|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Assessing risk should include testing of technology assets to identify any vulnerabilities.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2. Many cloud providers allow customers to perform penetration tests and vulnerability scans without permission and whenever is necessary.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 3. The classification designation of government documents is typically Top Secret, Secret, Unusual, Confidential, and Unclassified.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 4. A subject's privilege over an object should follow the principle of least privilege.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 5. The FIT calculation is another way of reporting MTTF.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 6. A security control is any device or process that is used to reduce risk.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 7. A physical control attempts to discourage security violations before they occur.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8. Distributive allocation refers to "eliminating" the risk.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 9. Risk avoidance involves identifying the risk and making the decision to engage in the activity.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 10. Vendor-specific guides are useful for configuring web servers, operating systems, applications servers, and network infrastructure devices.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 11. What term can be described as a function of threats, consequences of those threats, and the resulting vulnerabilities?   |  |  |  | | --- | --- | --- | |  | a. | threat | |  | b. | mitigation | |  | c. | risk | |  | d. | management |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 12. Due to the potential impact of changes that can affect all users in an organization, and considering that security vulnerabilities can arise from uncoordinated changes, what should an organization create to oversee changes?   |  |  |  | | --- | --- | --- | |  | a. | change management team | |  | b. | incident response team | |  | c. | security control team | |  | d. | compliance team |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 13. What is the name for a framework and corresponding functions required to enable incident response and incident handling within an organization?   |  |  |  | | --- | --- | --- | |  | a. | incident reporting | |  | b. | incident management | |  | c. | incident handling | |  | d. | incident planning |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 14. What can be defined as the planning, coordination, and communications functions that are needed to resolve an incident in an efficient manner?   |  |  |  | | --- | --- | --- | |  | a. | incident reporting | |  | b. | incident management | |  | c. | incident handling | |  | d. | incident planning |  |  |  | | --- | --- | | *ANSWER:* | c | |
| 15. A written document that states how an organization plans to protect the company's information technology assets is a:   |  |  |  | | --- | --- | --- | |  | a. | security policy | |  | b. | guideline | |  | c. | security procedure | |  | d. | standard |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 16. A collection of suggestions that should be implemented is referred to as a:   |  |  |  | | --- | --- | --- | |  | a. | security policy | |  | b. | baseline | |  | c. | guideline | |  | d. | security procedure |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 17. Select the option that best describes an asset:   |  |  |  | | --- | --- | --- | |  | a. | any item that is used by all employees | |  | b. | any item that is owned by an enterprise | |  | c. | any item that has a positive economic value | |  | d. | any item that is used by management |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 18. Select the option that best describes a policy:   |  |  |  | | --- | --- | --- | |  | a. | A collection of requirements specific to the system or procedure that must be met by everyone | |  | b. | A collection of suggestions that should be implemented | |  | c. | A list of all items that have a positive economic value | |  | d. | A document that outlines specific requirements or rules that must be met |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 19. Generally considered to be the most important information security policies, what item below defines the actions a user may perform while accessing systems and networking equipment?   |  |  |  | | --- | --- | --- | |  | a. | acceptable use policies | |  | b. | encryption policies | |  | c. | data loss policies | |  | d. | VPN policies |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 20. What kind of policy defines the actions users may perform while accessing systems and networking equipment?   |  |  |  | | --- | --- | --- | |  | a. | VPN access policy | |  | b. | network use policy | |  | c. | privacy use policy | |  | d. | acceptable use policy |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 21. Websites that group individuals and organizations into clusters or groups based on some sort are considered to be what type of networks?   |  |  |  | | --- | --- | --- | |  | a. | social media network | |  | b. | social engineering network | |  | c. | social management network | |  | d. | social control network |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 22. Which term below describes the art of helping an adult learn?   |  |  |  | | --- | --- | --- | |  | a. | andragogical | |  | b. | pedagogical | |  | c. | deontological | |  | d. | metagogical |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 23. What term best describes the ability to continue to function as the size or volume of the enterprise data center expands to meet the growing demands?   |  |  |  | | --- | --- | --- | |  | a. | adaptability | |  | b. | automation | |  | c. | flexibility | |  | d. | scalability |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 24. What type of learner tends to sit in the middle of the class and learns best through lectures and discussions?   |  |  |  | | --- | --- | --- | |  | a. | visual | |  | b. | auditory | |  | c. | kinesthetic | |  | d. | spatial |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 25. What type of learner learns best through hands-on approaches?   |  |  |  | | --- | --- | --- | |  | a. | visual | |  | b. | auditory | |  | c. | kinesthetic | |  | d. | spatial |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 26. What type of control is designed to provide an alternative to normal controls that for some reason cannot be used.?   |  |  |  | | --- | --- | --- | |  | a. | preventive control | |  | b. | compensating control | |  | c. | detective control | |  | d. | deterrent control |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 27. Which of the following refers to the start-up relationship between partners?   |  |  |  | | --- | --- | --- | |  | a. | partner on-boarding | |  | b. | partner trust | |  | c. | partner beginning | |  | d. | starting partner agreement |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 28. What is a service contract between a vendor and a client that specifies what services will be provided, the responsibilities of each party, and any guarantees of service?   |  |  |  | | --- | --- | --- | |  | a. | MOU | |  | b. | SLA | |  | c. | BPA | |  | d. | ISA |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 29. What describes an agreement between two or more parties and demonstrates a "convergence of will" between the parties so that they can work together?   |  |  |  | | --- | --- | --- | |  | a. | MOU | |  | b. | NDA | |  | c. | BPA | |  | d. | ISA |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 30. Which of the following is an agreement that is intended to minimize security risks for data transmitted across a network?   |  |  |  | | --- | --- | --- | |  | a. | MOU | |  | b. | SLA | |  | c. | BPA | |  | d. | ISA |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 31. Which of the following is considered to be a common security issue? (Choose all that apply.)   |  |  |  | | --- | --- | --- | |  | a. | management issues | |  | b. | certificate issues | |  | c. | encrypted credentials | |  | d. | authentication issues |  |  |  | | --- | --- | | *ANSWER:* | b, d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 32. Select the specific type of interview that is usually conducted when an employee leaves the company?   |  |  |  | | --- | --- | --- | |  | a. | last interview | |  | b. | initial interview | |  | c. | exit interview | |  | d. | post interview |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 33. What specific type of mechanism should be utilized by all types of training to provide input from participants on the training's effectiveness so that any needed modifications can be made for future training?   |  |  |  | | --- | --- | --- | |  | a. | participant feedback mechanism | |  | b. | survey feedback mechanism | |  | c. | training mechanism | |  | d. | feedback mechanism |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 34. What control is designed to identify any threat that has reached the system?   |  |  |  | | --- | --- | --- | |  | a. | preventive control | |  | b. | compensating control | |  | c. | detective control | |  | d. | deterrent control |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 35. What type of threat is a threat related to the natural surroundings of an enterprise?   |  |  |  | | --- | --- | --- | |  | a. | external threat | |  | b. | environmental threat | |  | c. | internal threat | |  | d. | biological threat |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 36. What type of risk calculation uses an "educated guess" based on observation?   |  |  |  | | --- | --- | --- | |  | a. | quantitative risk calculation | |  | b. | environmental risk calculation | |  | c. | qualitative risk calculation | |  | d. | observational risk calculation |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 37. Which threat category affects the long-term goals of the organization?   |  |  |  | | --- | --- | --- | |  | a. | operational | |  | b. | compliance | |  | c. | strategic | |  | d. | managerial |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 38. Which threat category impacts the daily business of the organization?   |  |  |  | | --- | --- | --- | |  | a. | operational | |  | b. | compliance | |  | c. | strategic | |  | d. | managerial |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 39. Which of the following is a network that moves a product from the supplier to the customer and is comprised of vendors that supply raw material, manufacturers who convert the material into products, warehouses that store products, distribution centers that deliver them to the retailers, and retailers who bring the product to the consumer?   |  |  |  | | --- | --- | --- | |  | a. | supply chain | |  | b. | supply chain assessment | |  | c. | supply sphere | |  | d. | supply network |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 40. Which of the following is a basic measure of reliability for systems that cannot be repaired?   |  |  |  | | --- | --- | --- | |  | a. | mean time to recovery | |  | b. | mean time to failure | |  | c. | mean time to operate | |  | d. | failure in time |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |
| --- | --- | --- |
| 41. What are the two risk calculation formulas commonly used to calculate expected losses?   |  |  | | --- | --- | | *ANSWER:* | The Single Loss Expectancy (SLE) is the expected monetary loss every time a risk occurs and the the Annualized Loss Expectancy (ALE) is the expected monetary loss that can be expected for an asset due to a risk over a one-year period. | |

|  |  |  |
| --- | --- | --- |
| 42. What is mean time to recovery (MTTR)?   |  |  | | --- | --- | | *ANSWER:* | MTTR is the average amount of time that it will take a device to recover from a failure that is not a terminal failure. | |

|  |  |  |
| --- | --- | --- |
| 43. What is a risk register?   |  |  | | --- | --- | | *ANSWER:* | A risk register is a list of potential threats and associated risks. The threats are sometimes rated both before and after controls have been implemented. Often shown as a table, a risk register can help provide a clear snapshot of vulnerabilities and risks. | |

|  |  |  |
| --- | --- | --- |
| 44. Explain how continuous monitoring can benefit an IT enterprise's operations.   |  |  | | --- | --- | | *ANSWER:* | Continuous monitoring allows for a continuous stream of near real-time views of the state of risk to clients, security devices, networks, cloud devices, applications and data. Continuous monitoring can provide valuable insight into assessing existing security controls. | |

|  |  |  |
| --- | --- | --- |
| 45. Contrast the difference between a pedagogical approach versus an andragogical approach to subject matter.   |  |  | | --- | --- | | *ANSWER:* | In a pedagogical approach, the subject matter is defined by what the teacher wants to give. In an andragogical approach, learning is organized around situations in life or at work. | |

|  |  |  |
| --- | --- | --- |
| 46. List and describe three of the six risk categories.   |  |  | | --- | --- | | *ANSWER:* | Strategic: Action that affects the long-term goals of the organization. Compliance: Following a regulation or standard. Financial: Impact of financial decisions or market factors. Operational: Events that impact the daily business of the organization. Technical: Events that affect information technology systems. Managerial: Actions that are related to the management of the organization. | |

|  |  |  |
| --- | --- | --- |
| 47. Why should authorization be obtained for penetration testing and vulnerability testing?   |  |  | | --- | --- | | *ANSWER:* | A penetration or vulnerability test is an attempt to break into a computer network. Because computer crime can carry severe penalties, a tester should have written and signed authority to conduct these tests. Penetration testing may result in disruption or even damage to data, or a third party may want to file a claim against the tester (such as a tester of a hospital system who corrupts patient information). Having prior authorization can help limit these risks. Although not common, there have been instances of penetration testers who have been successful in entering computer networks only to have technical support personnel "turn the tables" and instigate a retaliation attack against the tester. | |

|  |  |  |
| --- | --- | --- |
| 48. Explain the concept of change management.   |  |  | | --- | --- | | *ANSWER:* | Change management refers to a methodology for making modifications to a system and keeping track of those changes. In some instances, changes to network or system configurations are made haphazardly to alleviate a pressing problem. Without proper documentation, a future change may negate or diminish a previous change or even unknowingly create a security vulnerability. Change management seeks to approach changes systematically and provide the necessary documentation of the changes. | |

|  |  |  |
| --- | --- | --- |
| 49. What is privilege management?   |  |  | | --- | --- | | *ANSWER:* | Privilege management is the process of assigning and revoking privileges to objects; that is, it covers the procedures of managing object authorizations. | |

|  |  |  |
| --- | --- | --- |
| 50. What is a security control?   |  |  | | --- | --- | | *ANSWER:* | A security control is any device or process that is used to reduce risk. That is, it attempts to limit exposure to a danger. There are two levels of security controls, administrative controls and technical controls. Administrative controls are the processes for developing and ensuring that policies and procedures are carried out. Technical controls consists of security controls carried out or managed by devices. | |