẩn và CSATTT cho mọi cấp quản lý, nhân viên và các bên.
* Cung cấp tài chính cho các hoạt động quản lý ATTT.
* Cung cấp nhận thức, đào tạo và giáo dục thích hợp.
* Thiết lập một quá trình hiệu lực kiểm soát sự cố ATTT.
* Áp dụng một hệ thống đo lường để đánh giá hoạt động hệ thống.

Trải qua nhiều hoạt động khác nhau, trong đó nổi bật là hai phần kiểm tra tài liệu hiện hành và kiểm tra vận hành thực tế

Về việc kiểm tra tài liệu hiện hành, giai đoạn này nhấn mạnh vào việc xem xét và đánh giá các tài liệu liên quan đến hệ thống quản lý an toàn thông tin của tổ chức.

Về kiểm tra vận hành thực tế, kiểm toán viên sẽ đánh giá việc thực hiện ISMS và xác minh tính tuân thủ của tổ chức đối với tiêu chuẩn ISO/IEC 27001.

## Lập kế hoạch dự phòng (CP) là gì; Trình bày ngắn gọn về mục đích của các thành phần chính trong CP.

Lập kế hoạch dự phòng (Contingency planning - CP) là quá trình mà các cộng đồng quan tâm đến CNTT và ATTT định vị tổ chức của họ để chuẩn bị, phát hiện, phản ứng và phục hồi từ các sự kiện đe dọa đến an toàn của tài nguyên và tài sản thông tin, cả con người và nhân tạo.

CP được tạo thành từ 4 thành phần chính:

* **Quy trình thu thập dữ liệu và tài liệu được gọi là phân tích tác động kinh doanh (business impact analysis - BIA)**: là nền tảng quan trọng cho các giai đoạn lập kế hoạch ban đầu. Là một cuộc điều tra và đánh giá các sự kiện bất lợi có thể ảnh hưởng đến tổ chức, bao gồm việc xác định mức độ quan trọng của hệ thống hoặc bộ thông tin đối với các quá trình cốt lõi của tổ chức và các ưu tiên phục hồi của nó.
* **Kế hoạch Ứng phó sự cố (Incident response plan - IRP):** Là một tập hợp chi tiết các quy trình và thủ tục lập kế hoạch, phát hiện và giải quyết các ảnh hưởng của một sự kiện bất ngờ đối với tài nguyên và tài sản thông tin, hướng dẫn giúp người ứng phó sự cố phát hiện và ứng phó với các sự cố an toàn. Là bước quan trọng đầu tiên của quản lý sự cố ATTT. Lãnh đạo cao nhất phải xác nhận kế hoạch này và tham gia vào mọi bước của chu trình quản lý sự cố.
* **Kế hoạch khôi phục sau thảm họa (Disaster recovery plan - DRP):** đòi hỏi sự chuẩn bị và phục hồi sau thảm họa, cho dù là tự nhiên hay nhân tạo. Mục đích là xử lý và khôi phục hiệu quả những sự cố mà IRP không có khả năng xử lý.
* **Kế hoạch liên tục kinh doanh (Business continuity plan BCP):** Đảm bảo các chức năng kinh doanh quan trọng vẫn tiếp tục nếu một sự cố nghiêm trọng hoặc thảm họa xảy ra. BCP có thể bao gồm các điều khoản cho địa điểm nóng, địa điểm ấm, địa điểm lạnh, chia sẻ thời gian, văn phòng dịch vụ và các thỏa thuận chung.

## A/C hãy cho biết nhóm CP tạo ra ba bộ quy trình xử lý sự cố như thế nào. (phân vân)

Nhóm CP tạo ra ba bộ quy trình xử lý sự cố:

* **Trong khi xảy ra sự cố** - Các nhà lập kế hoạch phát triển và ghi lại các thủ tục phải được thực hiện trong sự cố. Các thủ tục này được nhóm lại và giao cho các cá nhân. Nhiệm vụ của quản trị viên hệ thống khác với nhiệm vụ quản lý, vì vậy các thành viên của uỷ ban lập kế hoạch phải soạn thảo một bộ quy trình cụ thể theo chức năng.
* **Sau khi sự cố xảy ra** - Sau khi các thủ tục xử lý sự cố được soạn thảo, các nhà lập kế hoạch xây dựng và ghi lại các thủ tục phải được thực hiện ngay sau khi sự cố chấm dứt. Một lần nữa, các khu vực chức năng riêng biệt có thể phát triển các thủ tục khác nhau.
* **Trước khi sự cố xảy ra** - Các nhà lập kế hoạch soạn thảo một bộ thủ tục thứ ba: những nhiệm vụ phải được thực hiện để chuẩn bị cho sự cố, bao gồm các hành động có thể giảm thiểu bất kỳ thiệt hại nào từ sự cố. Các thủ tục này bao gồm chi tiết về lịch trình sao lưu này bao gồm chi tiết về lịch trình sao lưu dữ liệu, chuẩn bị khắc phục thảm họa, lịch đào tạo, kế hoạch thử nghiệm.

## A/c hãy trình bày các giai đoạn cơ bản của hành động ứng cứu sự cố.

Cái này lấy ở đâu thế? sao thấy slide có 6 giai đoạn hay theo Nist thì có 4 giai đoạn? thấy cũng đúng nhưng bổ sung thêm để tham khảo (lan anh)

* Sự chuẩn bị: theo dõi, thu thập các sự kiện ATTT
* Phát hiện và phân tích: nhận diện, cảnh báo, điều tra và xác minh sự cố (xem có đúng sự cố đang xảy ra hay không)
* Phản ứng sự cố: Ngăn chặn và xóa bỏ sự cố => giúp giảm thiểu tối đa thiệt hại mà sự cố gây ra
* Phục hồi: khôi phục dữ liệu và khôi phục hoạt động bình thường của hệ thống
* Hành động sau sự cố: tài liệu hóa sự cố, đánh giá xây dựng chiến lược ứng cứu sự cố.

(Thắng)

Các hành động ứng cứu sự cố có thể được tổ chức thành ba giai đoạn cơ bản:

* Phát hiện - Nhận biết rằng một sự cố đang được tiến hành.
* Phản ứng - Phản ứng với sự cố theo cách thức định trước để ngăn chặn và giảm thiểu thiệt hại tiềm ẩn của nó.
* Phục hồi - Trả lại tất cả các hệ thống và dữ liệu về trạng thái của chúng trước khi xảy ra sự cố.

## Trình bày các tùy chọn của tổ chức để bảo vệ thông tin sau một sự cố.

Các tùy chọn của tổ chức để bảo vệ thông tin sau một sự cố là:

* Sao lưu dữ liệu truyền thống.
* Kho lưu trữ điện tử.
* Ghi nhận ký từ xa.
* CSDL shadowing.

Khuyến nghị:

* Quy tắc “3-2-1”: Khuyến khích duy trì ba bản sao dữ liệu quan trọng (bản gốc và 2 bản sao lưu) trên ít nhất hai phương tiện khác nhau (như ổ cứng và sao lưu băng), với ít nhất một bản sao được lưu trữ ngoài trang web.
* Các bản sao lưu hàng ngày được lưu trữ tại chỗ và bản sao lưu hàng tuần được lưu trữ bên ngoài.

## Donald Pipkin đã xác định các loại chỉ báo sự cố nào Để giúp việc phát hiện sự cố trở nên đáng tin cậy hơn; Trình bày về các chỉ số đó.

Ba loại chỉ số sự cố được sử dụng: có thể, có thể xảy ra và xác định.

Chỉ số có thể:

* Sự hiện diện của các file không quen thuộc.
* Hiện diện hoặc thực thi các chương trình hoặc quy trình không xác định.
* Tiêu thụ tài nguyên máy tính một cách bất thường.
* Hệ thống bị treo bất thường.

Chỉ số có thể xảy ra:

* Hoạt động vào những thời điểm không mong muốn.
* Sự hiện diện của các tài khoản mới.
* Các cuộc tấn công được báo cáo.
* Thông báo từ IDPS.

Chỉ số xác định:

* Sử dụng tài khoản không bình thường.
* Thay đổi nhật ký.
* Sự hiện diện của các công cụ hacker.
* Thông báo của đối tác hoặc đồng nghiệp.
* Thông báo của tin tặc.

## Trình bày quy trình phục hồi sau sự cố; Khi nào sự cố trở thành thảm họa.

Khi sự cố được kiểm soát và kiểm soát hệ thống đã được khôi phục, quá trình khắc phục sự cố có thể bắt đầu.

Quy trình phục hồi:

* Xác định các lỗ hổng cho phép sự cố xảy ra và lan rộng. Giải quyết chúng.
* Xử lý các biện pháp bảo vệ không thể ngăn chặn hoặc hạn chế sự cố hoặc không có trong hệ thống ngay từ đầu. Cài đặt, thay thế hoặc nâng cấp chúng.
* Đánh giá khả năng giám sát (nếu có). Cải thiện các phương pháp phát hiện và báo cáo hoặc cài đặt các khả năng giám sát mới.
* Khôi phục dữ liệu từ các bản sao lưu, nếu cần.
* Khôi phục cách dịch vụ và quy trình đang sử dụng.
* Liên tục giám sát hệ thống.
* Khôi phục niềm tin của các thành viên trong cộng đồng quan tâm của tổ chức => để ngăn chặn sự hoảng loạn hoặc nhầm lẫn gây ra gián đoạn thêm cho hoạt động của tổ chức.

Sự cố trở thành thảm hoạ khi:

* Tổ chức không thể giảm thiểu tác động của một sự cố trong khi sự cố xảy ra.
* Mức độ thiệt hại hoặc phá huỷ quá nghiêm trọng khiến tổ chức không thể nhanh chóng phục hồi.
* Tuỳ thuộc vào tổ chức để quyết định sự cố nào được phân loại là thảm hoạ và do đó nhận được mức độ phản ứng thích hợp.

**Phần 2: Bài tập**

Bài 1. Xây dựng chính sách an toàn thông tin cho một hệ thống cụ thể (một hệ thống nhỏ hoặc một phần trong hệ thống, cần phải tuân thủ khuôn mẫu của chính sách an toàn thông tin).

Thực hiện viết 1 số chính sách ISSP:

* + Chính sách an toàn thông tin cho máy tính cá nhân của nhân viên trong một tổ chức bán hàng trực tuyến.
  + Chính sách cho bàn làm việc sạch sẽ cho các nhân viên trong công ty
  + Chính sách về mật khẩu mạnh
  + Chính sách về bảo mật thông tin khách hàng trong giao dịch thương mại điện tử
  + Chính sách về sử dụng email trong tổ chức
  + Chính sách về sao lưu phục hồi
  + Chính sách về trao đổi thông tin
  + Chính sách bảo mật nhân sự

Bài 2. Ước lượng rủi ro cho một hệ thống.

**Bố cục đề thi**: 02 câu lý thuyết mỗi câu 02 điểm, 02 câu bài tập mỗi câu 03 điểm