**崑山科技大學資工系IPAS證照輔導班 練習**

**名稱:** *Risk Management*

|  |  |  |
| --- | --- | --- |
|  | | |
| 答案 | 編號 | 題目 |
|  | 1. | You are a manager of a bank and you suspect one of your tellers has stolen money from their station. After talking with your supervisor, you place the employee on leave with pay, suspend their computer account, and obtain their proximity card and keys to the building. Which of the following policies did you follow ?  **A.** Mandatory vacations **B.** Exit interviews  **C.** Adverse actions **D.** Onboarding |
|  | 2. | Which of the following principles stipulates that multiple changes to a computer system should not be made at the same time?  **A.** Due diligence **B.** Acceptable use  **C.** Change management **D.** Due care |
|  | 3. | Why are penetration test often not advised?  **A.** It can be disruptive for the business activities.  **B.** It is able to measure and authenticate the efficiency of a company’s defensive mechanisms.  **C.** It’s able to find both known and unknown hardware or software weaknesses.  **D.** It permits the exploration of real risks and gives a precise depiction of a company’s IT infrastructure security posture at any given time. |
|  | 4. | You are a security engineer and discovered an employee using the company’s computer systems to operate their small business. The employee installed their personal software on the company’s computer and is using the computer hardware, such as the USB port. What policy would you recommend the company implement to prevent any risk of the company’s data and network being compromised?  **A.** Acceptable use policy **B.** Clean desk policy  **C.** Mandatory vacation policy **D.** Job rotation policy |
|  | 5. | What should be done to back up tapes that are stored off-site?  **A.** Generate a file hash for each backup file.  **B.** Scan the backup data for viruses.  **C.** Perform a chain of custody on the backup tape.  **D.** Encrypt the backup dat**A.** |
|  | 6. | Which recovery site is the easiest to test?  **A.** Warm site **B.** Cold site  **C.** Hot site **D.** Medium site |
|  | 7. | Katelyn is a network technician for a manufacturing company. She is testing a network forensic capturing software and plugs her laptop into an Ethernet switch port and begins capturing network traffic. Later she begins to analyze the data and notices some broadcast and multicast packets, as well as her own laptop’s network traffic. Which of the following statements best describes why Katelyn was unable to capture all network traffic on the switch?  **A.** Each port on the switch is an isolated broadcast domain.  **B.** Each port on the switch is an isolated collision domain.  **C.** Promiscuous mode must be enabled on the NI**C.**  **D.** Promiscuous mode must be disabled on the NI**C.** |
|  | 8. | Which of the following is not a step of the incident response process?  **A.** Snapshot **B.** Preparation  **C.** Recovery **D.** Containment |
|  | 9. | Which of the following is another term for technical controls?  **A.** Access controls **B.** Logical controls  **C.** Detective controls **D.** Preventive controls |
|  | 10. | You are a security manager for your company and need to reduce the risk of employees working in collusion to embezzle funds. Which of the following policies would you implement?  **A.** Mandatory vacations **B.** Clean desk  **C.** NDA **D.** Continuing education |
|  | 11. | You are a security administrator, and your manager has asked you about protecting the privacy of personally identifiable information (PII) that is collected. Which of the following would be the best option to fulfill the request?  **A.** PIA **B.** BIA  **C.** RTO **D.** SPF |
|  | 12. | Which of the following plans best identifies critical systems and components to ensure the assets are protected?  **A.** DRP **B.** BCP  **C.** IT contingency plan **D.** Succession plan |
|  | 13. | After your company implemented a clean desk policy, you have been asked to secure physical documents every night. Which of the following would be the best solution?  **A.** Department door lock **B.** Locking cabinets and drawers  **C.** Proximity card **D.** Onboarding |
|  | 14. | Your manager has instructed the team to test certain systems based on the business continuity plan to ensure they are operating properly. The manager wants to ensure there are no overlaps in the plan before implementing the test. Which continuity of operation planning concept is your manager referring to?  **A.** After-action report **B.** Failover  **C.** Eradication **D.** Tabletop exercise |
|  | 15. | Which of the following is an example of PHI?  **A.** Passport number **B.** Criminal record  **C.** Fingerprints **D.** Name of school attended |
|  | 16. | Which of the following techniques attempts to predict the likelihood a threat will occur and assigns monetary values should a loss occur?  **A.** Change management **B.** Vulnerability assessment  **C.** Qualitative risk assessment **D.** Quantitative risk assessment |
|  | 17. | Your competitors are offering a new service that is predicted to sell strong. After much careful research, your company has decided not to launch a competing service due to the uncertainty of the market and the enormous investment required. Which of the following best describes the company’s decision?  **A.** Risk transfer **B.** Risk avoidance  **C.** Risk acceptance **D.** Risk mitigation |
|  | 18. | Which of the following agreements is less formal than a traditional contract but still has a certain level of importance to all parties involved?  **A.** SLA **B.** BPA  **C.** ISA **D.** MOU |
|  | 19. | Your company is considering moving its mail server to a hosting company. This will help reduce hardware and server administrator costs at the local site. Which of the following documents would formally state the reliability and recourse if the reliability is not met?  **A.** MOU **B.** SLA  **C.** ISA **D.** BPA |
|  | 20. | You have an asset that is valued at $16,000, the exposure factor of a risk affecting that asset is 35%, and the annualized rate of occurrence if 75%. What is the SLE?  **A.** $5,600 **B.** $5,000  **C.** $4,200 **D.** $3,000 |
|  | 21. | During a meeting, you present management with a list of access controls used on your network. Which of the following controls is an example of a corrective control?  **A.** IDS **B.** Audit logs  **C.** Antivirus software **D.** Router |
|  | 22. | You are the new security administrator and have discovered your company lacks deterrent controls. Which of the following would you install that satisfies your needs? (Choose two.)  **A.** Lighting **B.** Motion sensor  **C.** No trespassing signs **D.** Antivirus scanner |
|  | 23. | Your company’s security policy includes system testing and security awareness training guidelines. Which of the following control types is this?  **A.** Detective technical control **B.** Preventive technical control  **C.** Detective administrative control **D.** Preventive administrative control |
|  | 24. | Which step of the incident response process occurs after containment? **A.** Preparation **B.** Recovery **C.** Identification **D.** Eradication |
|  | 25. | You are a security administrator for your company and you identify a security risk. You decide to continue with the current security plan. However, you develop a contingency plan in case the security risk occurs. Which of the following type of risk response technique are you demonstrating?  **A.** Accept **B.** Transfer  **C.** Avoid **D.** Mitigate |
|  | 26. | Which of the following best visually shows the state of a computer at the time it was collected by law enforcement?  **A.** Screenshots **B.** Identification  **C.** Tabletop exercise **D.** Generate hash values |
|  | 27. | You are asked to protect the company’s data should a complete disaster occur. Which action would be the best option for this request? **A.** Back up all data to tape, and store those tapes at an alternate location within the city.  **B.** Back up all data to tape, and store those tapes at an alternate location in another city.  **C.** Back up all data to disk, and store the disk in a safe in the company’s basement.  **D.** Back up all data to disk, and store the disk in a safe at the network administrator’s home. |
|  | 28. | Which of the following would not be a purpose of a privacy threshold analysis?  **A.** Identify programs and systems that are privacy-sensitive.  **B.** Demonstrate the inclusion of privacy considerations during the review of a program or system.  **C.** Identify systems that are considered a single point of failure.  **D.** Demonstrate compliance with privacy laws and regulations. |
|  | 29. | You have purchased new laptops for your salespeople. You plan to dispose of the hard drives of the former laptops as part of a company computer sale. Which of the following methods would you use to properly dispose of the hard drives?  **A.** Destruction **B.** Shredding  **C.** Purging **D.** Formatting |
|  | 30. | You are the head of the IT department of a school and are looking for a way to promote safe and responsible use of the Internet for students. With the help of the teachers, you develop a document for students to sign that describes methods of accessing the Internet on the school’s network. Which of the following best describes this document?  **A.** Service level agreement **B.** Acceptable use policy  **C.** Incident response plan **D.** Chain of custody |
|  | 31. | You are the security administrator and have discovered a malware incident. Which of the following responses should you do first?  **A.** Recovery **B.** Eradication **C.** Containment **D.** Identification |
|  | 32. | You are an IT administrator for a company and you are adding new employees to an organization’s identity and access management system. Which of the following best describes the process you are performing?  **A.** Onboarding **B.** Offboarding **C.** Adverse action **D.** Job rotation |
|  | 33. | Your company is partnering with another company and requires systems to be shared. Which of the following agreements would outline how the shared systems should be interfaced?  **A.** BPA **B.** MOU **C.** SLA **D.** ISA |
|  | 34. | Mark is an office manager at a local bank branch. He wants to ensure customer information isn’t compromised when the deskside employees are away from their desks for the day. What security concept would Mark use to mitigate this concern?  **A.** Clean desk **B.** Background checks  **C.** Continuing education **D.** Job rotation |
|  | 35. | You are a security administrator and advise the web development team to include a CAPTCHA on the web page where users register for an account. Which of the following controls is this referring to?  **A.** Deterrent **B.** Detective  **C.** Compensating **D.** Degaussing |
|  | 36. | Which of the following is *not* a common security policy type?  **A.** Acceptable use policy **B.** Social media policy  **C.** Password policy **D.** Parking policy |
|  | 37. | As the IT security officer, you are configuring data label options for your company’s research and development file server. Regular users can label documents as contractor, public, or internal. Which label should be assigned to company trade secrets?  **A.** High **B.** Top secret **C.** Proprietary **D.** Low |
|  | 38. | Users are currently accessing their personal email through company computers, so you and your IT team have created a security policy for email use. What is the next step after creating and approving the email use policy?  **A.** Encrypt all user email messages.  **B.** Provide security user awareness training.  **C.** Provide every employee with their own device to access their personal email.  **D.** Forward all personal emails to their company email account. |
|  | 39. | Which of the following is not a physical security control?  **A.** Motion detector **B.** Fence  **C.** Antivirus software **D.** CCTV |
|  | 40. | Which of the following might you find in a DRP?  **A.** Single point of failure  **B.** Prioritized list of critical computer systems  **C.** Exposure factor  **D.** Asset value |
|  | 41. | Your security manager wants to decide which risks to mitigate based on cost. What is this an example of?  **A.** Quantitative risk assessment **B.** Qualitative risk assessment  **C.** Business impact analysis **D.** Threat assessment |
|  | 42. | Your company has outsourced its proprietary processes to Acme Corporation. Due to technical issues, Acme Corporation wants to include a third-party vendor to help resolve the technical issues. Which of the following must Acme Corporation consider before sending data to the third party?  **A.** This data should be encrypted before it is sent to the third-party vendor.  **B.** This may constitute unauthorized data sharing.  **C.** This may violate the privileged user role-based awareness training. **D.** This may violate a nondisclosure agreement. |
|  | 43. | Zack is a security administrator who has been given permission to run a vulnerability scan on the company’s wireless network infrastructure. The results show TCP ports 21 and 23 open on most hosts. What port numbers do these refer to? (Choose two.)  **A.** FTP **B.** SMTP **C.** Telnet **D.** DNS |
|  | 44. | Which of the following backup concepts is the quickest backup but slowest restore?  **A.** Incremental **B.** Differential **C.** Full **D.** Snapshots |
|  | 45. | Which of the following operations should you undertake to avoid mishandling of tapes, removal drives, CDs, and DVDs?  **A.** Degaussing **B.** Acceptable use  **C.** Data labeling **D.** Wiping |
|  | 46. | Which of the following can be classified as a single point of failure?  **A.** Failover **B.** A cluster  **C.** Load balancing **D.** A configuration |
|  | 47. | Which of the following are considered detective controls?  **A.** Closed-circuit television (CCTV) **B.** Guard  **C.** Firewall **D.** IPS |
|  | 48. | Your CIO wants to move the company’s large sets of sensitive data to an SaaS cloud provider to limit the storage and infrastructure costs. Both the cloud provider and the company are required to have a clear understanding of the security controls that will be applied to protect the sensitive data. What type of agreement would the SaaS cloud provider and your company initiate?  **A.** MOU **B.** BPA **C.** SLA **D.** ISA |
|  | 49. | . Which of the following is typically included in a BPA?  **A.** Clear statements detailing the expectation between a customer and a service provider  **B.** The agreement that a specific function or service will be delivered at the agreed-upon level of performance  **C.** Sharing of profits and losses and the addition or removal of a partner  **D.** Security requirements associated with interconnecting IT systems |
|  | 50. | Your team powered off the SQL database server for over 7 hours to perform a test. Which of the following is the most likely reason for this?  **A.** Business impact analysis **B.** Succession plan  **C.** Continuity of operations plan **D.** Service level agreement |
|  | 51. | Which of the following role-based positions should receive training on how to manage a particular system?  **A.** Users **B.** Privileged users  **C.** Executive users **D.** System owners |
|  | 52. | You maintain a network of 150 computers and must determine which hosts are secure and which are not. Which of the following tools would best meet your need?  **A.** Vulnerability scanner **B.** Protocol analyzer  **C.** Port scanner **D.** Password cracker |
|  | 53. | You have been instructed to introduce an affected system back into the company’s environment and be sure that it will not lead to another incident. You test, monitor, and validate that the system is not being compromised by any other means. Which of the incident response processes have you completed?  **A.** Lessons learned **B.** Preparation  **C.** Recovery **D.** Containment |
|  | 54. | You discover that an investigator made a few mistakes during a recent forensic investigation. You want to ensure the investigator follows the appropriate process for the collection, analysis, and preservation of evidence. Which of the following terms should you use for this process?  **A.** Incident handling **B.** Legal hold  **C.** Order of volatility **D.** Chain of custody |
|  | 55. | You receive a call from the help desk manager stating that there has been an increase in calls from users reporting their computers are infected with malware. Which of the following incident response steps should be completed first?  **A.** Containment **B.** Eradication  **C.** Lessons learned **D.** Identification |
|  | 56. | Which of the following are examples of custodian security roles? (Choose two.)  **A.** Human resources employee **B.** Sales executive  **C.** CEO **D.** Server backup operator |
|  | 57. | You are the network administrator of your company, and the manager of a retail site located across town has complained about the loss of power to their building several times this year. The branch manager is asking for a compensating control to overcome the power outage. What compensating control would you recommend?  **A.** Firewall **B.** Security guard  **C.** IDS **D.** Backup generator |
|  | 58. | James is a security administrator and is attempting to block unauthorized access to the desktop computers within the company’s network. He has configured the computers’ operating systems to lock after 5 minutes of no activity. What type of security control has James implemented?  **A.** Preventive **B.** Corrective  **C.** Deterrent **D.** Detective |
|  | 59. | Which of the following terms best describes sensitive medical information?  **A.** AES **B.** PHI **C.** PII **D.** TLS |
|  | 60. | An accounting employee changes roles with another accounting employee every 4 months. What is this an example of?  **A.** Separation of duties **B.** Mandatory vacation  **C.** Job rotation **D.** Onboarding |
|  | 61. | Which of the following are considered inappropriate places to store backup tapes? (Choose two.)  **A.** Near a workstation **B.** Near a speaker  **C.** Near a CRT monitor **D.** Near an LCD screen |
|  | 62. | You are a member of your company’s security response team and have discovered an incident within your network. You are instructed to remove and restore the affected system. You restore the system with the original disk image and then install patches and disable any unnecessary services to harden the system against any future attacks. Which incident response process have you completed?  **A.** Eradication **B.** Preparation  **C.** Containment **D.** Recovery |
|  | 63. | You are a security administrator and have decided to implement a unified threat management (UTM) appliance within your network. This appliance will provide antimalware, spam filtering, and content inspection along with other protections. Which of the following statements best describes the potential problem with this plan?  **A.** The protections can only be performed one at a time.  **B.** This is a complex plan because you will manage several complex platforms.  **C.** This could create the potential for a single point of failure.  **D.** You work with a single vendor and its support department. |
|  | 64. | You are attending a risk analysis meeting and are asked to define internal threats. Which of the following is not considered an internal threat?  **A.** Employees accessing external websites through the company’s hosts **B.** Embezzlement  **C.** Threat actors compromising a network through a firewall  **D.** Users connecting a personal USB thumb drive to a workstation |
|  | 65. | You are the network director and are creating the following year’s budget. You submit forensic dollar amounts for the cyber incident response team. Which of the following would you not submit? (Choose two.)  **A.** ALE amounts **B.** SLE amounts  **C.** Training expenses **D.** Man-hour expenses |
|  | 66. | Computer evidence of a crime is preserved by making an exact copy of the hard disk. Which of the following does this demonstrate?  **A.** Chain of custody **B.** Order of volatility  **C.** Capture system image **D.** Taking screenshots |
|  | 67. | Which option is an example of a workstation not hardened?  **A.** Risk **B.** Threat **C.** Exposure **D.** Mitigate |
|  | 68. | Which of the following elements should not be included in the preparation phase of the incident response process?  **A.** Policy **B.** Lesson learned documentation  **C.** Response plan/strategy **D.** Communication |
|  | 69. | Which of the following does not minimize security breaches committed by internal employees?  **A.** Job rotation  **B.** Separation of duties  **C.** Nondisclosure agreements signed by employees  **D.** Mandatory vacations |
|  | 70. | You find one of your employees posting negative comments about the company on Facebook and Twitter. You also discover the employee is sending negative comments from their personal email on the company’s computer. You are asked to implement a policy to help the company avoid any negative reputation in the marketplace. Which of the following would be the best option to fulfill the request?  **A.** Account policy enforcement **B.** Change management  **C.** Security policy **D.** Risk assessment |
|  | 71. | Which of the following statements best describes a differential backup?  **A.** Only the changed portions of files are backed up.  **B.** All files are copied to storage media.  **C.** Files that have changed since the last full backup are backed up.  **D.** Only files that have changed since the last full or incremental backup are backed up. |
|  | 72. | During which step of the incident response process does root cause analysis occur?  **A.** Preparation **B.** Lessons learned  **C.** Containment **D.** Recovery |
|  | 73. | Which of the following types of testing can help identify risks? (Choose two.)  **A.** Quantitative **B.** Penetration testing  **C.** Vulnerability testing **D.** Qualitative |
|  | 74. | What can a company do to prevent sensitive data from being retrieved by dumpster diving?  **A.** Degaussing **B.** Capture system image  **C.** Shredding **D.** Wiping |
|  | 75. | You are a network administrator and have been asked to send a large file that contains PII to an accounting firm. Which of the following protocols would it be best to use?  **A.** Telnet **B.** FTP **C.** SFTP **D.** SMTP |
|  | 76. | Zackary is a network backup engineer and performs a full backup each Sunday evening and an incremental backup Monday through Friday evenings. One of the company’s network servers crashes on Thursday afternoon. How many backups will Zack need to do to restore the server?  **A.** Two **B.** Three **C.** Four **D.** Five |
|  | 77. | Your company website is hosted by an Internet service provider. Which of the following risk response techniques is in use?  **A.** Risk avoidance **B.** Risk register  **C.** Risk acceptance **D.** Risk mitigation |
|  | 78. | A call center leases a new space across town, complete with a functioning computer network that mirrors the current live site. A high-speed network link continuously synchronizes data between the two sites. Which of the following describes the site at the new leased location?  **A.** Cold site **B.** Warm site  **C.** Hot site **D.** Differential site |
|  | 79. | A security administrator is reviewing the company’s continuity plan, and it specifies an RTO of 4 hours and an RPO of 1 day. Which of the following is the plan describing?  **A.** Systems should be restored within 1 day and should remain operational for at least 4 hours.  **B.** Systems should be restored within 4 hours and no later than 1 day after the incident.  **C.** Systems should be restored within 1 day and lose, at most, 4 hours’ worth of data.  **D.** Systems should be restored within 4 hours with a loss of 1 day’s worth of data at most. |
|  | 80. | Which of the following statements is true regarding a data retention policy?  **A.** Regulations require financial transactions to be stored for 7 years.  **B.** Employees must remove and lock up all sensitive and confidential documents when not in use.  **C.** It describes a formal process of managing configuration changes made to a network.  **D.** It is a legal document that describes a mutual agreement between parties. |
|  | 81. | You are attending a meeting with your manager and he wants to validate the cost of a warm site versus a cold site. Which of the following reasons best justify the cost of a warm site? (Choose two.)  **A.** Small amount of income loss during long downtime  **B.** Large amount of income loss during short downtime  **C.** Business contracts enduring no more than 72 hours of downtime  **D.** Business contracts enduring no more than 8 hours of downtime |
|  | 82. | Recently, company data that was sent over the Internet was intercepted and read by hackers. This damaged the company’s reputation with its customers. You have been asked to implement a policy that will protect against these attacks. Which of the following options would you choose to help protect data that is sent over the Internet? (Choose two.)  **A.** Confidentiality **B.** Safety  **C.** Availability **D.** Integrity |
|  | 83. | How do you calculate the annual loss expectancy (ALE) that may occur due to a threat?  **A.** Exposure Factor (EF) / Single Loss Expectancy (SLE)  **B.** Single Loss Expectancy (SLE) × Annual Rate of Occurrence (ARO)  **C.** Asset Value (AV) × Exposure Factor (EF)  **D.** Single Loss Expectancy (SLE) / Exposure Factor (EF) |
|  | 84. | Which of the following impact scenarios would include severe weather events? (Choose two.)  **A.** Life **B.** Reputation **C.** Salary **D.** Property |
|  | 85. | Which of the following outlines a business goal for system restoration and allowable data loss?  **A.** RPO **B.** Single point of failure  **C.** MTTR **D.** MTBF |
|  | 86. | Which of the following is an example of a preventive control? (Choose two.)  **A.** Data backups **B.** Security camera  **C.** Door alarm **D.** Cable locks |
|  | 87. | You are a security administrator for your company and you identify a security risk that you do not have in-house skills to address. You decide to acquire contract resources. The contractor will be responsible for handling and managing this security risk. Which of the following type of risk response technique are you demonstrating?  **A.** Accept **B.** Mitigate **C.** Transfer **D.** Avoid |
|  | 88. | You are an IT manager and discovered your department had a break-in, and the company’s computers were physically damaged. What type of impact best describes this situation?  **A.** Life **B.** Reputation **C.** Property **D.** Safety |
|  | 89. | Which of the following would help build informed decisions regarding a specific DRP?  **A.** Business impact analysis **B.** ROI analysis  **C.** RTO **D.** Life impact |
|  | 90. | Each salesperson who travels has a cable lock to lock down their laptop when they step away from the device. Which of the following controls does this apply?  **A.** Administrative **B.** Compensating  **C.** Deterrent **D.** Preventive |
|  | 91. | Which of the following secures access to company data in agreement to management policies?  **A.** Technical controls **B.** Administrative controls  **C.** HTTPS **D.** Integrity |
|  | 92. | You are a server administrator for your company’s private cloud. To provide service to employees, you are instructed to use reliable hard disks in the server to host a virtual environment. Which of the following best describes the reliability of hard drives?  **A.** MTTR **B.** RPO **C.** MTBF **D.** ALE |
|  | 93. | You are replacing a number of devices with a mobile appliance that combines several functions. Which of the following describes the new implementation?  **A.** Cloud computing **B.** Load balancing  **C.** Single point of failure **D.** Virtualization |
|  | 94. | Which of the following can help mitigate adware intrusions?  **A.** Antivirus **B.** Antispam  **C.** Spyware **D.** Pop-up blocker |
|  | 95. | . In the initial stages of a forensics investigation, Zack, a security administrator, was given the hard drive of the compromised workstation by the incident manager. Which of the following data acquisition procedures would Zack need to perform in order to begin the analysis? (Choose two.)  **A.** Take hashes **B.** Take screenshots  **C.** Capture the system image **D.** Start the order of volatility |
|  | 96. | Which of the following best describes a Computer Incident Response Team (CIRT)?  **A.** Personnel who participate in exercises to practice incident response procedures  **B.** Personnel who promptly and correctly handle incidents so they can be quickly contained, investigated, and recovered from  **C.** A team to identify planning flaws before an actual incident occurs **D.** Team members using a walk-through checklist to ensure understanding of roles in a DRP |
|  | 97. | Which of the following decreases the success of brute-force attacks? **A.** Password complexity **B.** Password hints  **C.** Account lockout threshold **D.** Enforce password history |
|  | 98. | A warrant has been issued to investigate a file server that is suspected to be part of an organized crime to steal credit card information. You are instructed to follow the order of volatility. Which data would you collect first?  **A.** RAM **B.** USB flash drive **C.** Hard disk **D.** Swap files |
|  | 99. | What should human resources personnel be trained in regarding security policies?  **A.** Guidelines and enforcement **B.** Order of volatility  **C.** Penetration assessment **D.** Vulnerability assessment |
|  | 100. | Which of the following is not a basic concept of computer forensics? **A.** Preserve evidence  **B.** Determine if the suspect is guilty based on the findings  **C.** Track man-hours and expenses  **D.** Interview all witnesses |
|  | 101. | The Chief Information Officer (CIO) wants to set up a redundant server location so that the production server images can be moved within 36 hours and the servers can be restored quickly, should a catastrophic failure occur at the primary location. Which of the following can be implemented?  **A.** Hot site **B.** Cold site **C.** Warm site **D.** Load balancing |
|  | 102. | Choose the correct order of volatility when collecting digital evidence. **A.** Hard disk drive, DVD-R, RAM, swap file  **B.** Swap file, RAM, DVD-R, hard disk drive  **C.** RAM, DVD-R, swap file, hard disk drive  **D.** RAM, swap file, hard disk drive, DVD-R |
|  | 103. | Which of the following pieces of information would be summarized in the lessons learned phase of the incident response process? (Choose three.)  **A.** When the problem was first detected and by whom  **B.** How the problem was contained and eradicated  **C.** The work that was performed during the recovery  **D.** Preparing a company’s team to be ready to handle an incident at a moment’s notice |
|  | 104. | You receive a phone call from an employee reporting that their workstation is acting strangely. You gather information from the intrusion detection system and notice unusual network traffic from the workstation, and you determine the event may be an incident. You report the event to your manager, who then begins to collect evidence and prepare for the next steps. Which phase of the incident response process is this?  **A.** Preparation **B.** Identification  **C.** Containment **D.** Eradication |
|  | 105. | Your manager has asked you to recommend a way to transmit PII via email and maintain its confidentiality. Which of the following options is the best solution?  **A.** Hash the information before sending.  **B.** Protect the information with a digital signature.  **C.** Protect the information by using RAI**D.**  **D.** Encrypt the information before sending. |
|  | 106. | Which of the following statements best defines change management? **A.** Responding to, containing, analyzing, and recovering from a computer-related incident  **B.** Means used to define which access permissions subjects have for a specific object  **C.** Procedures followed when configuration changes are made to a network  **D.** Categorizing threats and vulnerabilities and their potential impacts to a network |
|  | 107. | During which step of the incident response process does identification of incidents that can be prevented or mitigated occur?  **A.** Containment **B.** Eradication  **C.** Preparation **D.** Lessons learned |
|  | 108. | Which of the following best describes the disadvantages of quantitative risk analysis compared to qualitative risk analysis? (Choose two.)  **A.** Quantitative risk analysis requires complex calculations.  **B.** Quantitative risk analysis is sometimes subjective.  **C.** Quantitative risk analysis is generally scenario-based.  **D.** Quantitative risk analysis is more time-consuming than qualitative risk analysis. |
|  | 109. | Which of the following are disadvantages of using a cold site? (Choose two.)  **A.** Expense **B.** Recovery time  **C.** Testing availability **D.** Administration time |
|  | 110. | Which of the following policies should be implemented to minimize data loss or theft?  **A.** Password policy **B.** PII handling  **C.** Chain of custody **D.** Detective control |
|  | 111. | . Which of the following should a comprehensive data policy include? **A.** Wiping, disposing, storage, retention  **B.** Disposing, patching, storage, retention  **C.** Storage, retention, virtualization  **D.** Onboarding, storage, disposing |
|  | 112. | You have revealed a recent intrusion within the company’s network and have decided to execute incident response procedures. The incident response team has identified audit logs that hold information about the recent security breach. Prior to the incident, a security consultant firm recommended that your company install a NTP server within the network. Which of the following is a setback the incident response team will likely encounter during the assessment?  **A.** Order of volatility **B.** Chain of custody  **C.** Eradication **D.** Record time offset |
|  | 113. | You plan to provide a word processing program to the employees in your company. You decide not to install the program on each employee’s workstation but rather have a cloud service provider host the application. Which of the following risk response techniques best describes the situation?  **A.** Risk mitigation **B.** Risk acceptance  **C.** Risk avoidance **D.** Risk transfer |
|  | 114. | Which of the following statements is true about incremental backup? **A.** It backs up all files.  **B.** It backs up all files in a compressed format.  **C.** It backs up all new files and any files that have changed since the last full backup without resetting the archive bit.  **D.** It backs up all new files and any files that have changed since the last full or incremental backup and resets the archive bit. |
|  | 115. | The chief security officer (CSO) has seen four security breaches during the past 2 years. Each breach cost the company $30,000, and a third-party vendor has offered to repair the security weakness in the system for $250,000. The breached system is set to be replaced in 5 years. Which of the following risk response techniques should the CSO use?  **A.** Accept the risk. **B.** Transfer the risk.  **C.** Avoid the risk. **D.** Mitigate the risk. |
|  | 116. | Which of the following would not be a guideline for performing a BIA? **A.** Identify impact scenarios that put your business operations at risk. **B.** Identify mission-essential functions and the critical systems within each function.  **C.** Approve and execute changes in order to ensure maximum security and availability of IT services.  **D.** Calculate RPO, RTO, MTTR, and MTBF |
|  | 117. | . You are a network administrator and have purchased two devices that will work as failovers for each other. Which of the following does this best demonstrate?  **A.** Integrity **B.** Availability  **C.** Authentication **D.** Confidentiality |
|  | 118. | Your company has lost power and the salespeople cannot take orders because the computers and phone systems are unavailable. Which of the following would be the best options to an alternate business practice? (Choose two.)  **A.** Tell the salespeople to go home for the day until the power is restored.  **B.** Tell the salespeople to use their cell phones until the power is restored.  **C.** Have the salespeople use paper and pen to take orders until the power is restored.  **D.** Have the salespeople instruct customers to fax their orders until the power is restored. |
|  | 119. | Leigh Ann is the new network administrator for a local community bank. She studies the current file server folder structures and permissions. The previous administrator didn’t properly secure customer documents in the folders. Leigh Ann assigns appropriate file and folder permissions to be sure that only the authorized employees can access the data. What security role is Leigh Ann assuming?  **A.** Power user **B.** Data owner  **C.** User **D.** Custodian |
|  | 120. | Which of the following methods is not recommended for removing data from a storage media that is used to store confidential information?  **A.** Formatting **B.** Shredding  **C.** Wiping **D.** Degaussing |
|  | 121. | A SQL database server is scheduled for full backups on Sundays at 2:00 a.m. and incremental backups each weeknight at 11:00 p.m. Write verification is enabled, and backup tapes are stored off-site at a bank safety deposit box. Which of the following should be completed to ensure integrity and confidentiality of the backups? (Choose two.) **A.** Use SSL to encrypt the backup data.  **B.** Encrypt the backup data before it is stored off-site.  **C.** Ensure that an employee other than the backup operator analyzes each day’s backup logs.  **D.** Ensure that the employee performing the backup is a member of the administrators’ group. |
|  | 122. | You are planning to perform a security audit and would like to see what type of network traffic is transmitting within your company’s network. Which of the following tools would you use?  **A.** Port scanner **B.** Vulnerability scanner  **C.** Protocol analyzer **D.** Network intrusion detection system |
|  | 123. | Your company has hired a new administrative assistant to a commercial lender named Leigh Ann. She will be using a web browser on a company computer at the office to access internal documents on a public cloud provider over the Internet. Which type of document should Leigh Ann read and sign?  **A.** Internet acceptable use policy **B.** Audit policy  **C.** Password policy **D.** Privacy policy |
|  | 124. | During a conversation with another colleague, you suggest there is a single point of failure in the single load balancer in place for the company’s SQL server. You suggest implementing two load balancers in place with only one in service at a given time. What type of load balancing configuration have you described?  **A.** Active-active **B.** Active directory  **C.** Round robin **D.** Active-passive |
|  | 125. | Which of the following policies would you implement to help prevent the company’s users from revealing their login credentials for others to view?  **A.** Job rotation **B.** Data owner  **C.** Clean desk **D.** Separation of duties |
|  | 126. | Which of the following are part of the chain of custody?  **A.** Delegating evidence collection to your manager  **B.** Capturing the system image to another hard drive  **C.** Capturing memory contents before capturing hard disk contents  **D.** Preserving, protecting, and documenting evidence |
|  | 127. | Zackary has been assigned the task of performing a penetration test on a server and was given limited information about the inner workings of the server. Which of the following tests will he be performing?  **A.** White box **B.** Gray box **C.** Black box **D.** Clear box |
|  | 128. | Which of the following are considered administrative controls? (Choose two.)  **A.** Firewall rules **B.** Personnel hiring policy  **C.** Separation of duties **D.** Intrusion prevention system |
|  | 129. | Which of the following are examples of alternate business practices? (Choose two.)  **A.** The business’s point-of-sale terminal goes down, and employees use pen and paper to take orders and a calculator to determine customers’ bills.  **B.** The network system crashes due to an update, and employees are told to take time off until the company’s network system is restored.  **C.** Power is lost at a company’s site and the manager posts a closed sign until power is restored.  **D.** A bank location has lost power, and the employees are sent to another location to resume business. |
|  | 130. | Which of the following require careful handling and special policies for data retention and distribution? (Choose two.)  **A.** Personal electronic devices **B.** MOU  **C.** PII **D.** NDA |
|  | 131. | Matt is the head of IT security for a university department. He recently read articles about security breaches that involved malware on USB removable devices and is concerned about future incidents within the university. Matt reviews the past incident responses to determine how these occurrences may be prevented and how to improve the past responses. What type of document should Matt prepare?  **A.** MOU **B.** SLA  **C.** After-action report **D.** Nondisclosure agreement |
|  | 132. | Categorizing residual risk is most important to which of the following risk response techniques?  **A.** Risk mitigation **B.** Risk acceptance  **C.** Risk avoidance **D.** Risk transfer |
|  | 133. | You are the IT manager and one of your employees asks who assigns data labels. Which of the following assigns data labels?  **A.** Owner **B.** Custodian  **C.** Privacy officer **D.** System administrator |
|  | 134. | Which of the following is the most pressing security concern related to social media networks?  **A.** Other users can view your MAC address.  **B.** Other users can view your IP address.  **C.** Employees can leak a company’s confidential information.  **D.** Employees can express their opinion about their company. |
|  | 135. | You are a network administrator looking to test patches quickly and often before pushing them out to the production workstations. Which of the following would be the best way to do this?  **A.** Create a full disk image to restore the system after each patch installation.  **B.** Create a virtual machine and utilize snapshots.  **C.** Create an incremental backup of an unpatched workstation.  **D.** Create a differential backup of an unpatched workstation. |
|  | 136. | You have instructed your junior network administrator to test the integrity of the company’s backed-up data. Which of the following is the best way to test the integrity of a backup?  **A.** Review written procedures.  **B.** Use software to recover deleted files.  **C.** Restore part of the backup.  **D.** Conduct another backup. |
|  | 137. | What concept is being used when user accounts are created by one employee and user permissions are configured by another employee? **A.** Background checks **B.** Job rotation  **C.** Separation of duties **D.** Collusion |
|  | 138. | Your company is requesting the installation of a fence around the property and cipher locks on all front entrances. Which of the following concepts is your company concerned about?  **A.** Confidentiality **B.** Integrity  **C.** Availability **D.** Safety |
|  | 139. | Which of the following is an example of a vulnerability assessment tool?  **A.** Ophcrack **B.** John the Ripper  **C.** L0phtCrack **D.** Nessus |
|  | 140. | A security analyst is analyzing the cost the company could incur if the customer database was breached. The database contains 2,500 records with PII. Studies show the cost per record would be $300. The likelihood that the database would be breached in the next year is only 5%. Which of the following would be the ALE for a security breach?  **A.** $15,000 **B.** $37,500 **C.** $150,000 **D.** $750,000 |
|  | 141. | Your team must perform a test of a specific system to be sure the system operates at the alternate site. The results of the test must be compared with the company’s live environment. Which test is your team performing?  **A.** Cutover test **B.** Walk-through  **C.** Parallel test **D.** Simulation |
|  | 142. | Which of the following concepts defines a company goal for system restoration and acceptable data loss?  **A.** MTBF **B.** MTTR **C.** RPO **D.** ARO |
|  | 143. | Your IT team has created a disaster recovery plan to be used in case a SQL database server fails. What type of control is this?  **A.** Detective **B.** Corrective  **C.** Preventive **D.** Deterrent |
|  | 144. | Which of the following is not a step in the incident response process? **A.** Snapshot **B.** Preparation  **C.** Recovery **D.** Containment |
|  | 145. | Which of the following threats is mitigated by shredding paper documents?  **A.** Shoulder surfing **B.** Physical  **C.** Adware **D.** Spyware |
|  | 146. | Your company hires a third-party auditor to analyze the company’s data backup and long-term archiving policy. Which type of organization document should you provide to the auditor?  **A.** Clean desk policy **B.** Acceptable use policy  **C.** Security policy **D.** Data retention policy |
|  | 147. | You are a network administrator and have been given the duty of creating users accounts for new employees the company has hired. These employees are added to the identity and access management system and assigned mobile devices. What process are you performing?  **A.** Offboarding **B.** System owner  **C.** Onboarding **D.** Executive user |
|  | 148. | Which of the following defines a standard operating procedure (SOP)? (Choose three.)  **A.** Standard **B.** Privacy **C.** Procedure **D.** Guideline |
|  | 149. | Computer equipment was suspected to be involved in a computer crime and was seized. The computer equipment was left unattended in a corridor for 10 minutes while officers restrained a potential suspect. The seized equipment is no longer admissible as evidence because of which of the following violations?  **A.** Chain of custody **B.** Order of volatility  **C.** Preparation **D.** Eradication |
|  | 150. | Which of the following should be performed when conducting a qualitative risk analysis? (Choose two.)  **A.** ARO **B.** SLE  **C.** Asset estimation **D.** Rating potential threats |