MIS5206-Section Protecting Information Assets-Exam 1

Your Name _____ Date _____

1. Which of the following contains general approaches that also provide the necessary flexibility in the event of unforeseen circumstances?

a. Policies
b. Standards
c. Procedures
d. Guidelines

2. Which of the following statements is not true with respect to the relationships between threat, vulnerability, countermeasure and risk?

a. A threat agent takes advantage of a vulnerability
b. The probability of a fire causing damage is a risk
c. A countermeasure can mitigate a threat
d. A vulnerability can expose a system to possible damage

3. Steve is doing risk analysis as part of his company's Intervation Risk Management. He ends up with a calculation that the annualized loss expectancy (ALE) due to a virus attack on the company's network is $25,000. He also calculates that the single loss expectancy (SLE) due to this event would be $25,000. What can you say about the annualized rate of occurrence (ARO)?

a. The ARO will be greater than 1.0
b. The ARO will be less than 1.0
c. The ARO cannot be calculated in this case
d. The ARO equals 1.0

4. Once risk assessment of a company is performed, threats and vulnerabilities are identified, and the total and residual risk is determined. Which of the following is not one of the ways in which risk is handled?

a. Risk Inference
b. Risk Mitigation
c. Risk Acceptance
d. Risk Avoidance

5. In a secure network, personnel play a key role in the maintenance and promotion of security procedures. Which of the following roles is responsible for ensuring that the company complies with software license agreements?

a. Product-line manager
b. Process owner
c. Solution provider
d. Data analyst

6. Information such as data that is critical to a company needs to be properly identified and classified. In general, what are the guidelines to classify data?

a. Classify all data irrespective of format (digital, audio, video) excluding paper
b. Classify only data that is digital in nature and exists on the company servers
c. Classify all data irrespective of the format it exists in (paper, digital, audio, video)
d. Classify only data that is digital in nature and exists on the company servers, desktops and all computers in the company

7. Non-enforced password management on servers and workstations would be defined as a:

a. Risk
b. Threat Agent
c. Vulnerability
d. Threat

8. One of the primary steps in a quantitative risk analysis is to determine the annualized loss expectancy (ALE). How is the ALE calculated?

a. Single loss expectancy / Frequency per year
b. Asset value x 2. 8
c. Single loss expectancy X Frequency per year
d. Asset value + (Single loss expectancy / Frequency per year)

9. An Electrical provider must maintain documentation of their electronic security perimeter in precisely the way set forth in the North American Energy Reliability Corporation (NERC) Critical Infrastructure Protection documents, particularly CIP-005-1, or face significantly penalties. What is this an example of:

a. Standards
b. Baselines
c. Practices
d. Policies

10. Which of the following terms refers to a security hole that could result in an attack on a system?

a. Risk
b. Exposure
c. Threat
d. Vulnerability

11. Which of the following has the highest potential to be a security hazard to a company that has well-defined security procedures.

a. An employee who performs critical duties is fired
b. The Information Security Officer falls ill
c. Grid power is lost for 3 hours
d. A web server containing employee performance data crashes

12. After risks are mitigated, what is the amount of risk remaining called

a. Annualized Loss Expectancy
b. Single Loss Expectancy
c. Residual Risk
d. Exposure Factor

13. Before Joan can begin work at her new job, she must undergo a criminal background check and participate in security awareness training. What type of control are these preventative measures?

a. Technical Controls
b. Administrative Controls

c. Physical Controls
d. Resident Controls

14. Which of the following denotes the magnitude of potential losses due to a threat?

a. Risk
b. Exposure
c. Vulnerability
d. Loss

15. Which of the choices below is the most often used criteria to determine the classification of a business object?

a. Value
b. Useful life
c. Age
d. Personal association

16. What is a virus?

a. An email message
b. An image that embeds itself in your file directory
c. A program that replicates to “infect” a computer
d. Data in various and unusual forms

17. What is your best defense against virus infection?

a. Don't open e-mail attachments you are not expecting
b. Don't surf the Internet
c. Don't download files from the Internet
d. Don't use USB Storage to transfer data

18. The MOST important reason for conducting the same risk assessment more than once is because:

a. Mistakes are often made in the initial reviews
b. Security risks are subject to frequent change
c. Different reviewers analyze risk factors differently
d. It shows management that the security staff is adding value

19. The GREATEST reduction in overhead costs for security administration would be provided by:

a. Mandatory access control
b. Role-based access control
c. Decentralized access control
d. Discretionary access control

20. Which of the following are least likely to change in response to technological changes?

a. Standards
b. Procedures
c. Policies
d. Guidelines

MIS5206-Section Protecting Information Assets-Exam 1

21. Which of the choices below is NOT a common information gathering technique for risk assessment?

a. Distributing a questionnaire
b. Employing automation risk analysis tools
c. Review existing policy documents
d. Interview terminated employees

22. Which group represents the most likely source of an asset loss through inappropriate computer use?

a. Crackers
b. Hackers
c. Employees
d. Saboteurs

23. Which of the following message attachments would you be wise not to open? A message with an attachment that:

a. Appears more than once in your Inbox
b. Says it's a sample copy of a new game from a recognized company e-mail address
c. Is an unexpected note from a friend
d. All of the above

24. Best practice for a mandatory password change-cycle is:

a. Never
b. Daily
c. Yearly
d. Every 2 - 3 months

25. Which of the following is the BEST indicator that security awareness training has been effective?

a. Have employees sign to confirm they have read the security policy
b. More incidents are being reported
c. A majority of employees have received training
d. Feedback forms from training are favorable

26. Which of the following should be developed FIRST?

a. Standards
b. Procedures
c. Policies
d. Guidelines

27. The PRIMARY objective of security awareness is to:

a. Ensure that security policies are read and understood
b. Encourage security-conscious employee behavior

c. Meet legal and regulatory requirements
d. Put employees on notice in case follow-up action for noncompliance is necessary

28. Which choice below is an accurate statement about the difference between auditing and monitoring?

a. A system audit is an on-going, real-time activity that examines a system
b. Monitoring is on ongoing activity that may include auditing a system or users
c. A system audit cannot be automated
d. Monitoring is a one-time event to evaluate security

29. Which of the below definitions is the best description of a vulnerability?

a. A weakness in a system that could be exploited
b. A company resource that is lost due to an incident
c. The minimum loss associated with an incident
d. A potential incident that could cause harm

30. Which of the following should management use to determine the amount of resources to devote to mitigating exposures?

a. Risk analysis results
b. Audit report findings
c. Penetration test results
d. Fixed percentage of IT budget

31. Which of the following will best protect against deletion of data files by a former employee?

a. Pre-employment screening
b. Close monitoring of users
c. Periodic awareness training
d. Efficient termination procedures

32. Which of the following is the best method for ensuring that security procedures and guidelines are read and understood?

a. Periodic focus group meetings
b. Periodic reminder memos to management
c. Computer-based training (CBT) presentations
d. Employees signing an acknowledgement of receipt

33. Which best describes the difference between a system owner and an information owner?

a. A system owner is responsible for defining the rules for the use of information
b. One system could have multiple information owners
c. An information owner is responsible for defining a system's operating parameters
d. There is a 1:1 relationship between system and information owners

34. Which statement below best describes the purpose of risk analysis?

a. To develop a clear cost-to-value ration for implementing security controls
b. To influence the system design process
c. To influence site selection decisions

d. To quantify the impact of potential threats

35. Which of the following is most appropriate for inclusion in an information security strategy?

a. Business controls designated as key controls
b. Security processes, methods, tools and techniques
c. Firewall rule sets, network defaults and intrusion detection system (IDS) settings
d. Budget estimates to acquire specific security tools

36. Which of the choices below is an incorrect description of a control?

a. Detective controls discover attacks and trigger preventive or corrective controls
b. Corrective controls reduce the effect of an attack
c. Corrective controls reduce the likelihood of a deliberate attack
d. Controls are the countermeasures for vulnerabilities

37. What is the most common delivery method for viruses?

a. Email
b. Internet download
c. Infected disks
d. Instant messenger software

38. Where should you write down your passwords?

a. Someplace easily seen from your computer
b. Someplace that is out of sight, like beneath your keyboard or in a nearby drawer.
c. Wherever you really need it for your memory, but this information can only be kept in a secure location
d. You should never write down your password

39. Which of the following BEST provides access control to payroll data being processed on a local server?

a. Logging access to personal information
b. Using separate passwords for sensitive transactions
c. Using software that restricts access rules to authorized staff
d. Restricting system access to business hours

40. When residual risk is minimized:

a. Acceptable risk is achieved
b. Transferred risk is minimized
c. Control risk is reduced to zero
d. Residual risk equals transferred risk

41. Risk management programs are designed to reduce risk to:

a. A level this is too small to be measurable
b. The point at which the expense exceeds the benefit
c. A level that the organization is willing to accept
d. A level that exceeds internal Security Policy defined standards

42. Which of the following is MOST likely to be discretionary?

a. Policies
b. Procedures
c. Guidelines
d. Standards

43. Place the data categorization scheme below in order from least secure to most secure:

A. Confidential
B. Classified
C. Public
D. Proprietary

a. C, D, A, B
b. C, B, D, A
c. C, A, B, D
d. C, D, B, A

44. What is an ARO?

e. A dollar figure assigned to a single event
f. The annual expected financial loss to an organization from a threat
g. A number that represents the estimated frequency of an expected event
h. The percentage of loss that would be realized for a specific asset if a threat occurred

45. What requires not granting a system process, program or an individual no more access privileges than are necessary to perform the task?

a. Administrative controls
b. Principle of least privilege
c. Technical controls
d. Risk management

46. What is the technique used to manipulate people into performing actions or divulging confidential information known as:

a. Malware
b. Industrial espionage
c. Social engineering
d. Phishing

47. Which of the following is MOST indicative of the failure of information security governance within an organization?

a. The information security department has had difficulty filling vacancies
b. The chief information officer (CIO) approves changes to the security policy
c. The information security oversight committee only meets quarterly
d. The data center manager has final sign-off on all security projects

48. Which of the following is a good way to create a password?

a. Letter or number sequences
b. Your children's or pet's names
c. Substituting numbers of letters, such as 3 for E
d. A combination of upper and lowercase letters mixed with numbers and symbols

49. If you're not careful about your Internet browsing, which of the following can be the result?

a. Spyware
b. Viruses
c. Hacking
d. All of the above

50. Which of the following BEST indicates a successful risk management practice?

a. Overall risk is quantified
b. Inherent risk is eliminated
c. Residual risk is minimized
d. Control risk is tied to business units