**ĐỀ CƯƠNG ÔN TẬP MÔN QLATTT**

**Phần 1: Lý thuyết**

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

Mối quan hệ giữa hiểm họa, điểm yếu và rủi ro thường được liên kết chặt chẽ trong quản lý rủi ro và thảm họa. Dưới đây là phân tích của mối quan hệ này:

- ***Hiểm họa (Hazard):*** Là một sự kiện hoặc điều kiện tiềm ẩn có khả năng gây ra tổn thất hoặc thiệt hại cho con người, tài sản, hoặc môi trường. Hiểm họa có thể là tự nhiên như lũ lụt, động đất, hoặc do con người tạo ra như ô nhiễm môi trường, tai nạn công nghiệp.

- ***Điểm yếu (Vulnerability):*** Là mức độ mà một hệ thống, cộng đồng hoặc tài sản có thể bị ảnh hưởng hoặc bị tổn thương bởi hiểm họa. Điểm yếu phụ thuộc vào nhiều yếu tố như cấu trúc xã hội, kinh tế, cơ sở hạ tầng, và khả năng phục hồi.

- ***Rủi ro (Risk):*** Là khả năng xảy ra tổn thất do sự kết hợp giữa hiểm họa và điểm yếu. Rủi ro được định nghĩa là sản phẩm của hiểm họa và điểm yếu, và nó thường được biểu diễn qua công thức: Rủi ro = Hiểm họa x Điểm yếu / Khả năng đối phó.

Để giảm thiểu rủi ro, cần phải có các biện pháp nhằm giảm điểm yếu và tăng cường khả năng đối phó của cộng đồng trước hiểm họa. Việc sử dụng các kỹ thuật địa không gian trong quản lý rủi ro lũ lụt là một ví dụ về cách tiếp cận này, nơi mà dữ liệu sinh học và kinh tế xã hội được sử dụng để đánh giá rủi ro liên quan đến lũ lụt trong các môi trường khác nhau.

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

Việc xác định rủi ro đóng một vai trò cực kỳ quan trọng trong Quản lý an toàn thông tin (Information Security Management - ISM). Dưới đây là những điểm chính về tầm quan trọng của việc xác định rủi ro trong ISM:

***Xác định Mối Đe Dọa:*** Việc xác định rủi ro giúp tổ chức nhận diện các mối đe dọa tiềm ẩn đối với thông tin, từ phần mềm độc hại đến sự cố bảo mật CNTT và các sự kiện khác có thể làm gián đoạn hoạt động kinh doanh.

***Đánh Giá Tác Động:*** Nó cho phép đánh giá tác động tiềm ẩn của các rủi ro đã xác định, giúp tổ chức chuẩn bị tốt hơn để ứng phó với các mối đe dọa.

***Phát Triển Chiến Lược:*** Phân tích rủi ro cung cấp cơ sở khoa học để xây dựng chiến lược và quyết định quản lý an toàn thông tin, từ đó giúp tối ưu hóa tài nguyên và đảm bảo hiệu suất cao trong việc giảm thiểu rủi ro.

***Tuân Thủ Tiêu Chuẩn:*** Việc xác định rủi ro là một phần không thể thiếu trong việc tuân thủ các tiêu chuẩn quốc tế như ISO/IEC 27001, đặc biệt là trong việc thiết lập và duy trì Hệ thống quản lý an toàn thông tin.

***Cải Thiện An Toàn:*** Nó giúp thiết lập các biện pháp ngăn chặn hiệu quả, nâng cao nhận thức và kỹ năng an toàn thông tin cho nhân viên, và định hình một môi trường làm việc an toàn và bền vững.

Như vậy, việc xác định rủi ro là bước đầu tiên và quan trọng nhất trong quá trình quản lý an toàn thông tin, giúp tổ chức phòng ngừa và giảm thiểu rủi ro một cách hiệu quả

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

Luật pháp và đạo đức đóng vai trò rất quan trọng trong quản lý an toàn thông tin. Cả hai yếu tố này đều có mục đích là đảm bảo rằng thông tin quan trọng của tổ chức được bảo vệ khỏi các mối đe dọa bảo mật.

- 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

# 4. 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.

* ***Khái niệm:*** lập kế hoạch là quá trình xác định các mục tiêu và lựa chọn các phương thức hành động để đạt được các mục tiêu đó. Nó bao gồm việc phân tích tình hình hiện tại, đánh giá các điểm mạnh, điểm yếu, cơ hội và thách thức, từ đó xây dựng một loạt các bước cụ thể và lập lịch trình để thực hiện mục tiêu đã đặt ra. Lập kế hoạch đòi hỏi tính logic, sự sáng tạo và khả năng dự đoán để đạt được kết quả mong muốn trong tương lai.
* ***Vai trò:*** Lập kế hoạch là phương tiện chủ đạo để quản lý tài nguyên trong các tổ chức. Đòi hỏi việc liệt kê một chuỗi các hành động nhằm đạt được các mục tiêu, cụ thể trong một khoảng thời gian xác định và kiểm soát việc thực hiện các bước này. Cung cấp định hướng cho tương lai của tổ chức.
* ***Các thành phần cơ bản của một kế hoạch chiến lược cấp tổ chức điển hình:***
  1. Tóm tắt
  2. Tuyên bố về Sứ mệnh, Tầm nhìn và Giá trị
  3. Hồ sơ và lịch sử 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 (hoặc Sản phẩm/Dịch vụ)
  7. Phụ lục (nếu có, bao gồm phân tích thị trường, khảo sát nội bộ/bên ngoài, ngân sách và dự kiến R&D).

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

\* Việc triển khai ATTT thường được bắt đầu theo một trong hai cách: từ dưới lên hoặc từ trên xuống.

***Hướng tiếp cận từ trên xuống:***

- Để thành công, quản lý cấp cao phải nỗ lực và cung cấp hỗ trợ đầy đủ cho tất cả các bộ phận

- Sự tham gia và hỗ trợ của người dùng cuối cũng rất quan trọng đối với sự thành công này. Người dùng cuối chính cần được chỉ định cho các nhóm lập kế hoạch và thiết kế tương tự như nhóm thiết kế ứng dụng chung (JAD) được sử dụng trong phát triển hệ thống.

- Các quy trình và thủ tục phải được lập thành văn bản và tích hợp vào văn hóa tổ chức, phải được xác nhận, thúc đẩy và hỗ trợ bởi ban quản lý của tổ chức.

# 6. 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.



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

***Mục tiêu chính*** của Security System Development Life Cycle (SecSDLC) là thực hiện việc xác định các rủi ro cụ thể và mối đe dọa mà chúng gây ra. Quá trình này bao gồm việc nhận diện các mối đe dọa cụ thể và đánh giá rủi ro mà chúng tạo ra, cũng như việc triển khai các biện pháp kiểm soát an ninh để chống lại, giảm thiểu và quản lý rủi ro.

***Giai đoạn thiết kế:***

*- thiết kế logic:* các bản thiết kế an toàn được tạo ra và các chính sách quan trọng được kiểm tra và thực hiện. Ở giai đoạn này, các kế hoạch dự phòng quan trọng để ứng phó sự cố được phát triển. Tiếp theo, phân tích tính khả thi xác định xem dự án có nên tiếp tục tự thực hiện hay nên thuê ngoài.

*- thiết kế vật lý:* công nghệ an toàn cần thiết để hỗ trợ các bản thiết kế này được đánh giá, các giải pháp thay thế được tạo ra, và một thiết kế cuối cùng được xác định. Tiếp tục, phân tích tính khả thi về mức độ sẵn sàng của tổ chức đối với dự án được đề xuất, sau đó giám đốc điều hành cấp cao và người sử dụng sẽ được trình bày với thiết kế (các bên có cơ hội phê duyệt (hoặc không phê duyệt) dự án trước khi bắt đầu triển khai).

*CSATTT:* một tập hợp các quy tắc bảo vệ tài sản của tổ chức, cung cấp hướng dẫn và các yêu cầu để bảo vệ tài sản thông tin của tổ chức. Có ba loại: CSATTT tổ chức hoặc chung, CSATTT các vấn đề cụ thể (ISSP) và CSATTT hệ thống cụ thể.

- Chương trình SETA (security education, training, and awareness) là một biện pháp kiểm soát được thiết kế để giảm các vi phạm an toàn ngẫu nhiên của nhân viên.

- xây dựng các biện pháp kiểm soát được sử dụng để bảo vệ TT khỏi các cuộc tấn công bởi các mối đe dọa, Có ba loại kiểm soát:

* Kiểm soát quản lý: các quy trình AT được thiết kế bởi các nhà hoạch định chiến lược và được thực thi bởi cơ quan quản lý AT của tổ chức.
* Kiểm soát hoạt động liên quan đến chức năng hoạt động AT trong tổ chức.
* Kiểm soát kỹ thuật đề cập đến các phương pháp tiếp cận kỹ thuật được sử dụng để thực hiện AT trong tổ chức.

- Tạo ra các tài liệu chuẩn bị cần thiết: kế hoạch dự phòng (bao gồm kế hoạch liên tục kinh doanh, kế hoạch khắc phục thảm họa và kế hoạch ứng phó sự cố)

- An toàn vật lý: đòi hỏi thiết kế, triển khai và duy trì các biện pháp đối phó để bảo vệ các nguồn lực vật lý của một tổ chức. Tài nguyên vật lý bao gồm con người, phần cứng và các yếu tố hệ thống hỗ trợ và các tài nguyên liên quan đến việc quản lý thông tin ở tất cả các trạng thái của nó - truyền, lưu trữ và xử lý.

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

Giai đoạn bảo trì là giai đoạn quan trọng nhất, do tính linh hoạt và tính bền bỉ của nhiều mối đe dọa mà tổ chức phải đối mặt. Các hệ thống An toàn thông tin cần theo dõi, kiểm tra, sửa đổi, cập nhật và sửa chữa liên tục. Nếu không điều chỉnh thích hợp với những thay đổi của môi trường bên trong hoặc bên ngoài, có thể cần phải bắt đầu lại chu trình.

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

***Khái niệm:*** Chính sách ATTT 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 chúng thường khó thực hiện nhất. (chỉ tốn thời gian và nỗ lực mà nhóm quản lý dành để tạo, phê duyệt và truyền đạt chúng cũng như nhân viên bỏ ra để tích hợp các chính sách vào các hoạt động hàng ngày của họ, Chi phí thuê chuyên gia tư vấn là nhỏ so với kiểm soát kỹ thuật).
* Các chính sách 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
* Chính sách có thể là một trong số rất ít các biện pháp kiểm soát hoặc biện pháp bảo vệ bảo vệ một số thông tin nhất định

***Phân loại chính sách ATTT:***

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.

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

***Khái niệm:*** Chính sách là một tuyên bố về quan điểm của tổ chức nhằm tác động và xác định các quyết định và hành động, và được sử dụng để kiểm soát hành động của mọi người và sự phát triển của các thủ tục. không chỉ là một công cụ quản lý để đáp ứng các yêu cầu pháp lý. Để bảo vệ tổ chức và công việc của nhân viên. Có thể được xem như một tập hợp các quy tắc quy định hành vi được chấp nhận và không được chấp nhận trong một tổ chức.

***Thủ tục:*** Hướng dẫn từng bước được thiết kế để hỗ trợ nhân viên tuân theo các chính sách, tiêu chuẩn và 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.

# 11. 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 tạo và quản lý ISSP phổ biến nhất:***

* Tạo một số tài liệu ISSP, mỗi tài liệu phù hợp với một vấn đề cụ thể.
* Tạo một tài liệu ISSP toàn diện duy nhất bao gồm tất cả các vấn đề.
* 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.

***Đối với các tổ chức có quy mô nhỏ***, cách tiếp cận tạo một số tài liệu ISSP riêng lẻ thường được ưa chuộng hơn cả. Lý do là vì:

* *Tính linh hoạt cao:* Các tổ chức nhỏ có thể không cần đến một hệ thống chính sách phức tạp và toàn diện. Việc tạo ra các tài liệu riêng lẻ cho phép họ tập trung vào những vấn đề cụ thể và quan trọng nhất đối với họ.
* *Dễ dàng cập nhật:* Khi có thay đổi hoặc cần bổ sung, việc chỉnh sửa một tài liệu nhỏ sẽ dễ dàng hơn là phải cập nhật một tài liệu toàn diện lớn.
* *Tiết kiệm chi phí:* Việc phát triển và duy trì một tài liệu ISSP toàn diện có thể đòi hỏi nhiều nguồn lực và chi phí, điều mà các tổ chức nhỏ có thể không sẵn lòng hoặc không có khả năng chi trả.

***Đối với các tổ chức lớn***, cách tiếp cận tạo một tài liệu ISSP toàn diện duy nhất hoặc tài liệu ISSP mô-đun thường phù hợp hơn. Lý do là:

* Tài liệu ISSP toàn diện duy nhất:
* *Tính nhất quán:* Một tài liệu toàn diện giúp đảm bảo rằng tất cả các phòng ban và nhân viên trong tổ chức đều tuân theo cùng một bộ quy tắc và hướng dẫn.
* *Dễ dàng truyền đạt:* Việc có một tài liệu duy nhất giúp việc truyền đạt chính sách đến toàn bộ nhân viên trở nên dễ dàng và thống nhất hơn.
* *Quản lý rủi ro tốt hơn:* Một tài liệu toàn diện cho phép tổ chức có cái nhìn tổng quan về mọi khía cạnh của an ninh thông tin, từ đó giúp quản lý rủi ro một cách hiệu quả.
* Tài liệu ISSP mô-đun:
* *Tính linh hoạt:* Các tài liệu mô-đun cho phép tổ chức cập nhật hoặc thay đổi chính sách cho từng khía cạnh cụ thể mà không ảnh hưởng đến toàn bộ hệ thống.
* *Dễ dàng mở rộng:* Khi tổ chức phát triển, việc thêm chính sách mới hoặc điều chỉnh các chính sách hiện có trở nên dễ dàng hơn với cấu trúc mô-đun.
* *Phù hợp với các tổ chức đa dạng:* Đối với các tổ chức có nhiều phòng ban hoặc đơn vị kinh doanh khác nhau, tài liệu mô-đun giúp quản lý chính sách một cách hiệu quả, phản ánh đúng nhu cầu và yêu cầu của từng đơn vị.

# 12. 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.

# 13. 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).

***Các nguyên tắc phát triển chính sách và chuẩn:***

***1. 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

2. Nhận thức

3. Đạo đức

4. Đa ngành, đa lĩnh vực

5. Tỉ lệ (Proportionality)

6. Tích hợp

***7. 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.

8. Kịp thời

***9. 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.

10. Dân chủ

11. Kiểm soát nội bộ

12. Đối thủ (Adversary)

13. Đặc quyền tối thiểu

14. Phân chia nhiệm vụ

15. Tính liên tục

16. Tính đơn giản

17. AT lấy chính sách làm trung tâm

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

***Các thành phần trong khung mẫu chính sách ATTT:***

1. Mục đích

2. Tổng quan

3. Phạm vi

4. Chính sách

5. Vai trò và 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 chiếu.

***Khen thưởng và xử phạt, chúng không phải là thành phần cố định trong mọi khung mẫu chính sách ATTT là vì:***

* *Tập trung vào quy định:* Chính sách ATTT thường tập trung vào việc thiết lập các quy định và thủ tục an toàn thông tin, trong khi khen thưởng và xử phạt có thể được xem xét trong một khung pháp lý hoặc quy chế nội bộ riêng biệt.
* *Pháp lý và quản lý nhân sự:* Các vấn đề liên quan đến khen thưởng và xử phạt thường thuộc về phạm vi quản lý nhân sự và pháp lý, có thể được quy định trong các tài liệu khác như quy chế làm việc, quy định nội bộ hoặc hợp đồng lao động.
* *Linh hoạt trong ứng phó:* Việc không đưa khen thưởng và xử phạt vào chính sách ATTT cũng giúp tổ chức linh hoạt hơn trong việc ứng phó với các tình huống cụ thể, cho phép áp dụng các biện pháp phù hợp với từng trường hợp cụ thể.

# 15. 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.

***Khái niệm:*** Quản lí 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. Bao gồm: đánh giá, xử lý và chấp nhận rủi ro.

***Vai trò:***

*Quản lý cấp cao:* Là người chịu trách nhiệm cuối cùng trong việc hoàn thành nhiệm vụ của tổ chức.

*Giám đốc thông tin:* Chịu trách nhiệm về việc lập kế hoạch hoạt động cho hệ thống CNTT của tổ chức.

*Chủ sở hữu thông tin:* Đảm bảo rằng các biện pháp kiểm soát thích hợp được áp dụng để đảm bảo tính toàn vẹn, tính bảo mật và tính khả dụng của hệ thống và thông tin.

*Giám đốc kinh doanh:* Chịu trách nhiệm về hoạt động kinh doanh và quy trình mua công nghệ

*Cán bộ bảo mật hệ thống thông tin*: Người quản lý và có trách nhiệm với chương trình ATTT.

*Chuyên gia về bảo mật thông tin:* Cần hiểu rõ quá trình quản lý rủi ro và phát triển tài liệu hướng dẫn cho người dùng cuối của hệ thống.

***Truyền thông và tư vấn rủi ro, cũng như giám sát và soát xét rủi ro, cần thực hiện song song và xuyên suốt quá trình vì:***

*Tăng cường sự chuẩn bị*: Giúp tổ chức sẵn sàng ứng phó với rủi ro khi chúng xảy ra.

*Đảm bảo mục tiêu:* Đảm bảo rằng dự án tiến hành thuận lợi và đạt được mục tiêu đề ra.

*Tạo động lực và đồng thuận:* Giúp tăng động lực và sự đồng thuận cho các thành viên trong tổ chức.

*Liên tục cập nhật:* Rủi ro có thể thay đổi theo thời gian, do đó cần có sự giám sát và soát xét liên tục để phản ứng kịp thời

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

***Cần tiến hành khảo sát và phân tích rủi ro vì để:***

* Đánh giá các hậu quả để xác định mức ảnh hưởng đối với cơ quan, tổ chức khi tài sản bị khai thác điểm yếu gây ra các mối nguy.
* Đánh giá khả năng xảy ra đối với từng loại sự cố.

=> Xác định được các hậu quả, mức ảnh hưởng mà cơ quan, tổ chức phải xử lý

***Thời gian Khảo sát và phân tích rủi ro nên được tiến hành:***

* *Trước khi bắt đầu dự án:* Để lập kế hoạch và chuẩn bị cho các rủi ro có thể xảy ra.
* *Định kỳ trong quá trình thực hiện dự án:* Để cập nhật và điều chỉnh kế hoạch quản lý rủi ro theo tình hình thực tế

***Các phương pháp:***

* *Định tính:* xác định hệ quả, xác suất và mức rủi ro bằng các mức như “cao”, “trung bình” và “thấp”, có thể kết hợp hệ quả và xác suất, và đánh giá mức 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.

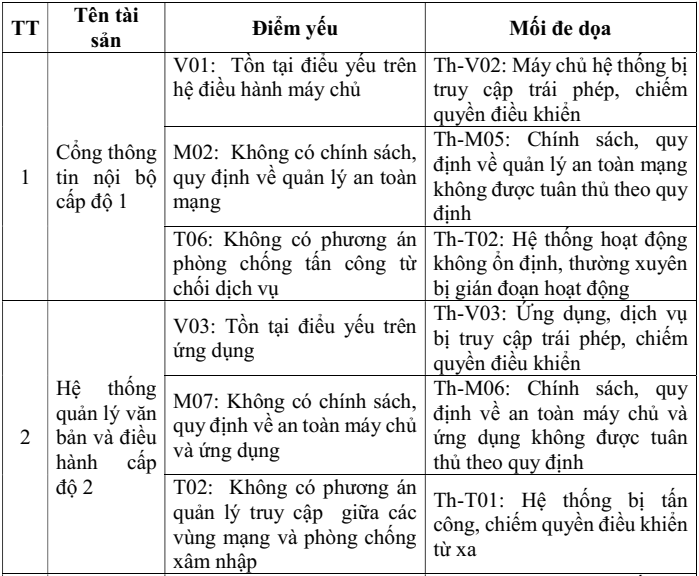
# 17. Mục đích của giai đoạn nhận diện rủi ro là gì; Nêu các phương pháp nhận diện rủi ro; Cho ví dụ minh họa về phương pháp thiết lập bảng kê trong nhận diện rủi ro.

***Mục đích của giai đoạn nhận diện rủi ro là***

* *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.

=> Danh mục các mối đe dọa và điểm yếu đối với các tài sản được xác định.

***Ví dụ:***



# 18. 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:*** Là quá trình đánh giá rủi ro như những đe dọa và cơ hội tiềm năng.

* 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.

***Mục đích của ước lượng rủi ro:***

* Xác suất rủi ro: Cho chúng ta 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

=> Đưa ra các quyết định phù hợp

***Các phương pháp giúp xác định ước lượng rủi ro.***

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

Sau khi xác định ước lượng rủi ro cho từng tài sản, tổ chức cần kiểm soát và hạn chế rủi ro:

*Thay đổi rủi ro*

* Là phương án thực hiện các biện pháp xử lý, khắc phục nhằm giảm mức rủi ro đã được xác định nhằm xác định các rủi ro tồn đọng được đánh giá lại ở mức chấp nhận được.
* cần xây dựng một hệ thống các biện pháp kiểm soát phù hợp. Các biện pháp được lựa chọn căn cứ vào các tiêu chí liên quan đến chi phí, đầu tư và thời gian triển khai, trên cơ sở cân đối giữa nguồn lực bỏ ra và lợi ích đem lại đối với tổ chức khi thực hiện xử lý rủi ro đó.

*Duy trì rủi ro:* là phương án chấp nhận rủi ro đã xác định mà không đưa ra các phương án xử lý để giảm thiểu rủi ro. Việc xác định rủi ro nào có thể được chấp nhận dựa vào mức rủi ro và tiêu chí chấp nhận rủi ro.

*Tránh rủi ro*

* là phương án xử lý khi phải đối mặt với mức rủi ro quá cao bằng cách làm thay đổi, loại bỏ hoặc dừng hoạt động của HT, quy trình nghiệp vụ hoặc hoạt động của cơ quan, tổ chức để không phải phải đối mặt với rủi ro đã xác định.
* Thích hợp khi rủi ro được xác định vượt quá khả năng chấp nhận rủi ro của tổ chức.

*Chia sẻ rủi ro*

* là phương án chuyển rủi ro, một phần rủi ro phải đối mặt cho cơ quan, tổ chức khác.
* thường được thực hiện khi xác định rằng việc giải quyết rủi ro yêu cầu chuyên môn hoặc nguồn lực được cung cấp tốt hơn bởi các tổ chức khác.

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

**COSO**

COSO xác định kiểm soát nội bộ là một quá trình, thực hiện bởi hội đồng quản trị bao gồm tất cả các thành viên trong tổ chức, được thiết kế để cung cấp "sự bảo đảm hợp lý" liên quan đến việc đạt được các ***mục tiêu***:

* Hiệu quả và hiệu quả hoạt động
* Độ tin cậy của báo cáo tài chính
* Tuân thủ pháp luật và các quy định hiện hành.

***Nguyên tắc:*** COSO dựa trên 17 nguyên tắc mở rộng theo mô hình kết cấu bởi 5 thành phần cấu thành kiểm soát nội bộ.

***5 thành phần liên quan:***

* + Môi trường kiểm soát
  + Đánh giá rủi ro
  + Các hoạt động kiểm soát
  + Thông tin và truyền thông
  + Giám sát

**COBIT 5**

***Mục tiêu của COBIT 5:***

* Đáp ứng nhu cầu của các bên liên quan.
* Tạo lập một framework thống nhất và toàn diện cho hoạt động kinh doanh của doanh nghiệp

***COBIT 5 sẽ vận hành dựa trên 5 nguyên tắc cốt lõi sau:***

* Đáp ứng nhu cầu của các bên liên quan (cổ đông, đối tác).
* Có một phạm vi bảo hiểm toàn diện cho tổ chức, doanh nghiệp.
* Tạo lập một framework thống nhất tuyệt đối, duy nhất.
* Tạo lập một phương thức tiếp cận toàn diện hơn cho hoạt động kinh doanh của doanh nghiệp.
* Chỉ rõ sự khác biệt giữa quản lý (management) và quản trị (governance).

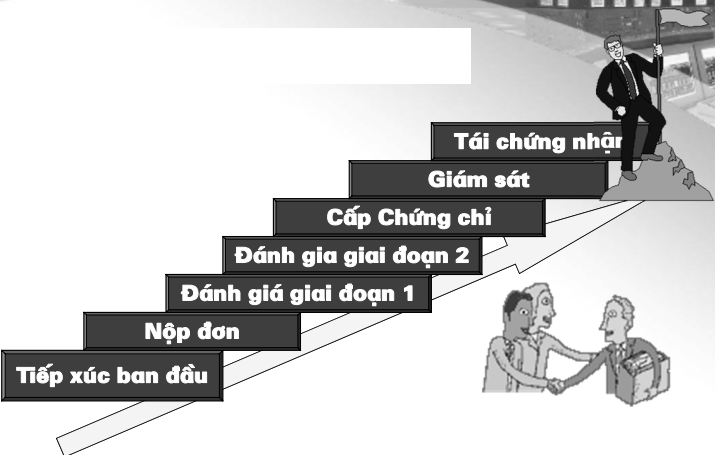
***COBIT 5 bao gồm 7 thành phần chính, các thành phần này là:***

* Principles (Nguyên tắc): Cung cấp các nguyên tắc cơ bản cho việc quản trị và quản lý IT.
* Enablers (Những yếu tố hỗ trợ): Bao gồm các nguồn lực và cấu trúc cần thiết để hỗ trợ việc áp dụng các nguyên tắc.
* Governance and Management Objectives (Mục tiêu quản trị và quản lý): Xác định các mục tiêu cụ thể cho việc quản trị và quản lý IT.
* Process Capability Model (Mô hình năng lực quy trình): Đánh giá và phát triển năng lực của các quy trình IT.
* Information Model (Mô hình thông tin): Quản lý thông tin dựa trên các yêu cầu và mục tiêu của tổ chức.
* Professional Guides (Hướng dẫn chuyên nghiệp): Cung cấp hướng dẫn chi tiết về việc áp dụng COBIT 5 trong thực tế.
* Other Guidance (Hướng dẫn khác): Bao gồm các công cụ, tài liệu và tài nguyên khác để hỗ trợ việc triển khai COBIT 5.

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

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

***Quá tình chứng nhận:***



***Các yếu tố quan trọng của việc áp dụng thành công chuẩn:***

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

# 23. 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 AT của tài nguyên và tài sản TT, cả con người và nhân tạo.

***CP được tạo thành từ bốn thành phần chính, mục đích của chúng là:***

* *Quy trình thu thập dữ liệu và tài liệu được gọi là phân tích tác động kinh doanh (Business impact analysis - BIA):* Xác định và đánh giá tác động của các sự kiện không lường trước được đối với hoạt động kinh doanh, từ đó xác định các tài nguyên quan trọng cần được bảo vệ ưu tiên.
* *Kế hoạch Ứng phó Sự cố (Incident response plan- IRP):* Thiết lập các quy trình để phát hiện, đánh giá và giải quyết các sự cố an ninh thông tin, giúp tổ chức nhanh chóng khôi phục hoạt động bình thường.
* *Kế hoạch khôi phục sau thảm họa (Disaster recovery plan - DRP):* Phát triển các chiến lược để khôi phục hệ thống và dịch vụ IT sau một sự kiện thảm họa, đảm bảo rằng dữ liệu quan trọng có thể được phục hồi và hoạt động kinh doanh có thể tiếp tục*.*
* *Kế hoạch liên tục kinh doanh (Business continuity plan - BCP):* Đảm bảo rằng các hoạt động kinh doanh thiết yếu có thể tiếp tục hoặc nhanh chóng được khôi phục trong trường hợp xảy ra sự cố hoặc thảm họa, giúp tổ chức duy trì hoạt động và giảm thiểu thiệt hại.

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

Có thể tạo và phát triển ba yếu tố lập kế hoạch của quá trình CP (kế hoạch IR, DR và ​​BC) như một kế hoạch thống nhất hoặc có thể tạo ba yếu tố riêng biệt kết hợp với một tập hợp các thủ tục lồng ghép với nhau để cho phép tính liên tục. Để đảm bảo tính liên tục trong quá trình tạo ra các thành phần CP, quy trình CP gồm 07 bước:

* 1. Xây dựng tuyên bố chính sách lập kế hoạch dự phòng.
  2. Tiến hành BIA.
  3. Xác định các biện pháp kiểm soát phòng ngừa.
  4. Tạo chiến lược dự phòng
  5. Xây dựng kế hoạch dự phòng
  6. Đảm bảo kế hoạch kiểm tra, đào tạo và bài tập
  7. Đảm bảo duy trì kế hoạch.

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

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

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

* + Thông báo của Nhân sự Chủ chốt: Có hai cách để kích hoạt danh sách cảnh báo: tuần tự và phân cấp (có sẵn nhiều HT tự động tạo điều kiện thuận lợi cho cả hai cách tiếp cận)
  + Ghi lại sự cố: phải ghi lại ai, cái gì, khi nào, ở đâu, tại sao và cách thức của từng hành động được thực hiện trong khi sự cố đang xảy ra.
  + Các chiến lược ngăn chặn sự cố:
    - Vô hiệu hóa tài khoản người dùng bị xâm phạm
    - Cấu hình lại tường lửa để chặn lưu lượng sự cố
    - Tạm thời vô hiệu hóa quy trình hoặc dịch vụ bị xâm phạm
    - Gỡ bỏ ứng dụng ống dẫn hoặc máy chủ - ví dụ: máy chủ e-mail
    - Ngắt kết nối mạng hoặc phân đoạn mạng bị ảnh hưởng
    - Dừng (tắt nguồn) tất cả các máy tính và thiết bị mạng
  + Báo cáo sự cố: trong quá trình BIA, phải xác định thời điểm một sự cố được coi là một thảm họa. Các tiêu chí này phải được bao gồm trong IRP. Tổ chức cũng phải lập thành văn bản khi nào cần sự tham gia của những người phản ứng bên ngoài

# 27. 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.

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

**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**
* Tên chính sách và thông tin định danh
  + **Chính sách bàn làm việc sạch sẽ**

1. **Mục đích:** chỉ ra mục đích của CS

Mục đích của CS này là để thiết lập các yêu cầu tối thiểu cho việc duy trì “bàn làm việc sạch sẽ” – nơi mà thông tin nhạy cảm/quan trọng về các nhân viên, sở hữu trí tuệ, khách hàng và nhà cung cấp AT, cất vào chỗ được khóa và thoát khỏi trang Web. CS bàn làm việc sạch sẽ tuân thủ cả ISO 27001/17700 lẫn các biện pháp kiểm soát riêng tư cơ bản.

1. **Tổng quan:** giới thiệu tổng quan về CS

CS bàn làm việc sạch sẽ có thể là một công cụ để đảm bảo các dữ liệu nhạy cảm/bí mật phải được người dùng loại bỏ khỏi chỗ làm việc và được khóa khi không sử dụng hoặc khi nhân viên rời khỏi chỗ làm. Đây là một trong những chiến lược hàng đầu được áp dụng để hạn chế rủi ro từ những vi phạm AT ở nơi làm việc. Một CS như vậy cũng có thể nâng cao nhận thức của nhân viên về việc bảo vệ thông tin nhạy cảm.

1. **Phạm vi:** phạm vi áp dụng của CS

CS này áp dụng cho tất cả các nhân viên và các chi nhánh của công ty X

1. **Chính sách:** liệt kê ra các nội dung CS
   * Phải khóa các máy tính khi không sử dụng
   * Hết ngày làm việc phải tắt hoàn toàn các máy tính
   * Tủ tài liệu chứa thông tin nhạy cảm hoặc thông tin không được phổ biến rộng phải được đóng và khóa khi không sử dụng hoặc khi không có mặt ở đó
2. **Vai trò và trách nhiệm:**

Liệt kê các thực thể và trách nhiệm liên quan tới việc thực thi CS

1. **Luật/Hướng dẫn áp dụng:**

Liệt kê các luật hoặc hướng dẫn mà CS có liên quan tới

1. **Tính hiệu lực**

Thông tin về thời gian thi hành và thời hạn điều chỉnh/xóa bỏ

1. **Thông tin và hỗ trợ:**

Chỉ ra nơi có thể liên hệ để biết thêm thông tin về CS

1. **Phê chuẩn:**

Đưa ra người và ngày phê chuẩn

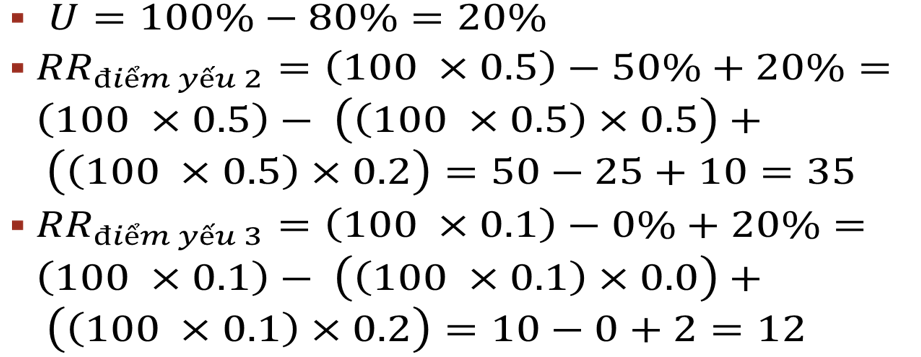
1. **Tài liệu tham chiếu**

Chỉ ra tài liệu bổ sung cho CS

* + 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.

Tính mức độ rủi ro cho các điểm yếu của tài sản: Tài sản B có giá trị là 100 và có hai điểm yếu (điểm yếu 2 và 3). Điểm yếu 2 có khả năng xuất hiện là 0.5 và hiện tại có một sự kiểm soát với mức độ đạt được là 50% rủi ro của nó. Điểm yếu 3 có khả năng xuất hiện là 0.1 và chưa có sự kiểm soát nào. Ước lượng các giả thiết và dữ liệu chính xác 80%



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