|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. A business impact analysis may include succession planning or determining in advance who will be authorized to take over in the event of the incapacitation or death of key employees.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2. Resumption planning is used for the recovery of critical business functions separate from IT, such as resuming a critical manufacturing process.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 3. A business continuity plan will help determine the mission-essential function or the activity that serves as the core purpose of the enterprise.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 4. A privacy impact assessment is used to identify and mitigate privacy risks.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 5. A disaster recovery plan is developed for restoring the IT functions and services to their former state.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 6. A snapshot of the data is essentially a series of "reference markers" of the data at a specific point in time.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 7. An enterprise contingency plan is copying information to a different medium and storing it at an off-site location so that it can be used in the event of a disaster.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8. Forensics is the application of science to questions that are of interest to the technology professions.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 9. An incident response plan is a set of written instructions for reacting to a security incident.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 10. A legal stop order is a notification sent from the legal team to employees instructing them not to delete electronically stored information or paper documents that may be relevant to the incident.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 11. The process of identifying exposure to threats, creating preventive and recovery procedures, and then testing them to determine if they are sufficient, is known as:   |  |  |  | | --- | --- | --- | |  | a. | business continuity planning | |  | b. | disaster planning | |  | c. | business management planning | |  | d. | enterprise disaster planning |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 12. When does a company need to identify mission-critical business functions and quantify the impact a loss of such functions may have on the organization in terms of its operational and financial position, what should be performed?   |  |  |  | | --- | --- | --- | |  | a. | business risk analysis | |  | b. | business alert assessment | |  | c. | business productivity analysis | |  | d. | business impact analysis |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 13. What type of element addresses the recovery of critical information technology (IT) assets, including systems, applications, databases, storage and network assets?   |  |  |  | | --- | --- | --- | |  | a. | enterprise recovery | |  | b. | disaster recovery | |  | c. | business recovery | |  | d. | crisis management |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 14. Which term below describes a component or entity in a system which, if it no longer functions, will disable an entire system?   |  |  |  | | --- | --- | --- | |  | a. | recovery site | |  | b. | recovery point | |  | c. | single point of failure | |  | d. | cascade point of failure |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 15. 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, is known as:   |  |  |  | | --- | --- | --- | |  | a. | service level agreement | |  | b. | recovery point objective | |  | c. | recovery time objective | |  | d. | service point agreement |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 16. Select below the type of cluster where standby server exists only to take over for another server in the event of its failure.   |  |  |  | | --- | --- | --- | |  | a. | symmetric network | |  | b. | symmetric server | |  | c. | asymmetric network | |  | d. | asymmetric server |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 17. In what type of cluster does every server perform useful work so that if one fails, the remaining servers take on the additional load?   |  |  |  | | --- | --- | --- | |  | a. | symmetric network | |  | b. | asymmetric network | |  | c. | symmetric server | |  | d. | asymmetric server |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 18. How can an administrator keep devices powered when power is interrupted?   |  |  |  | | --- | --- | --- | |  | a. | uninterruptible power supply | |  | b. | redundant power supply | |  | c. | uninterruptible system supply | |  | d. | replica power supply |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 19. A location that has all the equipment installed but does not have active Internet or telecommunications facilities, and does not have current backups of data, is an example of a:   |  |  |  | | --- | --- | --- | |  | a. | cold site | |  | b. | hot site | |  | c. | spare site | |  | d. | warm site |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 20. Which of the following is a location that provides office space, but the customer must provide and install all the equipment needed to continue operations?   |  |  |  | | --- | --- | --- | |  | a. | cold site | |  | b. | hot site | |  | c. | spare site | |  | d. | warm site |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 21. A metallic enclosure that prevents the entry or escape of an electromagnetic field is known as a:   |  |  |  | | --- | --- | --- | |  | a. | bollard cage | |  | b. | mantrap | |  | c. | Faraday cage | |  | d. | Newton cage |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 22. Using technology to search for computer evidence of a crime in order to retrieve information, even if it has been altered or erased, that can be used in pursuit of an attacker or criminal is an example of:   |  |  |  | | --- | --- | --- | |  | a. | computer forensics | |  | b. | penetration testing | |  | c. | vulnerability testing | |  | d. | risk management |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 23. What kind of data can be lost when a computer is turned off?   |  |  |  | | --- | --- | --- | |  | a. | volatile | |  | b. | static | |  | c. | non-volatile | |  | d. | persistent |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 24. A snapshot of the current state of a computer that contains all current settings and data is known as what option below:   |  |  |  | | --- | --- | --- | |  | a. | system standard | |  | b. | system view | |  | c. | system image | |  | d. | system baseline |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 25. What is the name for an image that consists of an evidence-grade backup because its accuracy meets evidence standards?   |  |  |  | | --- | --- | --- | |  | a. | baseline | |  | b. | mirror image | |  | c. | logical image | |  | d. | thin image |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 26. What term is used to describe a documentation of control over evidence, which is used to ensure that no unauthorized person was given the opportunity to corrupt the evidence?   |  |  |  | | --- | --- | --- | |  | a. | chain of value | |  | b. | chain of use | |  | c. | chain of property | |  | d. | chain of custody |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 27. Multiple sectors on a disk, when combined, are referred to as a:   |  |  |  | | --- | --- | --- | |  | a. | cluster | |  | b. | track | |  | c. | slice | |  | d. | platter |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 28. When the remaining cluster space of a partially filled sector is padded with contents from RAM. What is the name for this type of scenario?   |  |  |  | | --- | --- | --- | |  | a. | Disk slack | |  | b. | RAM slack | |  | c. | ROM slack | |  | d. | Edge slack |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 29. What kind of slack is created from information stored on a hard drive, which can contain remnants of previously deleted files or data?   |  |  |  | | --- | --- | --- | |  | a. | RAM slack | |  | b. | Edge slack | |  | c. | Drive file slack | |  | d. | Sector slack |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 30. What RAID type below utilizes parity data across all drives instead of using a separate drive to hold parity error checking information?   |  |  |  | | --- | --- | --- | |  | a. | RAID 0 | |  | b. | RAID 1 | |  | c. | RAID 2 | |  | d. | RAID 5 |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 31. What value refers to the average amount of time until a component fails, cannot be repaired, and must be replaced?   |  |  |  | | --- | --- | --- | |  | a. | average time between failures | |  | b. | mean time to recovery | |  | c. | mean time between failures | |  | d. | median time between failures |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 32. The goal of redundancy is to reduce what variable?   |  |  |  | | --- | --- | --- | |  | a. | average time between failures | |  | b. | mean time to recovery | |  | c. | median time to recovery | |  | d. | median time between failures |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 33. What RAID type is based on striping, uses multiple drives, and is not fault tolerant if one of the drives fails?   |  |  |  | | --- | --- | --- | |  | a. | RAID 0 | |  | b. | RAID 1 | |  | c. | RAID 2 | |  | d. | RAID 5 |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 34. What specific way can disaster recovery plans be tested?   |  |  |  | | --- | --- | --- | |  | a. | alternative processing | |  | b. | restoration simulation | |  | c. | tabletop exercises | |  | d. | alternative exercises |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 35. What type of assessment can determine if a system contains PII, whether a privacy impact assessment is required, and if any other privacy requirements apply to the IT system?   |  |  |  | | --- | --- | --- | |  | a. | privacy threshold | |  | b. | privacy impact | |  | c. | privacy availability | |  | d. | privacy identification |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 36. What type of planning do many enterprises participate in that addresses a future event or circumstance that might possibly occur but cannot be predicted with any certainty?   |  |  |  | | --- | --- | --- | |  | a. | contingency system evaluation | |  | b. | IT disaster planning | |  | c. | IT contingency planning | |  | d. | disaster recovery scenario |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 37. Which of the following is usually addressed in a disaster recovery plan? (Choose all that apply.)   |  |  |  | | --- | --- | --- | |  | a. | Purpose and Scope | |  | b. | Restoration Procedures | |  | c. | Recovery Team | |  | d. | Business Procedures |  |  |  | | --- | --- | | *ANSWER:* | a, b, c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 38. Which of the following is a system of hard drives based on redundancy and used for increased reliability and performance?   |  |  |  | | --- | --- | --- | |  | a. | MTBF | |  | b. | RPO | |  | c. | RAID | |  | d. | ESD |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 39. Which of the following is caused by a short-duration burst of energy by the source?   |  |  |  | | --- | --- | --- | |  | a. | electromagnetic interference | |  | b. | Faraday interference | |  | c. | electrostatic discharge | |  | d. | electromagnetic pulse |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 40. Which of the following is the sudden flow of electric current between two objects?   |  |  |  | | --- | --- | --- | |  | a. | electromagnetic interference | |  | b. | Faraday interference | |  | c. | electrostatic discharge | |  | d. | electromagnetic pulse |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |
| --- | --- | --- |
| 41. Describe the purpose of a disaster recovery plan.   |  |  | | --- | --- | | *ANSWER:* | A disaster recovery plan (DRP) is a written document that details the process for restoring IT resources following an event that causes a significant disruption in service. Comprehensive in its scope, a DRP is intended to be a detailed document that is updated regularly. | |

|  |  |  |
| --- | --- | --- |
| 42. What are the objectives of disaster exercises?   |  |  | | --- | --- | | *ANSWER:* | The objectives of disaster exercises are to test the efficiency of interdepartmental planning and coordination in managing a disaster, test current procedures of the DRP, and determine the strengths and weaknesses in responses. | |

|  |  |  |
| --- | --- | --- |
| 43. What are the steps in damage control?   |  |  | | --- | --- | | *ANSWER:* | Report the incident to security or the police. Confront any suspects (if the situation allows). Neutralize the suspected perpetrator from harming others (if necessary). Secure physical security features. Quarantine electronic equipment. Contact the response team. | |

|  |  |  |
| --- | --- | --- |
| 44. Explain how to best secure volatile data.   |  |  | | --- | --- | | *ANSWER:* | Securing volatile information can best be performed by capturing the entire system image, which is a snapshot of the current state of the computer that contains all current settings and data. | |

|  |  |  |
| --- | --- | --- |
| 45. Discuss the purpose and importance of the chain of custody.   |  |  | | --- | --- | | *ANSWER:* | The chain of custody documents that the evidence was under strict control at all times and no unauthorized person was given the opportunity to corrupt the evidence. A chain of custody includes documenting all of the serial numbers of the systems involved, who handled and had custody of the systems and for what length of time, how the computer was shipped, and any other steps in the process. In short, a chain of custody is a detailed document describing where the evidence was at all times. Gaps in this chain of custody can result in severe legal consequences. Courts have dismissed cases involving computer forensics because a secure chain of custody could not be verified. | |

|  |  |  |
| --- | --- | --- |
| 46. What do Windows computers do if a file being saved is not long enough to fill up the last sector on the disk?   |  |  | | --- | --- | | *ANSWER:* | When a file that is being saved is not long enough to fill up the last sector on a disk (a common occurrence because a file size only rarely matches the sector size), Windows pads the remaining cluster space with data that is currently stored in RAM. This padding creates RAM slack, which can contain any information that has been created, viewed, modified, downloaded, or copied since the computer was last booted. | |

|  |  |  |
| --- | --- | --- |
| 47. What is required upon completion of an evidence examination?   |  |  | | --- | --- | | *ANSWER:* | Upon completion of the examination, a detailed report is required that lists the steps that were taken and any evidence that was uncovered in the forensic investigation. | |

|  |  |  |
| --- | --- | --- |
| 48. Why should redundant networks be implemented in many enterprise environments?   |  |  | | --- | --- | | *ANSWER:* | Due to the critical nature of connectivity today, redundant networks also may be necessary. A redundant network waits in the background during normal operations and uses a replication scheme to keep its copy of the live network information current. If a disaster occurs, the redundant network automatically launches so that it is transparent to users. A redundant network ensures that network services are always accessible. | |

|  |  |  |
| --- | --- | --- |
| 49. Explain how an on-line UPS works and why their advantages when compared to off-line UPS units.   |  |  | | --- | --- | | *ANSWER:* | An on-line UPS is always running off its battery while the main power runs the battery charger. An advantage of an on-line UPS is that it is not affected by dips or sags in voltage. An on-line UPS can clean the electrical power before it reaches the server to ensure that a correct and constant level of power is delivered to the server. The on- line UPS also can serve as a surge protector, which keeps intense spikes of electrical current, common during thunderstorms, from reaching systems. | |

|  |  |  |
| --- | --- | --- |
| 50. What is a hot site?   |  |  | | --- | --- | | *ANSWER:* | hot site is generally run by a commercial disaster recovery service that allows a business to continue computer and network operations to maintain business continuity. A hot site is essentially a duplicate of the production site and has all the equipment needed for an organization to continue running, including office space and furniture, telephone jacks, computer equipment, and a live telecommunications link. Data backups of information can be quickly moved to the hot site, and in some instances the production site automatically synchronizes all its data with the hot site so that all data is immediately accessible. | |