**Chapter 9 - Business Continuity Planning Answers**

1. Which of the following provides coordinated procedures for minimizing loss of life or injury and protecting property damage in response to a physical threat?
   1. Business continuity plan
   2. Incident response plan
   3. Disaster recovery plan
   4. Occupant emergency plan
2. Which of the following statements pertaining to the maintenance of an IT contingency plan is incorrect?
   1. The plan should be reviewed at least once a year for accuracy and completeness.
   2. The Contingency Planning Coordinator should make sure that every employee gets an up-to-date copy of the plan.
   3. Strict version control should be maintained.
   4. Copies of the plan should be provided to recovery personnel for storage at home and office.
3. If your property Insurance has Replacement Cost Valuation (RCV) clause, your damaged property will be compensated:
   1. Based on the value of item on the date of loss
   2. Based on new item for old, regardless of condition of lost item
   3. Based on value of item one month before the loss
   4. Based on value of item on the date of loss plus 10 percent
4. Which of the following is NOT a transaction redundancy implementation?
   1. on-site mirroring
   2. electronic vaulting
   3. remote journaling
   4. database shadowing
5. Valuable paper insurance coverage does not cover damage to which of the following?
   1. Inscribed, printed and Written documents
   2. Manuscripts
   3. Records
   4. Money and Securities
6. A business impact assessment is one element in business continuity planning. What are the three primary goals of a BIA?
   1. Data processing continuity planning, data recovery plan maintenance, and testing the disaster recovery plan.
   2. Scope and plan initiation, business continuity plan development, and plan approval and implementation.
   3. Facility requirements planning, facility security management, and administrative personnel controls.
   4. Criticality prioritization, downtime estimation, and resource requirements.
7. Which of the following focuses on sustaining an organization's business functions during and after a disruption?
   1. Business continuity plan
   2. Business recovery plan
   3. Continuity of operations plan
   4. Disaster recovery plan
8. Which of the following statements pertaining to disaster recovery planning is incorrect?
   1. Every organization needs a disaster recovery plan
   2. A disaster recovery plan contains actions to be taken before, during and after a disruptive even.
   3. The major goal of disaster recovery planning is to provide an organized way to make decisions if a disruptive event occurs.
   4. A disaster recovery plan should cover return from alternate facilities to primary facilities.
9. Which backup type has the quickest backup time?
   1. Full Backup
   2. Differential Backup
   3. Incremental Backup
   4. Disk Mirroring
10. Which of the following specifically addresses cyber attacks against an organization's IT systems?
    1. Continuity of support plan
    2. Business continuity plan
    3. Incident response plan
    4. Continuity of operations plan
11. System reliability is increased by:
    1. A lower MTBF and a lower MTTR.
    2. A higher MTBF and a lower MTTR.
    3. A lower MTBF and a higher MTTR.
    4. A higher MTBF and a higher MTTR.
12. What can be defined as a batch process of dumping backup data through communications lines to a server at an alternate location?
    1. Remote journaling
    2. Electronic vaulting
    3. Data clustering
    4. Database shadowing
13. Which of the following best describes remote journaling?
    1. Send hourly tapes containing transactions off-site.
    2. Send daily tapes containing transactions off-site.
    3. Real-time capture of transactions to multiple storage devices.
    4. Parallel processing of transactions to an alternate site.
14. During the course of a Business Impact Analysis (BIA) you will less likely:
    1. Estimate the financial and operational impacts of a disruption.
    2. Identify regulatory exposure.
    3. Determine a function's Recovery Time Objective (RTO).
    4. Determine the impact upon the organization's market share and corporate image.
15. Business continuity plan development depends most on:
    1. Directives of Senior Management
    2. Business Impact Analysis (BIA)
    3. Scope and Plan Initiation
    4. Skills of BCP committee
16. Emergency actions are taken at the incipient stage of a disaster with the objectives of preventing injuries or loss of life and of:
    1. determining the extent of property damage.
    2. protecting evidence.
    3. preventing looting and further damage.
    4. mitigating the damage to avoid the need for recovery.
17. What assesses potential loss that could be caused by a disaster?
    1. The Business Assessment (BA)
    2. The Business Impact Analysis (BIA)
    3. The Risk Assessment (RA)
    4. The Business Continuity Plan (BCP)
18. Which of the following server contingency solutions offers the highest availability?
    1. System backups
    2. Electronic vaulting/remote journaling
    3. Redundant arrays of independent disks (RAID)
    4. Load balancing/disk replication
19. Which of the following steps should be performed first in a business impact analysis (BIA)?
    1. Identify all business units within the organization.
    2. Evaluate the impact of disruptive events.
    3. Estimate the Recovery Time Objectives (RTO).
    4. Evaluate the criticality of business functions.
20. When preparing a business continuity plan, who of the following is responsible for identifying and prioritizing time-critical systems?
    1. Executive management staff
    2. Senior business unit management
    3. BCP committee
    4. Functional business units
21. Organizations should not view disaster recovery as which of the following?
    1. committed expense
    2. discretionary expense
    3. enforcement of legal statutes
    4. compliance with regulations
22. Prior to a live disaster test, which of the following is most important?
    1. Restore all files in preparation for the test.
    2. Document expected findings.
    3. Arrange physical security for the test site.
    4. Conduct a successful structured walk-through.
23. Which of the following is used to help business units understand the impact of a disruptive event?
    1. A risk analysis
    2. A business impact assessment
    3. A vulnerability assessment
    4. A disaster recovery plan
24. Who should direct short-term recovery actions immediately following a disaster?
    1. Chief Information Officer
    2. Chief Operating Officer
    3. Disaster Recovery Manager
    4. Chief Executive Officer
25. Which of the following could lead to the conclusion that the disaster recovery plan may not be operational within the timeframe the business needs to recover?
    1. The alternate site is a warm site.
    2. Critical recovery priority levels are not defined
    3. Offsite backups are located away from the alternate site.
    4. The alternate site is located 70 miles away from the primary site
26. Of the following, which is not a specific loss criteria that should be considered while developing a BIA?
    1. Loss of skilled workers knowledge
    2. Loss in revenue
    3. Loss in profits
    4. Loss in reputation
27. Which of the following is the most important consideration in locating an alternate computing facility during the development of a disaster recovery plan?
    1. It is unlikely to be affected by the same contingency.
    2. It is close enough to become operational quickly.
    3. It is close enough to serve its users.
    4. It is convenient to airports and hotels.
28. Which of the following actions would be most appropriate after discovering that an organization's business continuity plan provides for an alternate processing site which will accommodate fifty percent of the primary processing facility's processing capability?
    1. Do nothing, because generally, less than twenty five percent of all processing is critical to an organizations survival and the backup capacity is therefore adequate.
    2. Identify applications that could be processed at the alternate site and develop manual procedures to back up other processing.
    3. Ensure that critical applications have been identified and that the alternate site could process all such applications.
    4. Recommend that the information processing facility arrange for an alternate processing site with the capacity to handle at least seventy five percent of normal processing.
29. Qualitative loss resulting from the business interruption does not include:
    1. Loss of revenue
    2. Loss of competitive advantage or market share
    3. Loss of public confidence and credibility
    4. Public embarrassment
30. During Recovery, which of following is most critical?
    1. Data
    2. Hardware/Software
    3. Communication Links
    4. Software Applications
31. Which of the following is covered under Crime Insurance Policy Coverage?
    1. Inscribed, printed and Written documents
    2. Manuscripts
    3. Account Receiveble
    4. Money and Securities
32. During the recovery of Local Area Network and Servers, which of the following steps would normally be performed first?
    1. Damage mitigation
    2. Install LAN communications network and servers
    3. Assess damage to LAN and servers
    4. Recover equipment
33. Notifying the appropriate parties to take action in order to determine the extent of the severity of an incident and to remediate the incident's effects includes:
    1. Intrusion Evaluation (IE) and Response
    2. Intrusion Recognition (IR) and Response
    3. Intrusion Protection (IP) and Response
    4. Intrusion Detection (ID) and Response
34. Which of the following recovery plan test results would be most useful to management?
    1. elapsed time to perform various activities
    2. list of successful and unsuccessful activities
    3. amount of work completed
    4. description of each activity
35. What is the window of time for recovery of information processing capabilities based on?
    1. Quality of the data to be processed.
    2. Nature of the disaster.
    3. Criticality of the operations affected.
    4. Applications that are mainframe based.
36. Which of the following statements pertaining to dealing with the media after a disaster occurred and disturbed the organization's activities is incorrect?
    1. The CEO should always be the spokesperson for the company during a disaster.
    2. The disaster recovery plan must include how the media is to be handled during the disaster.
    3. The organization's spokesperson should report bad news before the press gets a hold of it through another channel.
    4. An emergency press conference site should be planned ahead.
37. Which of the following computer recovery sites is only partially equipped?
    1. non-mobile hot site
    2. mobile hot site
    3. warm site
    4. cold site
38. If your property Insurance has Actual Cost Valuation (ACV) clause your damaged property will be compensated:
    1. Based on the value of item on the date of loss
    2. Based on new item for old regardless of condition of lost item
    3. Based on value of item one month before the loss
    4. Based on value of item on the date of loss plus 10 percent
39. A business continuity plan should list and prioritize the services that need to be brought back after a disaster strikes. Which of the following services is more likely to be of primary concern?
    1. Marketing/Public relations
    2. Data/Telecomm/IS facilities
    3. IS Operations
    4. Facilities security
40. Which of the following enables the person responsible for contingency planning to focus risk management efforts and resources in a prioritized manner only on the identified risks?
    1. A risk assessment
    2. Residual risks
    3. Security controls
    4. Business units
41. Which of the following will a Business Impact Analysis NOT identify?
    1. Areas that would suffer the greatest financial or operational loss in the event of a disaster.
    2. Systems critical to the survival of the enterprise.
    3. The names of individuals to be contacted during a disaster.
    4. The outage time that can be tolerated by the enterprise as a result of a disaster.
42. Of the reasons why a Disaster Recovery plan gets outdated, which of the following is not true?
    1. Personnel turnover
    2. Large plans can take a lot of work to maintain
    3. Continuous auditing makes a Disaster Recovery plan irrelevant
    4. Infrastructure and environment changes
43. Which is not one of the primary goals of BIA?
    1. Criticality Prioritization
    2. Down time estimation
    3. Determining requirements for critical business functions
    4. Deciding on various test to be performed to validate Business Contuity Plan
44. Which of the following computer recovery sites is the least expensive and the most difficult to test?
    1. non-mobile hot site
    2. mobile hot site
    3. warm site
    4. cold site
45. How often should tests and disaster recovery drills be performed?
    1. At least once a quarter
    2. At least once every 6 months
    3. At least once a year
    4. At least once every 2 years
46. Most threats come from:
    1. Disgruntled employees
    2. Fire, water and electrical
    3. Errors and omissions
    4. Outsider threats
47. Which of the following should be most emphasized as a business impact analysis critically examines business processes?
    1. composition
    2. priorities
    3. dependencies
    4. service levels
48. Business Continuity and Disaster Recovery Planning (Primarily) addresses the:
    1. Availability of the CIA triad
    2. Confidentiality of the CIA triad
    3. Integrity of the CIA triad
    4. Availability, Confidentiality and Integrity of the CIA triad
49. What is not one of the drawbacks of hot sites?
    1. Need Security controls, as it usually contain mirrored copies of live production data
    2. Full redundancy in hardware, software, communication lines and applications is very expensive
    3. The hot sites are available immediately or within maximum tolerable downtime (MTD)
    4. They are administratively resource intensive, as transaction redundacy controls need to be implemented to keep data up-to-date
50. Which of the following teams should not be included in an organization's contingency plan?
    1. Damage assessment team
    2. Hardware salvage team
    3. Tiger team
    4. Legal affairs team
51. Which of the following statements pertaining to a Criticality Survey is incorrect?
    1. It is implemented to gather input from all personnel that is going to be part of the recovery teams.
    2. The purpose of the survey must be clearly stated.
    3. Management's approval should be obtained before distributing the survey.
    4. Its intend is to find out what services and systems are critical to keeping the organization in business.
52. Which of the following is the most complete disaster recovery plan test type after the full-interruption test?
    1. Parallel test
    2. Checklist test
    3. Simulation test
    4. Structured walk-through test
53. The term critical support areas is defined as:
    1. Business units or functions that must be present to sustain continuity of business, maintain life safety and avoid public embarrassment
    2. Business units or functions that may be replaced by others in disaster situation
    3. Human Resource and Information technologies
    4. Business units or functions that require support against man-made disasters
54. What is electronic vaulting?
    1. Information is backed up to tape on a hourly basis and is stored in a on-site vault.
    2. Information is backed up to tape on a daily basis and is stored in a on-site vault.
    3. Transferring electronic journals or transaction logs to an off-site storage facility
    4. A transfer of bulk information to a remote central backup facility.
55. What is the LEAST expensive alternative providing processing facilities in case a disaster should strike?
    1. Warm site
    2. Hot site
    3. Reciprocal agreement
    4. Cold site
56. Which of the following steps is NOT one of the four steps of a Business Impact Assessment (BIA):
    1. Notifying senior management.
    2. Gathering the needed assessment materials.
    3. Performing the vulnerability assessment.
    4. Analyzing the information compiled.
57. The first step in contingency planning is to perform:
    1. A hardware backup
    2. A data backup
    3. An operating systems software backup
    4. An application software backup
58. When conducting a business continuity audit, which of the following would be the MOST important to review?
    1. A hot site is contracted for and available as needed
    2. A business continuity manual is available and current
    3. Insurance coverage is adequate and premiums are current
    4. Media backups are performed on a timely basis and stored off-site
59. Which of the following statements is the most important assumption behind the warm site concept?
    1. The warm site is partially configured with selected network equipments and peripheral devices.
    2. Heat, ventilation and air conditioning are installed at the warm site.
    3. The main equipment can be obtained quickly for emergency installation at a warm site.
    4. The choice of a warm site is less expensive than that of a hot site.
60. A Business Impact Analysis (BIA) does not:
    1. Recommend the appropriate recovery solution.
    2. Determine critical and necessary business functions and their resource dependencies.
    3. Identify critical computer applications and the associated outage tolerance.
    4. Estimate the financial and operational impact of a disruption.
61. Which of the following rules pertaining to a Business Continuity Plan/Disaster Recovery Plan is incorrect?
    1. In order to facilitate recovery, a single plan should cover all locations.
    2. There should be requirements to form a committee to decide a course of action. These decisions should be made ahead of time and incorporated into the plan.
    3. In its procedures and tasks, the plan should refer to functions, not specific individuals.
    4. Critical vendors should be contacted ahead of time to validate equipment can be obtained in a timely manner.
62. All risks must be:
    1. Transferred
    2. Eliminated
    3. Identified
    4. Insured for
63. What can be defined as the maximum acceptable length of time that elapses before the unavailability of the system severely affects the organization?
    1. Recovery Point Objectives (RPO)
    2. Recovery Time Objectives (RTO)
    3. Recovery Time Period (RTP)
    4. Critical Recovery Time (CRT)
64. Under "Named Perils" form of Property Insurance:
    1. Burden of proof that particular loss is covered is on Insurer
    2. Burden of proof that particular loss is not covered is on Insurer
    3. Burden of proof that particular loss is covered is on Insured
    4. Burden of proof that particular loss is not covered is on Insured
65. Which of the following questions is less likely to help in assessing an organization's contingency planning controls?
    1. Is damaged media stored and/or destroyed?
    2. Are the backup storage site and alternate site geographically removed from the primary site?
    3. Is there an up-to-date copy of the plan stored securely off-site?
    4. Is the location of stored backups identified?
66. An offsite backup facility intended to operate an information processing facility, having no computer or communications equipment, but having flooring, electrical writing, air conditioning, etc. is better known as a:
    1. Hot site
    2. Duplicate processing facility
    3. Cold site
    4. Warm site
67. A business continuity plan is an example of which of the following?
    1. Corrective control
    2. Detective control
    3. Preventive control
    4. Compensating control
68. Minimum level of transaction redundancy implementation is usually employed at hot sites is:
    1. Daily backup
    2. Electronic Vaulting
    3. Electronic Journaling
    4. Database Shadowing
69. Which of the following \*must\* be at a "hot site"?
    1. Backup data, computers, climate control, cables and peripherals
    2. Computers and peripherals
    3. Computers, peripherals, and dedicated climate control systems
    4. Dedicated climate control systems
70. What is a disaster recovery plan for a company's computer system usually focused on?
    1. Alternate procedures to process transactions
    2. The probability that a disaster will occur
    3. Strategic long-range planning
    4. Availability of compatible equipment at a hot site
71. Which of the following is not a direct benefit of successful Disaster Recovery Planning?
    1. Maintenance of Business Continuity
    2. Protection of Critical Data
    3. Increase in IS performance
    4. Minimized Impact of a disaster
72. Contracts and agreements are unenforceable in which of the following alternate backup facilities?
    1. hot site
    2. warm site
    3. cold site
    4. reciprocal agreement
73. Which of the following statements regarding an off-site information processing facility is TRUE?
    1. It should have the same amount of physical access restrictions as the primary processing site.
    2. It should be located in proximity to the originating site so that it can quickly be made operational.
    3. It should be easily identified from the outside so in the event of an emergency it can be easily found.
    4. Need not have the same level of environmental monitoring as the originating site since this would be cost prohibitive.
74. What is the MAIN concern when reviewing a reciprocal disaster recovery agreement between two companies?
    1. The soundness of the business impact analysis.
    2. Hardware and software compatibility.
    3. Frequency of system testing.
    4. Differences in IS policies and procedures.
75. Failure of a contingency plan is usually:
    1. A technical failure.
    2. A management failure.
    3. Because of a lack of awareness.
    4. Because of a lack of training.
76. The Recovery Point Objective in Disaster Recovery Planning refers to which of the following?
    1. Point to which application data must be recovered to resume business transactions
    2. Maximum elapsed time required to complete recovery of application data
    3. Point to which application data must be recovered to resume system operations
    4. Point to which information system must be operational at alternate site
77. Which of the following is an advantage of the use of hot sites as a backup alternative?
    1. The costs associated with hot sites are low.
    2. Hot sites can be made ready for operation within a short period of time.
    3. Hot sites can be used for an extended amount of time.
    4. Hot sites do not require that equipment and systems software be compatible with the primary installation being backed up.
78. What is the MAIN purpose for periodically testing off-site hardware backup facilities?
    1. To eliminate the need to develop detailed contingency plans.
    2. To ensure that program and system documentation remains current.
    3. To ensure the integrity of the data in the database.
    4. To ensure the continued compatibility of the contingency facilities.
79. Which of the following tasks is not usually part of a Business Impact Analysis (BIA)?
    1. Identify the type and quantity of resources required for the recovery.
    2. Identify critical business processes and the dependencies between them.
    3. Identify organizational risks.
    4. Develop a mission statement.
80. What is the most critical piece to disaster recovery and continuity planning?
    1. Security policy
    2. Management support
    3. Availability of backup information processing facilities
    4. Staff training
81. What would be the primary purpose of periodically testing offsite hardware backup facilities?
    1. Ensure the continued compatibility of the contingency facilities
    2. Ensure that data can be restored at offsite facilities.
    3. Eliminate the need to develop detailed contingency plans
    4. Ensure that operations documentation remains current
82. The main advantage of using hot sites is:
    1. Costs associated with this solution are relatively low.
    2. Hot sites can be used for an extended amount of time.
    3. Hot sites do not require that equipment and systems software be compatible with the primary installation being backed up.
    4. Hot sites can be made ready for operation within a short period of time.
83. Once an intrusion into your organization's information system has been detected, which of the following actions should be performed first?
    1. Eliminate all means of intruder access.
    2. Contain the intrusion.
    3. Determine to what extent systems and data are compromised.
    4. Communicate with relevant parties.
84. What is the most correct choice below when talking about the steps to resume normal operation?
    1. Most critical operations are moved from alternate site to primary site before others
    2. Operation may be carried by a completely different team than disaster recovery team
    3. Non critical systems are moved first from alternate site to the primary business location
    4. Business operations cannot be moved back, until green light is given by the salvage team that primary site is ready
85. For which areas of the enterprise are business continuity plans required?
    1. All areas of the enterprise.
    2. The financial and information processing areas of the enterprise.
    3. The operating areas of the enterprise.
    4. The marketing, finance, and information processing areas.
86. What is a hot-site facility?
    1. A site with pre-installed computers, raised flooring, air conditioning, telecommunications and networking equipment, and UPS.
    2. A site in which space is reserved with pre-installed wiring and raised floors.
    3. A site with raised flooring, air conditioning, telecommunications, and networking equipment, and UPS.
    4. A site with a ready-made work space with telecommunications equipment, LANs, PCs, and terminals for work groups.
87. Which of the following backup sites is most effective for disaster recovery?
    1. Time brokers
    2. Hot sites
    3. Cold sites
    4. Reciprocal Agreement
88. Which primary element of BCP includes carrying out vulnerability analysis?
    1. Scope and Plan Initiation
    2. Business Impact Assessment
    3. Business Continuity Plan Development
    4. Plan Approval and Implementation
89. What is the Maximum Tolerable Downtime (MTD)?
    1. Maximum elapsed time required to complete recovery of application data
    2. Minimum elapsed time required to complete recovery of application data
    3. Maximum elapsed time required to move back to primary site after a major disruption
    4. It is maximum delay businesses can tolerate and still remain viable
90. Which one of the following is not one of the outcomes of a vulnerability analysis?
    1. Quantitative loss assessment
    2. Qualitative loss assessment
    3. Formal approval of BCP scope and initiation document
    4. Defining critical support areas
91. What is not a benefit of cold sites?
    1. No resource contention with other organization
    2. Quick Recovery
    3. Geographical location that is not affected by the same disaster
    4. Low Cost
92. Which disaster recovery plan test involves functional representatives meeting to review the plan in detail?
    1. Simulation test
    2. Checklist test
    3. Parallel test
    4. Structured walk-through test
93. Which of the following results in the most devastating business interruptions?
    1. Loss of Hardware/Software
    2. Loss of Data
    3. Loss of Communication Links
    4. Loss of Applications
94. The results of a test of the disaster recovery plan conducted at a warm site notes that clients were unable to log on to the restored online systems as there were insufficient data lines connecting the client premises to the recovery site. The MOST likely conclusion that can be drawn is that:
    1. The use of a warm site is inappropriate.
    2. The impact of a potential disaster was not fully analyzed.
    3. The clients were not sufficiently involved in plan development.
    4. The external communications service providers were not involved in the test.
95. After a company is out of an emergency state, what should be moved back to the original site first?
    1. Executives
    2. Least critical work
    3. IT support staff
    4. Most critical work
96. A contingency plan should address:
    1. Potential risks
    2. Residual risks
    3. Identified risks
    4. All of the above
97. In which of the following phases of system development life cycle (SDLC) is contingency planning most important?
    1. Initiation
    2. Development/acquisition
    3. Implementation
    4. Operation/maintenance
98. Which of the following alternative business recovery strategies would be LEAST appropriate in a large database and on-line communications network environment where the critical business continuity period is 7 days?
    1. Hot site
    2. Warm site
    3. Duplicate information processing facilities
    4. Reciprocal agreement
99. A Business Continuity Plan should be tested:
    1. Once a month.
    2. At least twice a year.
    3. At least once a year.
    4. At least once every two years.
100. Classification of information systems is essential in business continuity planning. Which of the following system types cannot be replaced by manual methods?
     1. Critical system
     2. Vital system
     3. Sensitive system
     4. Non critical system
101. Which of the following is less likely to accompany a contingency plan, either within the plan itself or in the form of an appendix?
     1. Contact information for all personnel.
     2. Vendor contact information, including offsite storage and alternate site.
     3. Equipment and system requirements lists of the hardware, software, firmware and other resources required to support system operations.
     4. The Business Impact Analysis.
102. Which of the following would best help an organization to gain a common understanding of functions that are critical to its survival?
     1. A risk assessment
     2. A business assessment
     3. A disaster recovery plan
     4. A business impact analysis