Quizizz bảng tính

Tên

ATBMHTTT_PTIT_Chương 5 (Chính sách& Pháp Luật ATTT)

Lớp học

Tổng số câu hỏi: 55

Thời gian làm bài: 33phút

Ngày

Tên người hướng dẫn: Ngọ Văn Trọng

1. Quản lý an toàn thông tin (Information security management) là một tiến trình (process) nhằm ... các tài sản quan trọng của cơ quan, tổ chức, doanh nghiệp được bảo vệ ... với ...

a) Bảo vệ / Đầy đủ / Chi phí rẻ

b) Đảm bảo / Đầy đủ / Chi phí phù hợp

c) Bảo vệ / Toàn diện / Chi phí phù hợp

d) Đảm bảo / Toàn diện / Chi phí rẻ

2. Quá trình quản lý ATTT cần được thực hiện liên tục theo chu trình do

a) Sự thay đổi nhanh chóng của công nghệ

b) Môi trường xuất hiện các mối đe dọa mới

c) Môi trường xuất hiện rủi ro liên tục thay đổi

d) Sự thay đổi nhanh chóng của môi trường trong và ngoài

3. Tài sản ATTT có thể gồm:

a) Thông tin

b) Phần cứng

c) Phần mềm

d) Cơ sở dữ liệu

e) Hệ thống CNTT

4. Các phương pháp tiếp cận đánh giá rủi ro :

a) Phân tích chi tiết rủi ro

b) Kết hợp

c) Đường cơ sở

d) Tổng hợp

e) Không chính thức

5. Mục đích của Phương pháp đường cơ sở là thực thi các kiểm soát an ninh ở mức cơ bản dựa trên:

a) Các tài liệu cơ bản
b) Các quy tắc thực hành
c) Các hướng dẫn có sẵn
d) Các thực tế tốt nhất của ngành đã được áp dụng
e) Kinh nghiệm từ những người giỏi trong ngành

6. Quản lý ATTT có thể gồm các khâu:

a) Xây dựng hồ sơ tổng hợp về các rủi ro
b) Đánh giá rủi ro với từng tài sản ATTT cần bảo vệ
c) Xác định và triển khai các biện pháp quản lý, kỹ thuật kiểm soát, giảm rủi ro về mức chấp nhận được
d) Xác định rõ mục đích đảm bảo ATTT

7. Trên cơ sở xác định mức rủi ro, có thể đề ra các biện pháp xử lý, kiểm soát rủi ro trong mức ... , với mức chi phí ...

a) Chấp nhận được / Phù hợp
b) Tối đa / Rẻ nhất
c) Hiệu quả / Tốt nhất

8. Ưu điểm của phương pháp đường cơ sở :

a) Không xem xét kỹ đến các điều kiện nảy sinh các rủi ro ở các hệ thống của các tổ chức khác nhau
b) Không đòi hỏi các chi phí cho các tài nguyên bổ sung sử dụng trong đánh giá rủi ro chính thức
c) Mức đường cơ sở được xác định chung nên có thể không phù hợp với từng tổ chức cụ thể
d) Cùng nhóm các biện pháp có thể triển khai trên nhiều hệ thống

9. Nhược điểm của phương pháp đường cơ sở :

a) Không xem xét kỹ đến các điều kiện nảy sinh các rủi ro ở các hệ thống của các tổ chức khác nhau
b) Mức đường cơ sở được xác định chung nên có thể không phù hợp với từng tổ chức cụ thể
c) Cùng nhóm các biện pháp có thể triển khai trên nhiều hệ thống
d) Không đòi hỏi các chi phí cho các tài nguyên bổ sung sử dụng trong đánh giá rủi ro chính thức

10. Phương pháp không chính thức liên quan đến việc:

a) Đánh giá toàn diện các rủi ro đối với tất cả các tài sản CNTT của tổ chức

b) Sử dụng kiến thức chuyên gia của các nhân viên bên trong tổ chức, hoặc các nhà tư vấn từ bên ngoài

c) Thực hiện một số dạng phân tích rủi ro hệ thống CNTT của tổ chức một cách không chính thức

d) Không thực hiện đánh giá toàn diện các rủi ro đối với tất cả các tài sản CNTT của tổ chức

11. Ưu điểm của phương pháp không chính thức

a) Kết quả đánh giá dễ phục thuộc vào quan điểm của các cá nhân

b) Không đòi hỏi các nhân viên phân tích rủi ro có các kỹ năng bổ sung, nên có thể thực hiện nhanh với chi phí thấp

c) Việc có phân tích hệ thống CNTT của tổ chức giúp cho việc đánh giá rủi ro, lỗ hổng chính xác hơn và các biện pháp kiểm soát đưa ra cũng phù hợp hơn phương pháp đường cơ sở

d) Do đánh giá rủi ro không được thực hiện toàn diện nên có thể một rủi ro không được xem xét kỹ, nên có thể để lại nguy cơ cao cho tổ chức

12. Nhược điểm của phương pháp không chính thức

a) Kết quả đánh giá dễ phục thuộc vào quan điểm của các cá nhân

b) Không đòi hỏi các nhân viên phân tích rủi ro có các kỹ năng bổ sung, nên có thể thực hiện nhanh với chi phí thấp

c) Do đánh giá rủi ro không được thực hiện toàn diện nên có thể một rủi ro không được xem xét kỹ, nên có thể để lại nguy cơ cao cho tổ chức

d) Việc có phân tích hệ thống CNTT của tổ chức giúp cho việc đánh giá rủi ro, lỗ hổng chính xác hơn và các biện pháp kiểm soát đưa ra cũng phù hợp hơn phương pháp đường cơ sở

13. Phương pháp phân tích chi tiết rủi ro là phương pháp đánh giá ..., được thực hiện một cách ... và được chia thành nhiều giai đoạn

a) Chi tiết / Hiệu quả

b) Toàn diện / Chính thức

c) Hiệu quả / Cơ bản

14. Phương pháp phân tích chi tiết rủi ro bao gồm các bước

a) Lựa chọn các biện pháp xử lý rủi ro dựa trên kết quả đánh giá rủi ro của các giai đoạn trên

b) Nhận dạng các tài sản và các mối đe dọa và lổ hổng đối với các tài sản này

c) Xác định xác suất xuất hiện các rủi ro và các hậu quả có thể có nếu rủi ro xảy ra với tổ chức

15. Ưu điểm của phương pháp phân tích chi tiết rủi ro

a) Cung cấp thông tin tốt nhất cho việc tiếp tục quản lý vấn đề an ninh của các hệ thống CNTT khi chúng được nâng cấp, sửa đổi

b) Cho phép xem xét chi tiết các rủi ro đối với hệ thống CNTT của tổ chức, và lý giải rõ ràng các chi phí cho các biện pháp kiểm soát rủi do đề xuất

c) Có thể dẫn đến chậm trễ trong việc đưa ra các biện pháp xử lý, kiểm soát rủi ro phù hợp

d) Chi phí lớn về thời gian, các nguồn lực và yêu cầu kiến thức chuyên gia trình độ cao

16. Nhược điểm của phương pháp phân tích chi tiết rủi ro

a) Có thể dẫn đến chậm trễ trong việc đưa ra các biện pháp xử lý, kiểm soát rủi ro phù hợp

b) Cho phép xem xét chi tiết các rủi ro đối với hệ thống CNTT của tổ chức, và lý giải rõ ràng các chi phí cho các biện pháp kiểm soát rủi do đề xuất

c) Cung cấp thông tin tốt nhất cho việc tiếp tục quản lý vấn đề an ninh của các hệ thống CNTT khi chúng được nâng cấp, sửa đổi

d) Chi phí lớn về thời gian, các nguồn lực và yêu cầu kiến thức chuyên gia trình độ cao

17. Mục tiêu của phương pháp kết hợp

a) Cung cấp mức bảo vệ hợp lý chính xác nhất có thể , Sau đó điều chỉnh các biện pháp bảo vệ trên các hệ thống chính theo thời gian

b) Cung cấp mức bảo vệ hợp lý ngay hiện tại , Sau đó kiểm tra các biện pháp bảo vệ trên các hệ thống chính theo thời gian

c) Cung cấp mức bảo vệ hợp lý càng nhanh càng tốt , Sau đó kiểm tra và điều chỉnh các biện pháp bảo vệ trên các hệ thống chính theo thời gian

18. Ưu điểm của phương pháp kết hợp

a) Nếu đánh giá ở mức cao trong giai đoạn đầu không chính xác có thể dẫn đến áp dụng các biện pháp kiểm soát không phù hợp, hệ thống có thể gặp rủi ro trong thời gian chờ đánh giá chi tiết

b) Việc bắt đầu bằng việc đánh giá rủi ro ở mức cao dễ nhận được sự ủng hộ của cấp quản lý, thuận lợi cho việc lập kế hoạch quản lý ATTT

c) Có thể giúp giảm chi phí với đa số các tổ chức

d) Giúp sớm triển khai các biện pháp xử lý và kiểm soát rủi ro ngay từ giai đoạn đầu

19. Nhược điểm của phương pháp kết hợp

a) Nếu đánh giá ở mức cao trong giai đoạn đầu không chính xác có thể dẫn đến áp dụng các biện pháp kiểm soát không phù hợp, hệ thống có thể gặp rủi ro trong thời gian chờ đánh giá chi tiết

b) Việc bắt đầu bằng việc đánh giá rủi ro ở mức cao dễ nhận được sự ủng hộ của cấp quản lý, thuận lợi cho việc lập kế hoạch quản lý ATTT

c) Giúp sớm triển khai các biện pháp xử lý và kiểm soát rủi ro ngay từ giai đoạn đầu

d) Có thể giúp giảm chi phí với đa số các tổ chức

20. Bộ chuẩn ISO ..... là bộ chuẩn về quản lý ATTT (Information Technology - Code of Practice for Information Security Management) được tham chiếu rộng rãi nhất

a) 27002

b) 27000

c) 27001

d) 17799

21. Năm 2007, ISO ..... được đổi tên thành ISO 27002 song hành với ISO 27001

a) 17799:2004

b) 17799:2005

c) 17799:2006

d) 17788:2005

22. Bộ chuẩn ISO/IEC .... (được soạn thảo năm 2000 bởi International Organization for Standardization (ISO) và International Electrotechnical Commission (IEC)) là tiền thân của ISO 27000

a) 17770

b) 17798

c) 17788

d) 17799

23. ISO/IEC 27002 gồm ... điều

a) 127
b) 130
c) 128
d) 126

24. ISO/IEC 27002 đề ra các khuyến nghị về quản lý ATTT cho những người thực hiện việc ... trong tổ chức của họ

a) Khởi tạo, thực hiện và duy trì an ninh an toàn
b) Thiết lập hệ thống và đảm bảo an ninh an toàn
c) Thiết lập và duy trì an ninh an toàn

25. ISO 27001 cung cấp các thông tin để ...

a) Cài đặt một hệ thống quản lý an toàn thông tin
b) Thực thi các yêu cầu của ISO/IEC 27002
c) Thực thi các yêu cầu của ISO/IEC 27000
d) Cài đặt một hệ thống quản lý an toàn hệ thống

26. ISO 27001 cung cấp các thông tin để thực hiện việc quản lý ATTT, nhưng :

a) Cách thức thực hiện sơ sài
b) Nó chỉ tập trung vào các phần việc phải thực hiện
c) Không chỉ rõ cách thức thực hiện
d) Nó tập trung vào các phần việc phải thực hiện ngay

27. ISO/IEC 27001:2005 bao gồm mấy phần

a) 5
b) 4
c) 3
d) 2

28. Plan-Do-Check-Act -> Plan

a) Đề ra phạm vi , chính sách của ISMS và hướng tiếp cận đánh giá rủi ro
b) Nhận dạng , đánh giá rủi ro
c) Nhận dạng , đánh giá rủi ro và các phương pháp xử lý rủi ro
d) Chuẩn bị tuyên bố / báo cáo áp dụng
e) Lựa chọn các mục tiêu kiểm soát và biện pháp kiểm soát

29. Plan-Do-Check-Act -> Do:

a) Thực thi các chương trình đạo tạo chuyên môn và giáo dục ý thức
b) Xây dụng và thực thi kế hoạch rủi ro
c) Thực thi các kiểm soát và các chương trình đạo tạo chuyên môn và giáo dục ý thức
d) Quản lý các hoạt động và tài nguyên
e) Thực thi các thủ tục phát hiện và phản ứng lại các sự cố an ninh

30. Plan-Do-Check-Act -> Check:

a) Ghi lại các hành động và sự kiện ảnh hưởng đến ISMS
b) Thực thi các thủ tục giám sát và việc đánh giá thường xuyên tính hiệu quả của ISMS
c) Thực thi việc đánh giá thường xuyên với ISMS bởi bộ phận quản lý
d) Thực thi việc đánh giá thường xuyên với ISMS bởi bộ phận công nhân
e) Thực hiện việc kiểm toán (audit) nội bộ với ISMS

31. Plan-Do-Check-Act -> Act

a) Áp dụng các bài đã được học và Thảo luận kết quả với các bên quan tâm
b) Thực hiện các cải tiến đã được nhận dạng và ngăn chặn
c) Thực hiện các cải tiến đã được nhận dạng , các hành động sửa chữa và ngăn chặn
d) Đảm bảo các cải tiến đạt được các mục tiêu

32. Các nhân viên đảm bảo an toàn cho thông tin phải hiểu rõ những khía cạnh pháp lý và đạo đức ATTT :

a) Đôi khi thực hiện công việc nằm ngoài khuôn khổ cho phép của luật pháp
b) Luôn nắm vững môi trường pháp lý hiện tại và các luật và các quy định luật pháp
c) Luôn thực hiện công việc nằm trong khuôn khổ cho phép của luật pháp

33. DMCA là viết tắt của luật gì

a) Digital Millennium Copyright Act
b) Digital Millennia Copyright Act
c) Digital Minor Copyright Act
d) Digital Multiple Copyright Act

34. Luật: Gồm những điều khoản ... và Các điều luật thường được xây dựng từ ....

a) Bắt buộc hoặc cấm những hành vi cục bộ / Các vấn đề hình sự
b) Bắt buộc hoặc cấm những hành vi không tốt / Các vấn đề kinh tế và chính trị
c) Bắt buộc hoặc cấm những hành vi cụ thể / Các vấn đề đạo đức

35. Đạo đức: Định nghĩa những hành vi xã hội ...

a) có thể chấp nhận được
b) chấp nhận được
c) không chấp nhận được

36. Đạo đức thường dựa trên .... Do đó hành vi đạo đức giữa các dân tộc, các nhóm người khác nhau là ...

a) các đặc điểm tự nhiên / khác nhau
b) các đặc điểm tự nhiên / giống nhau
c) các đặc điểm xã hôi / giống nhau
d) các đặc điểm văn hóa / khác nhau

37. Khác biệt giữa luật và đạo đức :

a) Luật được thực thi bởi các cơ quan chính quyền còn đạo đức thì được thực thi nghiêm khắc hơn
b) Luật được thực thi bởi các cơ quan chính quyền còn đạo đức thì không
c) Luật được thực thi bởi các cơ quan chính quyền còn đạo đức thì được thực thi bởi gia đình

38. Luật ATTT mạng của Việt Nam được Quốc hội thông qua vào tháng ... (86/2015/QH13) và có hiệu lực từ ...

a) tháng 11.2015 / 1/7/2016:
b) tháng 6.2015 / 1/1/2016:
c) tháng 11.2015 / 1/1/2016:
d) tháng 6.2015 / 1/7/2016:

39. Luật ATTT mạng gồm ... chương với ... điều

a) 7 / 54
b) 8 / 56
c) 7 /60
d) 8 / 54

40. Luật An ninh mạng của Việt Nam được Quốc hội thông qua vào tháng ... và có hiệu lực từ 1/1/2019

a) 8/2018
b) 6/2018
c) 11/2018
d) 10/2018

41. Trách nhiệm của tổ chức :

a) Là trách nhiệm trước luật pháp của tổ chức đó
b) Là trách nhiệm trước luật pháp của tổ chức đó được mở rộng ngoài phạm vi luật hình sự và luật hợp đồng
c) Nếu một nhân viên của 1 công ty/tổ chức thực hiện hành vi phạm pháp hoặc phi đạo đức, gây thiệt hại cho cá nhân, tổ chức khác, thì công ty/tổ chức đó phải chịu trách nhiệm về pháp lý, tài chính
d) Gồm cả trách nhiệm pháp lý phải hoàn trả và đền bù cho những hành vi sai trái

42. Khác biệt giữa chính sách và luật :

a) Luật luôn bắt buộc / Chính sách: thiếu hiểu biết chính sách là 1 cách bào chữa không thể chấp nhận được
b) Luật luôn bắt buộc / Chính sách: thiếu hiểu biết chính sách là 1 cách bào chữa chấp nhận được
c) Luật không luôn luôn bắt buộc / Chính sách: thiếu hiểu biết chính sách là 1 cách bào chữa không thể chấp nhận được

43. Các yêu cầu của chính sách gồm .. điều và bao gồm : ...

a) 6 / Phổ biến , Xem xét , Có thể hiểu , Tuân thủ , Áp dụng đồng đều (Bình đẳng) , Nghiên cứu Kỹ
b) 3 / Xem xét , Có thể hiểu , Tuân thủ
c) 5 / Phổ biến , Xem xét , Có thể hiểu , Tuân thủ , Áp dụng đồng đều (Bình đẳng)
d) 4 / Xem xét , Có thể hiểu , Tuân thủ , Áp dụng đồng đều (Bình đẳng)

44. Có ... kiểu luật và bao gồm :

a) 3 / Luật dân sự , Luật hình sự , Luật riêng
b) 4 / Luật dân sự , Luật hình sự , Luật công cộng , Luật riêng
c) 2 / Luật dân sự , Luật hình sự

45. Các luật ATTT của Mỹ gồm ... Loại và bao gồm :

a) 5 / Các luật tội phạm máy tính , Các luật về sự riêng tư , Luật xuất khẩu và chống gián điệp , Luật bản quyền , Luật tự do thông tin

b) 4 / Các luật tội phạm máy tính , Các luật về sự riêng tư , Luật xuất khẩu và chống gián điệp , Luật bản quyền

c) 3 / Các luật tội phạm máy tính , Các luật về sự riêng tư , Luật xuất khẩu và chống gián điệp

46. Tài sản (Asset) trong lĩnh vực ATTT là

a) Phần cứng, phần mềm

b) Bất cứ các thành phần hỗ trợ các hoạt động liên quan tới thông tin

c) Không có đáp án đúng

d) Thông tin, thiết bị

47. Quản lý an toàn thông tin (Information security management) là một tiến trình (process) nhằm đảm bảo các tài sản quan trọng của ... được bảo vệ đầy đủ với ... phù hợp

a) Cơ quan, tổ chức, doanh nghiệp / chi phí

b) Cơ quan, tổ chức, doanh nghiệp / mục đích

c) Cơ quan, tổ chức / mục đích

d) Cơ quan, doanh nghiệp / chính sách

48. Quản lý ATTT phải trả lời được 3 câu hỏi về

a) Tài sản, đe doạ có thể có, biện pháp ứng phó

b) Tài sản, tình trạng hiện thời, cách phòng ngừa

c) Thông tin nào, tình trạng nào, cách phòng ngừa

d) Thông tin nào, nguy hiểm nào, biện pháp nào

49. Khâu không nằm trong việc quản lý ATTT

a) Đánh giá tình trạng hiện thời các tài sản cần bảo vệ

b) Xác định và triển khai các biện pháp quản lý, kỹ thuật kiểm soát, giảm rủi ro về mức chấp nhận được.

c) Xây dựng hồ sơ tổng hợp về các rủi ro

d) Xác định rõ mục đích đảm bảo ATTT

50. Quá trình quản lý ATTT cần được thực hiện liên tục theo chu trình do

a) Bảo trì và tăng cường hiệu năng

b) Giám sát và xem xét ISMS

c) Cài đặt và vận hành ISMS

d) Xác lập tài liệu ISMS

51. Phương pháp tiếp cận không dùng để đánh giá rủi ro ATTT:

a) Kết hợp
b) Chinh thức
c) Đường cơ sở
d) Chi tiết

52. Các doanh nghiệp viễn thông nhà mạng thì phù hợp với phương pháp đánh giá rủi ro nào?

a) Đường cơ sở
b) Không chính thức
c) Phân tích chi tiết
d) Kết hợp

53. Điều nào sau đây không đúng về ISO 27001

a) Thực thi các yêu cầu của ISO/IEC 27002
b) Cung cấp các chi tiết cho thực hiện chu kỳ PDCA
c) Chỉ rõ cách thức thực hiện để thực hiện quản lý ATTT
d) Cung cấp các thông tin để cài đặt một hệ thống quản lý an toàn thông tin

54. Vai trò của nhân viên đảm bảo an toàn cho thông tin là rất quan trọng trong việc giảm thiểu rủi ro, đảm bảo an toàn cho ... và giảm thiệt hại nếu xảy ra sự cố

a) Hệ thống CNTT
b) Thiết bị , thông tin và các thành phần khác
c) Thông tin
d) Thông tin , hệ thống và mạng

55. Security and Freedom through Encryption Act, 1999 liên quan tới

a) Luật về sư riêng tư
b) Luật xuất khẩu và chống gián điệp
c) Luật về tội phạm máy tính
d) Luật bản quyền

Phím trả lời

1. b) Đảm bảo / Đầy đủ / Chi phí phù hợp

2. c) Môi trường xuất hiện rủi ro liên tục thay đổi , a) Sự thay đổi nhanh chóng của công nghệ

3. b) Phần cứng , c) Phần mềm , a) Thông tin

4. c) Đường cơ sở , e) Không chính thức , a) Phân tích chi tiết rủi ro , b) Kết hợp

5. d) Các thực tế tốt nhất của ngành đã được áp dụng , b) Các quy tắc thực hành , a) Các tài liệu cơ bản

6. d) Xác định rõ mục đích đảm bảo ATTT , a) Xây dựng hồ sơ tổng hợp về các rủi ro , b) Đánh giá rủi ro với từng tài sản ATTT cần bảo vệ , c) Xác định và triển khai các biện pháp quản lý, kỹ thuật kiểm soát, giảm rủi ro về mức chấp nhận được

7. a) Chấp nhận được / Phù hợp

8. b) Không đòi hỏi các chi phí cho các tài nguyên bổ sung sử dụng trong đánh giá rủi ro chính thức , d) Cùng nhóm các biện pháp có thể triển khai trên nhiều hệ thống

9. a) Không xem xét kỹ đến các điều kiện nảy sinh các rủi ro ở các hệ thống của các tổ chức khác nhau , b) Mức đường cơ sở được xác định chung nên có thể không phù hợp với từng tổ chức cụ thể

10. c) Thực hiện một số dạng phân tích rủi ro hệ thống CNTT của tổ chức một cách không chính thức , b) Sử dụng kiến thức chuyên gia của các nhân viên bên trong tổ chức, hoặc các nhà tư vấn từ bên ngoài , d) Không thực hiện đánh giá toàn diện các rủi ro đối với tất cả các tài sản CNTT của tổ chức

11. b) Không đòi hỏi các nhân viên phân tích rủi ro có các kỹ năng bổ sung, nên có thể thực hiện nhanh với chi phí thấp , c) Việc có phân tích hệ thống CNTT của tổ chức giúp cho việc đánh giá rủi ro, lỗ hổng chính xác hơn và các biện pháp kiểm soát đưa ra cũng phù hợp hơn phương pháp đường cơ sở

12. c) Do đánh giá rủi ro không được thực hiện toàn diện nên có thể một rủi ro không được xem xét kỹ, nên có thể để lại nguy cơ cao cho tổ chức , a) Kết quả đánh giá dễ phục thuộc vào quan điểm của các cá nhân

13. b) Toàn diện / Chính thức

14. b) Nhận dạng các tài sản và các mối đe dọa và lổ hổng đối với các tài sản này , c) Xác định xác suất xuất hiện các rủi ro và các hậu quả có thể có nếu rủi ro xảy ra với tổ chức , a) Lựa chọn các biện pháp xử lý rủi ro dựa trên kết quả đánh giá rủi ro của các giai đoạn trên

15. b) Cho phép xem xét chi tiết các rủi ro đối với hệ thống CNTT của tổ chức, và lý giải rõ ràng các chi phí cho các biện pháp kiểm soát rủi do đề xuất , a) Cung cấp thông tin tốt nhất cho việc tiếp tục quản lý vấn đề an ninh của các hệ thống CNTT khi chúng được nâng cấp, sửa đổi

16. d) Chi phí lớn về thời gian, các nguồn lực và yêu cầu kiến thức chuyên gia trình độ cao , a) Có thể dẫn đến chậm trễ trong việc đưa ra các biện pháp xử lý, kiểm soát rủi ro phù hợp

17. c) Cung cấp mức bảo vệ hợp lý càng nhanh càng tốt , Sau đó kiểm tra và điều chỉnh các biện pháp bảo vệ trên các hệ thống chính theo thời gian

18. b) Việc bắt đầu bằng việc đánh giá rủi ro ở mức cao dễ nhận được sự ủng hộ của cấp quản lý, thuận lợi cho việc lập kế hoạch quản lý ATTT , d) Giúp sớm triển khai các biện pháp xử lý và kiểm soát rủi ro ngay từ giai đoạn đầu , c) Có thể giúp giảm chi phí với đa số các tổ chức

19. a) Nếu đánh giá ở mức cao trong giai đoạn đầu không chính xác có thể dẫn đến áp dụng các biện pháp kiểm soát không phù hợp, hệ thống có thể gặp rủi ro trong thời gian chờ đánh giá chi tiết

20. b) 27000

21. b) 17799:2005

22. d) 17799

23. a) 127

24. a) Khởi tạo, thực hiện và duy trì an ninh an toàn

25. b) Thực thi các yêu cầu của , a) Cài đặt một hệ thống

26. c) Không chỉ rõ cách , b) Nó chỉ tập trung vào các phần

27. b) 4

ISO/IEC 27002 quản lý an toàn thông tin thức thực hiện việc phải thực hiện

28. a) Đề ra , phạm vi , chính sách của ISMS và hướng tiếp cận đánh giá rủi ro , c) Nhận dạng , đánh giá rủi ro và các phương pháp xử lý rủi ro , e) Lựa chọn các mục tiêu kiểm soát và biện pháp kiểm soát

29. d) Quản , bị tuyên bố / báo cáo , c) Thực thi các kiểm soát và các chương trình đạo tạo chuyên môn và giáo dục ý thức , b) Xây dựng và thực thi kế hoạch rủi ro

30. a) Thực hiện các hành động và sự kiện ảnh hưởng đến ISMS , e) Thực hiện việc kiểm toán (audit) nội bộ với ISMS , c) Thực thi việc đánh giá thường xuyên với ISMS bởi bộ phận quản lý , b) Thi thủ giá sát việ đá giá thu xuy tín hiệ qu của ISM

31. c) Thực hiện các cải tiến đã được nhận dạng , các hành động sửa chữa và ngăn chặn , a) Áp dụng các bài đã được học và Thảo luận kết quả với các bên quan tâm , d) Đảm bảo các cải tiến đạt được các mục tiêu

32. c) Luôn thực hiện công việc nằm trong khuôn khổ cho phép của luật pháp , b) Luôn nắm vững môi trường pháp lý hiện tại và các luật và các quy định luật pháp

33. a) Digital Millennium Copyright Act

34. c) Bắt buộc hoặc cấm những hành vi cụ thể / Các vấn đề đạo đức

35. b) chấp nhận được

36. d) các đặc điểm văn hóa / khác nhau

37. b) Luật được thực thi bởi các cơ quan chính quyền còn đạo đức thì không

38. a) tháng 11.2015 / 1/7/2016:

39. d) 8 / 54

40. b) 6/2018

41. b) Là trách nhiệm trước luật pháp của tổ chức đó được mở rộng ngoài phạm vi luật hình sự và luật hợp đồng , d) Gồm cả trách nhiệm pháp lý phải hoàn trả và đền bù cho những hành vi sai trái , c) Nếu một nhân viên của 1 công ty/tổ chức thực hiện hành vi phạm pháp hoặc phi đạo đức, gây thiệt hại cho cá nhân, tổ chức khác, thì công ty/tổ chức đó phải chịu trách nhiệm về pháp

42. b) Luật luôn bắt buộc / Chính sách: thiếu hiểu biết chính sách là 1 cách bào chữa chấp nhận được

lý, tài chính

43. c) 5 / Phổ biến , Xem xét , Có thể hiểu , Tuân thủ , Áp dụng đồng đều (Bình đẳng)

44. b) 4 / Luật dân sự , Luật hình sự , Luật công cộng , Luật riêng

45. a) 5 / Các luật tội phạm máy tính , Các luật về sự riêng tư , Luật xuất khẩu và chống gián điệp , Luật bản quyền , Luật tự do thông tin

46. c) Không có đáp án đúng

47. a) Cơ quan, tổ chức, doanh nghiệp / chi phí

48. a) Tài sản, đe doạ có thể có, biện pháp ứng phó

49. a) Đánh giá tình trạng hiện thời các tài sản cần bảo vệ

50. a) Bảo trì và tăng cường hiệu năng

51. b) Chinh thức

52. c) Phân tích chi tiết

53. c) Chỉ rõ cách thức thực hiện để thực hiện quản lý ATTT

54. d) Thông tin , hệ thống và mạng

55. b) Luật xuất khẩu và chống gián điệp