

Management 414: SANS CISSP® 10 Domains +S QUIZ - Domain 3

1. Which of the following formulas is used to calculate Risk?
 - a) Risk {due to a threat} = Vulnerability x Threat {to that vulnerability}
 - b) Risk {due to a vulnerability} = Vulnerability x Threat {to that vulnerability}
 - c) Risk {due to a threat} = Threat x Vulnerability {to that threat}
 - d) Risk {due to a vulnerability} = Threat x Vulnerability {to that threat}

2. In the formula displayed below, what does 'Vulnerability' represent?
Risk = Threat x Vulnerability
 - a) Vulnerability to that specific threat
 - b) Vulnerability to threats in general
 - c) Vulnerability to unknown threats
 - d) Vulnerability to known threats

3. Which of the following choices specifies a certain way in which something should be done or a certain brand or type of equipment that must be used?
 - a) Standard
 - b) Baseline
 - c) Policy
 - d) Procedure

4. After you install a well-configured firewall, a web site inside your perimeter is defaced by an outside attack. Which security principal has NOT been addressed?
 - a) Defense-in-Depth
 - b) Deny all, then allow as needed
 - c) Least possible privilege
 - d) Know your system

5. When a threat connects to its vulnerability, what is the result?
 - a) Reduced risk
 - b) Possible system compromise
 - c) Increased impact
 - d) Increased uncertainty

6. Which of the following is the most common defense tactic?
 - a) Establishing a strong security policy
 - b) Applying software patches as soon as possible
 - c) Deploying perimeter defenses such as firewalls
 - d) Replacing hubs with switches

Management 414: SANS CISSP® 10 Domains +S QUIZ - Domain 3

7. The Risk Management option to "accept the risk" is most reasonable after which of the following steps has been taken?
- a) Perform penetration testing
 - b) Identify the probable threats
 - c) Deploy a perimeter defense
 - d) Mitigate or reduce the risk
8. Of the following, which best describes the 'insurance model' of Risk Management?
- a) Pass the risk over to a third-party.
 - b) Redirect the cost of insurance into Risk Avoidance efforts.
 - c) Follow best practices to insure security.
 - d) Ignore the risk
9. In the formula displayed below, what does the "Exposure Factor" represent?
- Single Loss Expectancy = Asset Values X Exposure Factor
- a) The degree to which an asset is vulnerable to attack.
 - b) The percentage of loss a threat event would have on the asset.
 - c) The cost to reduce the risk that an asset is subject to.
 - d) The likelihood that a threat would escalate into an event.
10. Which of the following are the two common approaches to risk assessment?
- a) Proactive and Reactive
 - b) In-house and vendor provided
 - c) Open Source and Closed Source
 - d) Qualitative and Quantitative
11. Which of the following methods of risk assessment is the more valuable tool for business decision-making?
- a) The Legal exposure method
 - b) The Human resources method
 - c) The Quantitative method
 - d) The Heuristic method
12. Which of the following statements is TRUE?
- a) Risk Management is as much about Security as anything.
 - b) Threats are as much about Risk Management as anything.
 - c) Vulnerabilities are as much about Security as anything.
 - d) Security is as much about Risk Management as anything.
13. Of the following, which best describes the 'insurance model' of Risk Management?
- a) Redirect the cost of insurance into Risk Avoidance efforts.
 - b) Follow best practices to insure security.

Management 414: SANS CISSP® 10 Domains +S QUIZ - Domain 3

- c) Pass the risk over to a third-party.
 - d) Escrow adequate funds to insure timely Risk Recovery.
14. Which approach to Risk Assessment tries to assign an objective numeric value to describe the degree of risk?
- a) The Qualitative approach
 - b) The Heuristic approach
 - c) The Elliptical Curve approach
 - d) The Quantitative approach
15. Which approach to risk assessment focuses on the more intangible values to describe the degree of risk?
- a) The Qualitative approach
 - b) The Quantitative approach
 - c) The Ephemeral approach
 - d) The Consensus approach
16. A security incident can be thought of in which of the following terms?
- a) Confidentiality, integrity and portability
 - b) Confidentiality, integrity and availability
 - c) Integrity, privacy and accountability
 - d) Availability, accountability and authority
17. Why is it that a firewall alone cannot provide acceptable security?
- a) Threats can come in different forms and sources.
 - b) A firewall can be compromised or bypassed.
 - c) A firewall cannot defend against most malware.
 - d) Threats can come from malicious insiders.
18. Which of the following is MOST required in order to reduce or prevent vulnerabilities?
- a) You must know about the vulnerabilities.
 - b) You must have proper authorization.
 - c) Authenticated vendor patches, hot fixes or alerts
 - d) Consensus from top management
19. Which of the following is NOT one of the three Risk Choices?
- a) Accept the risk as is.
 - b) Mitigate or reduce the risk.
 - c) Transfer the risk.
 - d) Reject the risk as is.

Management 414: SANS CISSP® 10 Domains +S QUIZ - Domain 3

20. Which of the following is required before deciding between accepting, mitigating, or transferring a risk?
- a) Our legal department should be consulted.
 - b) The threat should first be mitigated or reduced.
 - c) We should understand the risk and how it affects us.
 - d) Eliminate all uncertainty associated with the risk.
21. Which of the following is NOT a benefit of security awareness?
- a) Measurable reduction in unauthorized actions attempted by personnel
 - b) Increases the effectiveness of protection controls
 - c) Reduces the layers of 'defense-in-depth' to a more manageable level
 - d) Helps to avoid fraud, waste and abuse of computing resources
22. Which of the following terms is best defined by the statement below?
3. 'General, collective awareness of an organization's personnel of the importance of security and security controls.'
- a) Security Posture
 - b) Security Awareness
 - c) Security Management
 - d) Security Measurement
23. Regarding 'Data Classification Roles', an 'Owner' can be described any of the following, except one. Which of the following does NOT describe a data 'owner'?
- a) An executive or manager of an organization
 - b) Responsible for the asset of information that must be protected
 - c) Has the final corporate responsibility of data protection
 - d) Verifies the data's integrity
24. When talking about 'Data Classification Roles', a 'custodian' is concerned with all of the following except which one?
- a) Running regular backups and routinely testing the validity of the backup.
 - b) Performing data restoration from the backups when necessary.
 - c) Maintaining those retained records in accordance with the established information classification policy.
 - d) Determining the data's value to the organization and the threshold beyond which obsolete data is purged.
25. Which of the following is NOT one of the 'Data Classification Roles'?
- a) Owner
 - b) Developer
 - c) User
 - d) Custodian

Management 414: SANS CISSP® 10 Domains +S QUIZ - Domain 3

26. Integrity includes all of the following characteristics except which one?
- a) Prevent the intentional or unintentional unauthorized disclosure of a message's contents.
 - b) Modifications are not made to data by unauthorized personnel or processes.
 - c) Unauthorized modifications are not made to data by authorized personnel or processes.
 - d) Data is internally and externally consistent.
27. How can 'Confidentiality, Integrity, and Availability (C.I.A.)' also be expressed?
- a) Security Effectively Applied (S.E.A.)
 - b) Disclosure, Alteration, and Destruction (DAD.)
 - c) Anonymity, Precaution, and Evasion (A.P.E.)
 - d) Firewalls, Backups, Integrity (F.B.I.)
28. Which of the following is the central characteristic of accountability?
- a) The rights and permissions granted to an individual (or process), which enable access to a computer.
 - b) Reliable and timely access to data or computing resources by the appropriate personnel.
 - c) A system's ability to determine the actions and behavior of a single individual within a system.
 - d) Detailed steps to be followed by users, system operations personnel or others to accomplish a specific task.
29. One way to describe 'policies' is to say that they are a collection of senior management's directives. Which of the following would NOT be a senior management directive?
- a) Determine the products and components to be used.
 - b) Create a computer security program.
 - c) Establish the goals of the computer security program.
 - d) Assign responsibilities.
30. When talking about vulnerability there are certain requirements that turn a condition into a vulnerability. Which of the following is NOT a requirement of vulnerability?
- a) Weaknesses that allow threats to happen
 - b) Must be coupled with a threat to have an impact
 - c) Malicious damage to a system or data
 - d) Can be prevented (if you know about them)
31. Error checking is an example of which of the following control measures?
- a) Implementing strong integrity measures
 - b) Implementing strong availability measures

Management 414: SANS CISSP® 10 Domains +S QUIZ -- Domain 3

- c) Implementing strong confidentiality measures
 - d) Implementing data validation
32. Confidentiality, integrity, and availability can also be expressed by which of the following choices?
- a) Disclosure, Alteration, and Destruction
 - b) Denial of Service, Attenuation, and Destruction
 - c) Denial of Service, Alteration, and Disclosure
 - d) Disclosure, Attenuation, and Denial of Service
33. Which of the following labels is NOT commonly used by the government?
- a) Top Secret
 - b) Confidential
 - c) Sensitive but Unclassified
 - d) Trade Secret
34. Denial of Service attacks, hostile code, EMI, and power outages are example of threats that could affect which of the following choices?
- a) Availability
 - b) Integrity
 - c) Confidentiality
 - d) Visibility attacks
35. There are four categories of authentication. Which of the following choices is NOT a category?
- a) Someplace you are
 - b) Something you know
 - c) Something you have
 - d) Something you get
36. Which type of data classification is given the highest level of protection?
- a) Unclassified
 - b) Sensitive but Unclassified
 - c) Confidential
 - d) Top Secret
37. Which of the following choices is the first step when creating a data classification process?
- a) Create an enterprise awareness program
 - b) Identify the administrator
 - c) Specify the termination procedures
 - d) Specify the controls

Management 414: SANS CISSP® 10 Domains +S QUIZ -- Domain 3

38. Which of the following choices is NOT a responsibility of a data custodian?
- a) Provides hands on management
 - b) Administer the classification scheme
 - c) Makes critical decisions
 - d) Running regular backups
39. Which of the following choices defines the strategic goals for the organizations?
- a) Procedure
 - b) Guideline
 - c) Standard
 - d) Policy