|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 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 | |

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

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 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 | |

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

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |

|  |
| --- |
| 41. Describe the purpose of a disaster recovery plan. |

|  |
| --- |
| 42. What are the objectives of disaster exercises? |

|  |
| --- |
| 43. What are the steps in damage control? |

|  |
| --- |
| 44. Explain how to best secure volatile data. |

|  |
| --- |
| 45. Discuss the purpose and importance of the chain of custody. |

|  |
| --- |
| 46. What do Windows computers do if a file being saved is not long enough to fill up the last sector on the disk? |

|  |
| --- |
| 47. What is required upon completion of an evidence examination? |

|  |
| --- |
| 48. Why should redundant networks be implemented in many enterprise environments? |

|  |
| --- |
| 49. Explain how an on-line UPS works and why their advantages when compared to off-line UPS units. |

|  |
| --- |
| 50. What is a hot site? |