Post-Class Quiz: Information Security and Risk Management Domain

1. Which choice below is the role of an Information System Security Officer (ISSO)?
   A. The ISSO establishes the overall goals of the organization's computer security program.
   B. The ISSO is responsible for a day-to-day security administration.
   C. The ISSO is responsible for examining systems to see whether they are meeting stated security requirements.
   D. The ISSO is responsible for following security procedures and reporting security problems.

2. Security management practice focuses on the continual protection of:
   A. Company assets
   B. Classified information
   C. Security-related hardware and software
   D. Company data

3. Who has the ultimate responsibility for information security within an organization?
   A. IT Security Officer
   B. Project Managers
   C. Department Directors
   D. Senior Management

4. The following term is used to represent the likelihood of a threat source taking advantage of a vulnerability:
   A. Vulnerability
   B. Threat
   C. Risk
   D. Exposure

5. The following term is used to represent an instance of being exposed to losses:
   A. Vulnerably
   B. Threat
   C. Risk
   D. Exposure

6. A deviation from an organization-wide security policy requires which of the following?
   A. Risk acceptance
   B. Risk assessment
   C. Risk reduction
   D. Risk containment

7. Which of the following statement is true for threats?
   A. Cannot be eliminated
   B. Can always be mitigated
   C. Are always understood
   D. Are the main reason for creating security policies

8. In a "top-down approach", the security program is driven by:
   A. Senior management
   B. Senior security staff
   C. All personnel
   D. Senior auditing staff

9. Organizational security goals are typically:
   A. Monthly (every 30 days)
   B. Operational (mid-term)
   C. Tactical (daily)
   D. Strategic (long-term)

10. Security policies are best developed after performing:

A. Risk analysis
B. Cost-benefit analysis
C. Risk management analysis
D. Security policy analysis

11. Risk management helps you do all of the followings except:

A. Identify risks
B. Assess risks
C. Reduce risk to an *acceptable level*
D. Completely avoid risk

12. Risk analysis helps you accomplish all of the followings except:

A. Identify risks
B. Identify individual attackers
C. Justify security safeguards
D. Budget appropriately for risks

13. Risk analysis allows you to do all of the followings except:

A. Quantify the impact of potential risks
B. Create an economic balance between the impact of a risk and the cost of a countermeasure
C. Provides a cost/benefit comparison
D. Prevent risk

14. The two risk analysis approaches are:

A. Quantitative and numerical
B. Qualitative and judgmental
C. Judgmental and numerical
D. Quantitative and qualitative

15. The following risk analysis approach deals with concrete probability percentages:

A. Quantitative
B. Qualitative
C. Judgmental
D. Numerical

16. The potential loss per risk is known as the:

A. Single loss expectancy (SLE)
B. Annualized rate of occurrence (ARO)
C. Exposure factor (EF)
D. Asses value (AV)

17. The estimated frequency a threat will occur within a year is known as the:

A. Single loss expectancy (SLE)
B. Annualized rate of occurrence (ARO)
C. Exposure factor (EF)
D. Asses value (AV)

18. The percentage of loss a realized threat could have on a certain asset is known as the:

A. Single loss expectancy (SLE)
B. Annualized rate of occurrence (ARO)
C. Exposure factor (EF)
D. Asset value (AV)

19. Which of the following is the correct calculation?

A. Asset value (%) x exposure factor (%) = single loss expectancy (%)
B. Asset value ($) x exposure factor (%) = single loss expectancy ($)
C. Asset value (%) x exposure factor ($) = single loss expectancy ($)
D. Asset value ($) x exposure factor ($) = single loss expectancy ($)

20. Which of the following is not true with respect to qualitative risk analysis?

A. It uses scenarios
B. It is based on judgment, intuition and experience
C. May include the Delphi technique
D. Results in concrete probability percentages

21. Countermeasures, or safeguards, should be all of the followings except:

A. Cost effective
B. Its benefits must outweigh or equal its cost
C. May require a cost/benefit analysis
D. Best of breed

22. Total risk exists when:

A. An organization decides to not implement safeguards due to the results of cost/benefit analysis
B. Risk is so overwhelming that even safeguards can't protect against it
C. Safeguards have failed to an extent where attackers own the target network
D. Performing risk analysis and all risks are added up together

23. Any risk left over after implementing safeguards is known as:

A. Leftover risk
B. Residual risk
C. Remaining risk
D. Totally leftover risk

24. Methods of handling risk include all of the followings except:

A. Transferring risk
B. Reducing risk
C. Accepting risk
D. Selling risk

25. Which of the following is not true regarding security policy?

A. It is a general statement

B. It is promulgated by senior IT security staff

C. It describes the role of security in the organization

D. It is broad

26. Which of the following is considered "strategic"?

A. Security policy

B. Mandatory standards

C. Recommended guidelines

D. Detailed procedures

27. Which of the following is not true regarding standards?

A. Ensure uniformity

B. Are usually compulsory

C. Are typically developed from baselines

D. Only relate to hardware

28. Which of the following is not true regarding procedures?

A. Describe how policy, standards, and guidelines will actually be implemented

B. Are detailed

C. Are step-by-step actions

D. Are used during unforeseen circumstances

29. Which of the following terms describes activities that make sure protection mechanisms are maintained and operational?

A. Due care

B. Due diligence

C. Due care but not due diligence

D. Due care and due diligence

30. Which of the following is not true regarding data classification?

    A. It helps determine the level of confidentiality required
    B. It helps determine the level of integrity required
    C. It helps determine the level of authentication required
    D. It ensures data is protected in the most cost-effective manner

31. The member of senior management who is ultimately responsible for an organization's data is known as the:

    A. Data custodian
    B. Data owner
    C. Data guardian
    D. Data boss

32. When there is a "separation of duties", parts of tasks are assigned to different people so that:

    A. Collusion is required to perform an unauthorized act
    B. Better planning is required to break into systems
    C. Defense-in-depth is achieved by creating multiple layers an attacker must circumvent
    D. The weakest link, people, are not easily flipped

33. Which of the following organization placement is ideal for IT Security function?

    A. Security as function within the Information Technology Organization.
    B. Security reporting to a specialized business unit such as legal, corporate security or insurance.
    C. Chief Security Officer reporting directly to the CEO.
    D. None of the above.

34. Which of the following is the highest level of documentation?

    A. Standards
    B. Guidelines
    C. Policies
    D. Baselines

35. Which choice below is not an example of an issue-specific policy?

A. E-mail privacy policy

B. Virus-checking disk policy

C. Defined router ACLs

D. Unfriendly employee termination

36. Which choice below is not a generally accepted benefit of security awareness, training and education?

A. A security awareness program can help operators understand the value of the information.

B. A security education program can help system administrators recognize unauthorized intrusion attempts.

C. A security awareness and training program will help prevent natural disasters from occurring.

D. A security awareness and training program can help an organization reduce the number and severity of errors and omissions.

37. Which choice below is an incorrect description of a control?

A. Detective controls discover attacks and trigger preventive or corrective controls

B. Corrective controls reduce the likelihood of a deliberate attack

C. Corrective controls reduce the affect of a an attack

D. Controls are the countermeasures for vulnerabilities

38. How often should an independent review of the security controls be performed, according to OMB Circular A-130?

A. Every year

B. Every three years

C. Every five years

D. Never

39. Which choice below would not be considered an element of proper user account management?

A. Users should never be rotated out of their current duties.

B. The user's accounts should be reviewed periodically.

C. A process for tracking access authorizations should be implemented.

D. Periodically re-screen personnel in sensitive positions.

40. Which choice below represents an application or system demonstrating a need for a high level of confidentiality protection and controls?

A. Unavailability of the system could result in inability to meet payroll obligations and could cause work stoppage and failure of user organizations to meet critical mission requirements. The system requires 24-hour access.

B. The application contains proprietary business information and other financial information, which if disclosed to unauthorized source, could cause an unfair advantage for vendors, contractors, or individuals and could result in financial loss or adverse legal action to user organizations.

C. Destruction of the information would require significant expenditures of time and effort to replace. Although corrupted information would present an inconvenience to the staff, most information, and all vital information, is backed up by the either paper documentation or on disk.

D. The mission of this system is to produce local weather forecast information that is made available to the news media forecasters and the general public at all times. None of the information requires protection against disclosure.

41. Which of the following is the best reason for the use of an automated risk analysis tool?

A. Much of the data gathered during the review cannot be reused for subsequent analysis.

B. Automated methodologies require minimal training and knowledge of risk analysis.

C. Most software tools have user interfaces that are easy to use.

D. Minimal information gathering is required due to the amount of information built into the tool.

42. Which must bear the primary responsibility for determining the level of protection needed for information systems resources?

A. Data Owner

B. Senior Management

C. System Administrator

D. Project Manager

43. What is the inverse of the confidentiality integrity and availability (CIA) triad in risk management?

    A. Misuse, exposure, and destruction.

    B. Authorization, non-repudiation, and integrity.

    C. Disclosure, alteration, and destruction.

    D. Confidentiality, integrity, and availability.

44. What would be the Annualized Rate of Occurrence (ARO) where a company employs 100 data entry clerks each of whom averages one input error per month?

    A. 100

    B. 120

    C. 1,000

    D. 1,200

45. How is Annualized Loss Expectancy (ALE) derived?

    A. ARO x (SLE – EF)

    B. SLE x ARO

    C. SLE/EF

    D. AV x EF

46. What is the difference between quantitative and qualitative risk analysis?

    A. Qualitative analysis uses mathematical formulas and while quantitative analysis does not.

    B. Purely qualitative analysis is not possible, while purely quantitative is possible.

    C. Quantitative analysis provides formal cost/benefit information while qualitative analysis does not.

    D. There is no difference between qualitative and quantitative analysis.

47. Which choice is an accurate statement about standards?

    A. Standards are the high-level statements made by senior management in support of information systems security.

    B. Standards are the first element created in an effective security policy program

C. Standards are used to describe how policies will be implemented.

D. Standards are senior management's directives to create a computer security program.

48. If risk is defined as "the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets" the risk has all of the following elements except?

A. An impact of assets based on threats and vulnerabilities.

B. Controls addressing the threats.

C. Threats to and vulnerabilities of processes and/or assets.

D. Probabilities of the threats.

49. Which of the following should not be a role of the security administrator?

A. Authorizing access rights.

B. Implementing security rules.

C. Insuring that local policies have been authorized by management.

D. Allocating access rights.

50. Which of the following is not accurate regarding the process of risk management?

A. The likelihood of a threat must be determined as an element of the risk assessment.

B. The level of impact of a threat must be determined as an element of the risk assessment.

C. Risk assessment is the first process in the risk management methodology.

D. Risk assessment is the final result of the risk management methodology.

51. Which choice below most accurately reflects the goals of risk mitigation?

A. Defining the acceptable level of risk the organization can tolerate, and reducing risk to that level.

B. Analyzing and removing all vulnerabilities and threats to security within the organization.

C. Defining the acceptable level of risk the organization can tolerate, and assigning any costs associated with loss or disruption to a third party such as an insurance carrier.

D. Analyzing the effects of a business disruption and preparing the company's response.

52. Which answer below is the best description of Single Loss Expectancy (SLE)?

A. An algorithm that represents the magnitude of a loss to an asset from a threat.

B. An algorithm that expresses the annual frequency with which a threat is expected to occur.

C. An algorithm used to determine the monetary impact of each occurrence for a threat.

D. An algorithm that determines the expected annual loss to an organization from a threat.

53. Which choice below is the best description of an Annualized Loss Expectancy (ALE)?

A. The expected risk factor of annual threat event, derived by multiplying the SLE by its ARO

B. An estimate of how often a given threat event may occur annually.

C. The percentile of the value of the asset expected to be lost, used to calculate the SLE.

D. A value determined by multiplying the value of the asset by its exposure factor.

54. Which choice below is not an example of appropriate security management practice?

A. Reviewing access logs for unauthorized behavior.

B. Monitoring employee performance in the workplace.

C. Researching information on a new intrusion exploits.

D. Promoting and implementing security awareness programs.

55. Which choice below is not an accurate description of an information policy?

A. Information policy is senior management's directive to create a computer security program.

B. An information policy could be a decision pertaining to use of the organization's fax.

C. Information policy is a documentation of computer security decisions.

D. Information policies are created after the system's infrastructure has been designed and built.