ATE Phá Tổn Thò	UIZIZZ bảng tính BMHTTT_PTIT_Chương 5 (Chính sách& ip Luật ATTT) g số câu hỏi: 55 ri gian làm bài: 33phút người hướng dẫn: Ngọ Văn Trọng	Tên Lớp học Ngày
1.	Quản lý an toàn thông tin (Information security các tài sản quan trọng của cơ quan, tổ chức, ca) Bảo vệ / Đầy đủ / Chi phí rẻ c) Bảo vệ / Toàn diện / Chi phí phù hợp	·
2.	Quá trình quản lý ATTT cần được thực hiện liên a) Sự thay đổi nhanh chóng của công nghệ c) Môi trường xuất hiện rủi ro liên tục thay đổi	
3.	Tài sản ATTT có thể gồm: a) Thông tin c) Phần mềm e) Hệ thống CNTT	b) Phần cứng d) Cơ sở dữ liệu
4.	Các phương pháp tiếp cận đánh giá rủi ro: a) Phân tích chi tiết rủi ro c) Đường cơ sở e) Không chính thức	b) Kết hợp d) Tổng hợp

- ATBMHTTT_PTIT_Chương 5 (Chính sách& Pháp Luật ATTT) | Quizizz Mục đích của Phương pháp đường cơ sở là thực thi các kiểm soát an ninh ở mức cơ bản dựa trên: b) Các quy tắc thực hành a) Các tài liêu cơ bản 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 vê c) Xác định và triển khai các biện pháp quản lý, d) Xác định rõ mục đích đảm bảo ATTT kỹ thuật kiểm soát, giảm rủi ro về mức chấp nhận được 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 b) Không đòi hỏi các chi phí cho các tài nguyên sinh các rủi ro ở các hệ thống của các tổ bổ sung sử dụng trong đánh giá rủi ro chính chức khác nhau thức c) Mức đường cơ sở được xác định chung nên d) Cùng nhóm các biện pháp có thể triển khai có thể không phù hợp với từng tổ chức cụ trên nhiều hệ thống thể
- 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
 - c) Cùng nhóm các biện pháp có thể triển khai trên nhiều hệ thống
- b) Mức đường cơ sở được xác định chung nên có thể không phù hợp với từng tổ chức cụ thể
- 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

- Phương pháp phân tích chi tiết rủi ro bao gồm các bước 14.
 - a) Lựa chọn các biện pháp xử lý rủi ro dựa trên kết quả đánh giá rủi ro của các giai đoan trên
 - 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
- b) Nhận dạng các tài sản và các mối đe dọa và lổ hổng đối với các tài sản này

- Ưu điểm của phương pháp phân tích chi tiết rủi ro 15.
 - 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
 - c) 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
- 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
 - 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
- 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
- d) Chi phí lớn về thời gian, các nguồn lực và yêu cầu kiến thức chuyên gia trình độ cao

- Mục tiêu của phương pháp kết hợp
 - a) Cung cấp mức bảo vệ hợp lý chính xác nhất b) Cung cấp mức bảo vệ hợp lý ngay hiện tại, có thể , Sau đó điều chỉnh 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
- Sau đó kiểm tra 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
 - ng phù quản lý, thuận lợi cho việc lập kế hoạch ng thời 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

b) Việc bắt đầu bằng việc đánh giá rủi ro ở

mức cao dễ nhận được sự ủng hộ của cấp

- 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 lợ tổ chức của họ	ý ATTT cho những người thực hiện việc tro	วทรู	
	a) Khởi tạo, thực hiện và duy trì an ninh an toàn	b) Thiết lập hệ thống và đảm bảo an ninh toàn	an	
	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 h thống	ıệ	
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 phả thực hiện 	i	
	c) Không chỉ rõ cách thức thực hiện	d) Nó tập trung vào các phần việc phải thư hiện ngay	'nc	
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 d) Quản lý các hoạt động và tài nguyên đạo tạo chuyên môn và giáo dục ý thức
- e) Thực thi các thủ tục phát hiện và phản ứng lai các sư cố an ninh

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

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

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
- các hành động sửa chữa và ngăn chặn
- c) Thực hiện các cải tiến đã được nhận dạng, d) Đảm bảo các cải tiến đạt được các mục tiêu
- 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

14/6/24	ATBMHTTT_PTIT_Chương 5 (Chính sách& Pháp Luật ATTT) Quizizz				
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 nhau là	đú	rc giữa các dân tộc, các nhóm người khác		
	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 thiệu lực từ	hôr	ng qua vào tháng (86/2015/QH13) và có		
	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		

d) 8/54

c) 7/60

- 40. Luât An ninh mang 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:
 - đó
 - a) Là trách nhiệm trước luật pháp của tổ chức 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

- Khác biệt giữa chính sách và luật: 42.
 - biết chính sách là 1 cách bào chữa không thể chấp nhận được
 - a) Luật luôn bắt buộc / Chính sách: thiếu hiểu 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
- Các yêu cầu của chính sách gồm .. điều và bao gồm : ... 43.
 - 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 b) 4 / 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
 - c) 3 / Các luật tội phạm máy tính , Các luật về sự riêng tư , Luật xuất khẩu và chống gián điệp
- sự riêng tư , Luật xuất khẩu và chống gián điệp, Luật bản quyền

- 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 vê
- 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 thiể 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,	199	9 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 2. c) Môi , Sự thay 3. b) Phần , Phần , Thông phí phù hợp trường a) đổi nhanh cứng c) mềm a) tin xuất hiện chóng của rủi ro liên công tục thay nghệ đổi
- 4. c) Đường, Không, Phân, 5xếd) Các thực, Các, Các 6. d) Xác , Xây , Đánh , Xác cơ sở e) chính a) tích b) hợp tế tốt b) quy a) tài định a) dựng b) giá c) định thức chi nhất của tắc hồ và liêu rõ růi tiết triển thưc ngành cσ muc sσ ro đã được růi khai hành bản đích tổng với đảm hợp các ro áp dụng từng bảo về tài biện **ATTT** các sản pháp rủi **ATTT** quản ro cần lý, kỹ bảo thuật vê kiểm soát, giảm růi ro về mức chấp nhận được
- 7. a) Chấp nhận được / Phù 8. b) Không đòi 9. a) Không , Mức , Cùng xem xét kỹ b) đường cơ hợp hỏi các chi d) nhóm phí cho các các biên đến các sở được tài nguyên pháp có điều kiện xác định bổ sung sử thể nảy sinh chung nên có triển các rủi ro dung trong đánh giá rủi khai ở các hê thể không ro chính trên thống của phù hợp thức nhiều các tổ với từng hệ chức khác tổ chức cụ thể thống nhau

- 10. c) Thưc , Sử , Không 1. b) Không , Việc có 12. c) Do đánh giá , Kết hiện b) dụng d) thực đòi hỏi c) phân tích rủi ro không a) quả môt kiến hiên các hê thống được thực đánh số thức CNTT của tổ đánh nhân hiện toàn giá dễ chuyên viên chức giúp diện nên có phục dạng giá phân gia của toàn phân cho viêc thể một rủi thuôc tích các diện tích rủi đánh giá rủi ro không vào được xem xét rủi ro nhân các ro có ro, lỗ hổng quan hệ viên rủi ro các kỹ chính xác kỹ, nên có điểm đối thể để lại của thống bên năng hơn và các CNTT bổ biện pháp các cá trong với tất nguy cơ cao của tổ tổ cả các kiểm soát cho tổ chức nhân sung, chức chức, tài nên có đưa ra cũng một hoặc sản thể phù hợp cách các **CNTT** thưc hơn không nhà tư của tổ hiên phương chính vấn từ chức pháp đường nhanh thức bên với chi cơ sở phí ngoài thấp
- 13. b) Toàn diên / Chính thức 14. b) Nhận , Xác , Lưa 15. b) Cho phép , Cung cấp dạng c) định a) chọn xem xét a) thông tin các các chi tiết các tốt nhất xác tài suất biện rủi ro đối cho việc sản xuất pháp với hệ tiếp tục và hiên xử lý thống quản lý các rủi ro CNTT của vấn đề các rủi ro tổ chức, mối dựa an ninh đe và trên và lý giải của các doa các kết rõ ràng hệ thống và lổ các chi phí CNTT khi hậu quả hổng đánh cho các quả chúng đối có giá biện pháp được với thể rủi ro kiểm soát nâng các có của rủi do đề cấp, sửa tài nếu xuất đổi các sản rủi ro giai này xảy đoạn ra với trên tổ chức

16.	d)	Chi phí	,	Có thể
		lớn về	a)	dẫn đến
		thời gian,		chậm trễ
		các		trong việc
		nguồn		đưa ra
		lực và		các biện
		yêu cầu		pháp xử
		kiến thức		lý, kiểm
		chuyên		soát rủi
		gia trình		ro phù
		độ cao		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
- , Giúp , Có 18. b) Viêc bắt d) sớm c) thể đầu triển giúp bằng khai giảm việc các chi đánh biên phí giá rủi pháp với ro ở xử lý đa mức và số cao dễ kiểm các nhân soát tổ đươc rủi chức sự ro

ủng ngay hô của từ cấp giai quản đoạn lý, đầu thuận

lơi cho việc lập kế hoạch quản lý **ATTT**

- 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
- 20. b) 27000

21. b) 17799:2005

- tiết
- 22. d) 17799
- 23. a) 127

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

- 25. b) Thực thi , Cài đặt các yêu a) một hệ cầu của thống
- 26. c) Không , Nó chỉ tập chỉ rõ b) trung vào cách các phần
- 27. b) 4

```
ISO/IEC
                   quản lý an
                                      thức
                                                  viêc phải
      27002
                  toàn
                                      thưc
                                                  thực hiện
                  thông tin
                                      hiên
28. a) Đề ra , Nhân
                        , Lưa 29.Cdh) với dian
                                              , Thưc
                                                         , Xây 30, all hoệt ti lại, Thực
                                                                                        , Thưc
                                                                                                 , The
      phạm c) dạng,
                        e) chọn d) bị lý các
                                               c) thi các b) dụng e) thờác
                                                                              c) thi viêc e) hiên
                                                                                                  b) thi
      vi,
                đánh
                           các
                                   tuyêmoạt
                                                 kiểm
                                                            và
                                                                     cáttành
                                                                                đánh
                                                                                           viêc
                                                                                                    thu
      chính
                giá rủi
                                   bố /đông
                                                 soát và
                                                                     thođông
                                                                                           kiểm
                           muc
                                                            thưc
                                                                                giá
                                                                                                    giá
      sách
                                   báovà tài
                ro và
                           tiêu
                                                 các
                                                            thi kế
                                                                     tuvcà sư
                                                                                thường
                                                                                           toán
                                                                                                    sát
      của
                các
                           kiểm
                                   cáonguyên
                                                 chương
                                                            hoach
                                                                     plkánện
                                                                                xuyên
                                                                                           (audit)
                                                                                                    viê
      ISMS
                phương
                                   áp
                                                 trình
                                                            rủi ro
                                                                     hiệnh
                                                                                với
                                                                                           nội bộ
                                                                                                    đái
                           soát
      và
                                                                                           với
                pháp
                           và
                                   dụng
                                                 đạo
                                                                     vähưởng
                                                                                ISMS
                                                                                                    giá
                xử lý
                                                                                bởi bô
                                                                                                    thι
      hướng
                           biên
                                                                     photeen
                                                                                           ISMS
                                                 tao
      tiếp
                rủi ro
                           pháp
                                                 chuyên
                                                                     ứh⊊MS
                                                                                phận
                                                                                                    χu
      cận
                           kiểm
                                                 môn và
                                                                     lai
                                                                                quản lý
                                                                                                    tín
      đánh
                           soát
                                                 giáo
                                                                     các
                                                                                                    hiê
      giá rủi
                                                 dục ý
                                                                     sự
                                                                                                    qu
                                                 thức
                                                                     cố
                                                                                                    cůa
      ro
```

31. c) Thực , Áp , Đảm 32. c) Luôn , Luôn nắm 33. a) Digital Millennium hiên a) dụng d) bảo b) vững môi thưc Copyright Act các các các hiện trường cải bài cải công việc pháp lý nằm hiên tai và tiến đã tiến đã được đạt các luật và trong đươc hoc đươc khuôn các quy nhận và các khổ cho đinh luât Thảo phép của pháp dang, mục luât các luân tiêu hành kết pháp động quả sửa với

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

các

bên

quan

tâm

chữa và

ngăn

chặn

- 35. b) chấp nhận được
- 36. d) các đặc điểm văn hóa / khác nhau

an ninh ١Ś١

ty/tổ

chức

thực hiện

hành νi

phạm

pháp

hoặc

phi

đạo

đức,

- 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

- , Gồm , Nếu 42. b) Luật luôn bắt buộc / 41. b) Là trách d) cả c) một nhiêm trách nhân trước nhiệm viên luật của 1 pháp lý phải công
 - Chính sách: thiếu hiểu biết chính sách là 1 cách bào chữa chấp nhận được
 - pháp của tổ hoàn chức trả và đó đền được bù mở cho rộng những ngoài hành phạm vi sai vi luật trái hình sự và luật hợp đồng
- gây thiệt hại cho cá nhân, tổ chức khác, thì công ty/tổ chức đó phải chịu trách nhiệm

về

pháp

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 vê
- 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