

Management 414: SANS CISSP® 10 Domains +S QUIZ - Domain 8

1. Between which two areas should a security policy seek to achieve a balance?
 - a) Security and Confidentiality
 - b) Integrity and Access
 - c) Access and Security
 - d) Confidentiality, Integrity and Availability
2. There are many types of testing methods involved while exercising and maintaining a Business Continuity Plan. Which of the following types of testing is also known as consistency testing?
 - a) Validity testing
 - b) Simulation testing
 - c) Checklist testing
 - d) Structured walk-through testing
3. Which of the following topics is NOT part of a well defined Business Continuity Plan (BCP)?
 - a) Post-disaster recovery
 - b) Fiscal budget forecasting
 - c) Back-up operations
 - d) Emergency response
4. The distinction between a business continuity plan (BCP) and a disaster recovery plan (DRP) are best described as what?
 - a) The business continuity plan deals with the restoration or continued operations of the business processes, whereas the disaster recovery plan deals with the efforts to recover the physical environment from a natural disaster.
 - b) The business continuity plan deals with the restoration or continued operations of the business processes, whereas the disaster recovery plan deals with the restoration of the critical information systems that support the business processes.
 - c) The business continuity plan deals with the effort to spread information system upgrades and purchases over time so as to mitigate the risk of security incidents stemming from overworked staff and/or unsecured computers. The disaster recovery plan deals with the restoration of the critical information systems that support the business processes.
 - d) The distinction is minor, but can be characterized as the difference between what is done just before a disaster and what is done just after a disaster.
5. Which of the following characterizations concerning business continuity plans and disaster recovery plans is correct?
 - a) A business continuity plan is long term focused, and a disaster recovery plan is short term focused.

Management 414: SANS CISSP® 10 Domains +S QUIZ - Domain 8

- b) A business continuity plan is short term focused, and a disaster recovery plan is long term focused.
 - c) Both business continuity plans and a disaster recovery plans are long term focused.
 - d) Both business continuity plans and a disaster recovery plans are short term focused.
6. What is the most common source of security "disasters"?
- a) Disgruntled employees
 - b) Contractors and vendors
 - c) Hackers/crackers
 - d) Errors and omissions
7. The proper flow in the development of a business continuity plan (BCP) or disaster recovery plan (DRP) is characterized by which of the following set of steps?
- a) Business impact analysis, risk analysis, build the plan, test and validate, modify and update the plan, and approve and implement the plan.
 - b) Risk analysis, business impact analysis, build the plan, test and validate, modify and update the plan, and approve and implement the plan
 - c) Risk analysis, business impact analysis, build the plan, test and validate, and approve and implement the plan
 - d) Business impact analysis, build the plan, test and validate, modify and update the plan, and approve and implement the plan
8. A key part of developing a business continuity plan (BCP) is to get "C-level" support. What is "C-level" support?
- a) The support given by chief level positions in the company, such as CFO, CEO and CIO.
 - b) The support given by people "in the middle", or "C-level" to the organization, such as experienced system and security administrators.
 - c) The support given by the middle tier of management, or C-level management, which is the level at which most of the important day-to-day operations are made.
 - d) The support given by those whose job is to address the business continuity at an information systems level.
9. Which of the following is NOT a business continuity plan deliverable?
- a) Procedure to keep the plan up-to-date
 - b) Plan for testing
 - c) Plan for training
 - d) Tape backup storage plan

Management 414: SANS CISSP® 10 Domains +S QUIZ - Domain 8

10. There are many types of testing methods involved while exercising and maintaining a Business Continuity Plan. Which of the following types of testing is also known as validity testing?
 - a) Consistency testing
 - b) Simulation testing
 - c) Checklist testing
 - d) Structured walk-through testing
11. In the business impact analysis (BIA), answers to key questions such as "Would the disaster impact the level of service?" should come from or be concurred by whom?
 - a) The data owner
 - b) The customer
 - c) Executive management
 - d) The system administration staff
12. With respect to the business impact analysis (BIA), what is NOT true of the vulnerability assessment?
 - a) It provides sufficient detail to and scope to complete the BIA.
 - b) It is smaller than a full risk assessment.
 - c) It identifies crucial business functions.
 - d) It uses results as input to a recovery strategy.
13. The primary goal of a business impact analysis (BIA) is to determine what?
 - a) The minimum set of information system resources needed to operate
 - b) The maximum allowable downtime for any given system
 - c) The impact upon the financial and operating resources of the company for the first 24 and 72 hours periods after downtime has occurred
 - d) The average time any given system can be down before the business is "impacted" in a financial or operational manner
14. "Mirroring," a type of time-synchronized backup, is also known as what?
 - a) A bit-for-bit copy
 - b) RAID 5
 - c) An incremental backup
 - d) Electronic vaulting.
15. Which of the following types of business continuity plan testing is also known as "validity testing?"
 - a) Simulation testing
 - b) Structured walk-through testing
 - c) Full interpretation
 - d) Checklist

Management 414: SANS CISSP® 10 Domains +5 QUIZ - Domain 8

16. Why should all company staff, or at least a large subsection, be trained in the recovery process of the business continuity plan?
- a) The recovery process is a difficult and time-consuming task and requires as many staff as possible to oversee it.
 - b) Sufficient insurance coverage for a disaster can be obtained for the organization.
 - c) In the event of a drastic loss of life, there are most likely still trained individuals to help carry out the recovery process.
 - d) Each individual can be held liable for not following the recovery plan in the event of a disaster.
17. With respect to validity testing of the business continuity plan (BCP), what is the most important question to be answered?
- a) Does the plan seem valid when reviewing it in a non-emergency situation?
 - b) Does the plan validate the focus applied to the key business processes?
 - c) Does the plan truly enable recovery?
 - d) Do the "C-level" managers, such as the CIO, CEO and CTO, agree the plan is valid?
18. Which of the following is NOT a component of a good security policy?
- a) Purpose
 - b) Action
 - c) Responsibility
 - d) Incident handling instructions
19. What is a Business Continuity Plan (BCP)?
- a) A stand-alone plan that has few or no ties to other plans or documents
 - b) An overarching plan that includes a compilation or collection of other plans
 - c) A plan that is a subcomponent of the Disaster Recovery Plan (DRP)
 - d) A plan that is a subcomponent of the Continuity of Operations Plan (COOP)
20. What is a Disaster Recovery Plan (DRP)?
- a) A plan that contains the Business Recovery Plan (BRP) as a subcomponent.
 - b) A plan that has no relationship to the Business Recovery Plan (BRP).
 - c) Otherwise known as the Business Recovery Plan (BRP).
 - d) A subcomponent of the Business Recovery Plan (BRP).
21. Which of the following is NOT an element of basic contingency planning?
- a) Include a statement of urgency.
 - b) Include information on vital records.
 - c) Define an emergency response procedure.
 - d) Define roles and responsibilities for all employees in the event of an emergency.

22. Which of the following components of a policy explains the reason for the policy?
- a) **Scope**
 - b) **Background**
 - c) **Purpose**
 - d) Policy statement
23. Firewall or anti-virus policies are examples of which type of higher lever policy?
- a) Local Policy
 - b) Division-wide Policy
 - c) Issue-Specific Policy
 - d) Corporate Policy
24. Business Continuity Planning comprises multiple steps beginning with Project Initiation. Which of the following choices is the first task of the Project Initiation process?
- a) Defining the objectives and deliverables
 - b) Scoping the project
 - c) Building a team
 - d) Establishing executive support
 - e) Appointing a project manager
25. Which of the following choices is the goal of both the Disaster Recovery Plan and Business Continuity Plan?
- a) Recovery is complete once all business processes return to 'business as usual'.
 - b) Make the response time as short as possible as well as the time required for complete recovery.
 - c) Implements the recovery in regards to a disruption.
 - d) Makes the response to disruption as short as possible.
26. Which of the following choices is a business' last line of defense against risks that cannot be controlled or avoided by other risk management practices?
- a) Business Impact Analysis
 - b) Business Continuity Planning
 - c) Risk Analysis
 - d) Disaster Recovery Planning
27. Which of the following choices is the first step when developing a Contingency Plan?
- a) Develop an IT contingency plan
 - b) Identify preventive controls
 - c) Develop the contingency planning policy statement
 - d) Conduct the business impact analysis

Management 414: SANS CISSP® 10 Domains +5 QUIZ - Domain 8

28. Once you understand risk, you can decide to not become involved in the risk situation. Which of the choices below describes this decision?
- a) Risk reduction
 - b) Risk transfer
 - c) Risk acceptance
 - d) Risk avoidance
29. Once you understand risk, you can decide if you want to shift the responsibility to someone else. Which of the choices below describes this decision?
- a) Risk transfer
 - b) Risk reduction
 - c) Risk acceptance
 - d) Risk avoidance
30. When calculating the cost of a threat, you need to look at two factors. Which of the following choices is one of those factors?
- a) Exposure factor
 - b) Impact
 - c) Single Loss expectancy
 - d) Risk
31. Which of the following choices is the formula for calculating Annualized Loss Expectancy (ALE) when determining the cost of a threat?
- a) Annualized Loss Expectancy (ALE) = Single Loss Expectancy (SLE) + Annualized Rate of Occurrence (ARO)
 - b) Annualized Loss Expectancy (ALE) = Single Loss Expectancy (SLE) * Annualized Rate of Occurrence (ARO)
 - c) Annualized Loss Expectancy (ALE) = Single Loss Expectancy (SLE) n Annualized Rate of Occurrence (ARO)
 - d) Annualized Loss Expectancy (ALE) = Single Loss Expectancy (SLE) / Annualized Rate of Occurrence (ARO)
32. Which of the following alternate site choices combines multiple sites to afford maximum flexibility?
- a) Hybrid sites
 - b) Mobile sites
 - c) Cold sites
 - d) Warm sites

Management 414: SANS CISSP® 10 Domains +S QUIZ - Domain 8

33. Which of the following choices follows risk analysis in the Business Continuity Planning/Disaster Recovery Planning Process Lifecycle?
- a) Business Impact Analysis
 - b) Testing and Validating the Plan
 - c) Building the Plan
 - d) Project Initiation