Chapter 14

1. Raul has been asked to help develop an outline of procedures to be followed in the event of a major IT incident or an incident that directly impacts IT. What type of planning is this?
2. Disaster recovery planning
3. **IT contingency planning**
4. Business impact analysis planning
5. Risk IT planning
6. Dilma has been tasked with creating a list of potential employees to serve in an upcoming tabletop exercise. Which employees will be on her list?
7. All employees
8. **Individuals on a decision-making level**
9. Full-time employees
10. Only IT managers
11. What is the average amount of time that it will take a device to recover from a failure that is not a terminal failure?
12. **MTTR**
13. MTBR
14. MTBF
15. MTTI
16. Which of the following is NOT a category of fire suppression systems?
17. Water sprinkler system
18. **Wet chemical system**
19. Clean agent system
20. Dry chemical system
21. Which of the following is NOT required for a fire to occur?
22. A chemical reaction that is the fire itself
23. A type of fuel or combustible material
24. **A spark to start the process**
25. Sufficient oxygen to sustain the combustion
26. An electrical fire like that which would be found in a computer data center is known as what type of fire?
27. Class A
28. Class B
29. **Class C**
30. Class D
31. Which level of RAID uses disk mirroring and is considered fault-tolerant?
32. **Level 1**
33. Level 2
34. Level 3
35. Level 4
36. What is the amount of time added to or subtracted from Coordinated Universal Time to determine local time?
37. **Time offset**
38. Civil time
39. Daylight savings time
40. Greenwich Mean Time (GMT)
41. What does the abbreviation RAID represent?
42. Redundant Array of IDE Drives
43. Resilient Architecture for Interdependent Discs
44. **Redundant Array of Independent Drives**
45. Resistant Architecture of Inter-Related Data Storage
46. Which of these is an example of a nested RAID?
47. Level 1-0
48. Level 0-1
49. **Level 0+1**
50. Level 0/1
51. A(n) \_\_\_\_\_ is always running off its battery while the main power runs the battery charger.
52. secure UPS
53. backup UPS
54. off-line UPS
55. **on-line UPS**
56. Which type of site is essentially a duplicate of the production site and has all the equipment needed for an organization to continue running?
57. Cold site
58. Warm site
59. **Hot site**
60. Replicated site
61. Which of the following can a UPS NOT perform?
62. **Prevent certain applications from launching that will consume too much power**
63. Disconnect users and shut down the server
64. Prevent any new users from logging on
65. Notify all users that they must finish their work immediately and log off
66. Which of these is NOT a characteristic of a disaster recovery plan (DRP)?
67. It is updated regularly.
68. **It is a private document used only by top-level administrators for planning.**
69. It is written.
70. It is detailed.
71. What does an incremental backup do?
72. **Copies all files changed since the last full or incremental backup**
73. Copies selected files
74. Copies all files
75. Copies all files since the last full backup
76. Which question is NOT a basic question to be asked regarding creating a data backup?
77. What media should be used?
78. **How long will it take to finish the backup?**
79. Where should the backup be stored?
80. What information should be backed up?
81. The chain of \_\_\_\_\_ documents that the evidence was under strict control at all times and no unauthorized person was given the opportunity to corrupt the evidence.
82. forensics
83. evidence
84. **custody**
85. control
86. What is the maximum length of time that an organization can tolerate between data backups?
87. Recovery time objective (RTO)
88. Recovery service point (RSP)
89. **Recovery point objective (RPO)**
90. Optimal recovery timeframe (ORT)
91. Margaux has been asked to work on the report that will analyze the exercise results with the purpose of identifying strengths to be maintained and weaknesses to be addressed for improvement. What report will she be working on?
92. Identification of critical systems report
93. Containment report
94. Business continuity report
95. **After-action report**
96. When an unauthorized event occurs, what is the first duty of the cyber-incident response team?
97. To log off from the server
98. **To secure the crime scene**
99. To back up the hard drive
100. To reboot the system