Chapter 5

Governance, Risk, and Compliance

THE COMPTIA SECURITY+ EXAM SY0-601 TOPICS COVERED IN THIS CHAPTER INCLUDE THE FOLLOWING:

- ✓ **5.1 Compare and contrast various types of controls**
- ✓ **5.2 Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture**
- ✓ **5.3 Explain the importance of policies to organizational security**
- ✓ **5.4 Summarize risk management processes and concepts**
- ✓ **5.5 Explain privacy and sensitive data concepts in relation to security**

1. Caroline has been asked to find an international standard to guide her company's choices in implementing information security management systems. Which of the following would be the best choice for her?
   - **A.** ISO 27002
   - **B.** ISO 27017
   - **C.** NIST 800-12
   - **D.** NIST 800-14

2. Adam is concerned about malware infecting machines on his network. One of his concerns is that malware would be able to access sensitive system functionality that requires administrative access. What technique would best address this issue?
   - **A.** Implementing host-based antimalware
   - **B.** Using a nonadministrative account for normal activities
   - **C.** Implementing full-disk encryption (FDE)
   - **D.** Making certain the operating systems are patched

3. You are responsible for setting up new accounts for your company network. What is the most important thing to keep in mind when setting up new accounts?
   - **A.** Password length
   - **B.** Password complexity
   - **C.** Account age
   - **D.** Least privileges

4. 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

5. 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

6. What standard is used for credit card security?

A. GDPR

B. COPPA

C. PCI-DSS

D. CIS

7. 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

8. 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 at each desk

C. Proximity cards

D. Onboarding

9. 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

10. 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

11. As part of the response to a credit card breach, Sally discovers evidence that individuals in her organization were actively working to steal credit card information and personally identifiable information (PII). She calls the police to engage them for the investigation. What has she done?

A. Escalated the investigation

B. Public notification

C. Outsourced the investigation

D. Tokenized the data

12. You have an asset that is valued at $16,000, the exposure factor of a risk affecting that asset is 35 percent, and the annualized rate of occurrence is 75 percent. What is the SLE?

A. $5,600

B. $5,000

C. $4,200

D. $3,000

13. 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

14. 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?

A. Lighting

B. Motion sensor

C. Hidden video cameras

D. Antivirus scanner

15. 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

16. 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

17. Jim's company operates facilities in Illinois, Indiana, and Ohio, but the headquarters is in Illinois. Which state laws does Jim need to review and handle as part of his security program?

A. All U.S. state laws

B. Illinois

C. Only U.S. federal laws

D. State laws in Illinois, Indiana, and Ohio

18. 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

19. Mark is an office manager at a local bank branch. He wants to ensure that 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

20. 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

21. 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

22. As the IT security officer for your organization, 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

23. Which of the following is not a physical security control?

A. Motion detector

B. Fence

C. Antivirus software

D. Closed-circuit television (CCTV)

24. 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

25. Your company has outsourced its proprietary processes to Acme Corporation. Due to technical issues, Acme wants to include a third-party vendor to help resolve the technical issues. Which of the following must Acme 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.

26. Which of the following is considered a detective control?

A. Closed-circuit television (CCTV)

B. An acceptable use policy

C. Firewall

D. IPS

27. 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-on 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

28. 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

29. 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

30. 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

31. Tony's company wants to limit their risk due to customer data. What practice should they put in place to ensure that they have only the data needed for their business purposes?

A. Data masking

B. Data minimization

C. Tokenization

D. Anonymization

32. 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

33. A security administrator is reviewing the company's continuity plan, and it specifies an RTO of four hours and an RPO of one day. Which of the following is the plan describing?

A. Systems should be restored within one day and should remain operational for at least four hours.

B. Systems should be restored within four hours and no later than one day after the incident.

C. Systems should be restored within one day and lose, at most, four hours' worth of data.

D. Systems should be restored within four hours with a loss of one day's worth of data at most.

34. Which of the following statements is true regarding a data retention policy?

- **A.** Regulations require financial transactions to be stored for seven 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.

35. 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)

36. Michelle has been asked to use the CIS benchmark for Windows 10 as part of her system security process. What information will she be using?

- **A.** Information on how secure Windows 10 is in its default state
- **B.** A set of recommended security configurations to secure Windows 10
- **C.** Performance benchmark tools for Windows 10 systems, including network speed and firewall throughput
- **D.** Vulnerability scan data for Windows 10 systems provided by various manufacturers

37. Which of the following is the best example of a preventive control?

- **A.** Data backups
- **B.** Security camera
- **C.** Door alarm
- **D.** Smoke detectors

38. 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 techniques are you demonstrating?

- **A.** Accept
- **B.** Mitigate
- **C.** Transfer
- **D.** Avoid

39. Each salesperson who travels has a cable lock to lock down their laptop when they step away from the device. To which of the following controls does this apply?

- **A.** Administrative
- **B.** Compensating
- **C.** Deterrent
- **D.** Preventive

40. 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

41. All of your organization's traffic flows through a single connection to the Internet. Which of the following terms best describes this scenario?

A. Cloud computing

B. Load balancing

C. Single point of failure

D. Virtualization

42. Which of the following best describes the disadvantages of quantitative risk analysis compared to qualitative risk analysis?

A. Quantitative risk analysis requires detailed financial data.

B. Quantitative risk analysis is sometimes subjective.

C. Quantitative risk analysis requires expertise on systems and infrastructure.

D. Quantitative risk provides clear answers to risk-based questions.

43. 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

44. 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

45. 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

46. 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.

47. 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

48. A security analyst is analyzing the cost the company could incur if the customer database was breached. The database contains 2,500 records with personally identifiable information (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 percent. Which of the following would be the ALE for a security breach?

A. $15,000

B. $37,500

C. $150,000

D. $750,000

49. Which of the following concepts defines a company goal for system restoration and acceptable data loss?

A. MTBF

B. MTTR

C. RPO

D. ARO

50. 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

51. You are a network administrator and have been given the duty of creating user 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

52. What type of control is separation of duty?

A. Physical

B. Operational

C. Technical

D. Compensating

53. Which of the following rights is not included in the GDPR?

A. The right to access

B. The right to be forgotten

C. The right to data portability

D. The right to anonymity

54. Nick is following the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) and has completed the prepare and categorize steps. Which step in the risk management framework is next?

A. Assessing controls

B. Implementing controls

C. Monitoring controls

D. Selecting controls

55. Why are diversity of training techniques an important concept for security program administrators?

A. It allows for multiple funding sources.

B. Each person responds to training differently.

C. It avoids a single point of failure in training compliance.

D. It is required for compliance with PCI-DSS.

56. Alyssa has been asked to categorize the risk of outdated software in her organization. What type of risk categorization should she use?

A. Internal

B. Quantitative

C. Qualitative

D. External

57. What term is used to describe a listing of all of an organization's risks, including information about the risk's rating, how it is being remediated, remediation status, and who owns or is assigned responsibility for the risk?

A. An SSAE

B. A risk register

C. A risk table

D. A DSS

58. Which of the following terms is used to measure how maintainable a system or device is?

A. MTBF

B. MTTF

C. MTTR

D. MITM

59. The company that Olivia works for has recently experienced a data breach that exposed customer data, including their home addresses, shopping habits, email addresses, and contact information. Olivia's company is an industry leader in their space but has strong competitors as well. Which of the following impacts is not likely to occur now that the organization has completed their incident response process?

A. Identity theft

B. Financial loss

C. Reputation loss

D. Availability loss

60. Eric works for the U.S. government and needs to classify data. Which of the following is not a common classification type for U.S. government data?

A. Top Secret

B. Secret

C. Confidential

D. Civilian

61. Which of the following is not a common location for privacy practices to be recorded or codified?

A. A formal privacy notice

B. The source code for a product

C. The terms of the organization's agreement with customers

D. None of the above

62. What key difference separates pseudonymization and anonymization?

A. Anonymization uses encryption.

B. Pseudonymization requires additional data to reidentify the data subject.

C. Anonymization can be reversed using a hash.

D. Pseudonymization uses randomized tokens.

63. What policy clearly states the ownership of information created or used by an organization?

A. A data governance policy

B. An information security policy

C. An acceptable use policy

D. A data retention policy

64. Helen's organization provides telephone support for their entire customer base as a critical business function. She has created a plan that will ensure that her organization's Voice over IP (VoIP) phones will be restored in the event of a disaster. What type of plan has she created?

A. A disaster recovery plan

B. An RPO plan

C. A functional recovery plan

D. An MTBF plan

65. Greg has data that is classified as health information that his organization uses as part of their company's HR data. Which of the following statements is true for his company's security policy?

A. The health information must be encrypted.

B. Greg should review relevant law to ensure the health information is handled properly.

C. Companies are prohibited from storing health information and must outsource to third parties.

D. All of the above

66. What type of information does a control risk apply to?

A. Health information

B. Personally identifiable information (PII)

C. Financial information

D. Intellectual property

67. What type of impact is an individual most likely to experience if a data breach that includes PII occurs?

A. IP theft

B. Reputation damage

C. Fines

D. Identity theft

68. Isaac has been asked to write his organization's security policies. What policy is commonly put in place for service accounts?

A. They must be issued only to system administrators.

B. They must use multifactor authentication.

C. They cannot use interactive logins.

D. All of the above

69. Nina is tasked with putting radio frequency identification (RFID) tags on every new piece of equipment that enters her datacenter that costs more than $500. What type of organizational policy is most likely to include this type of requirement?

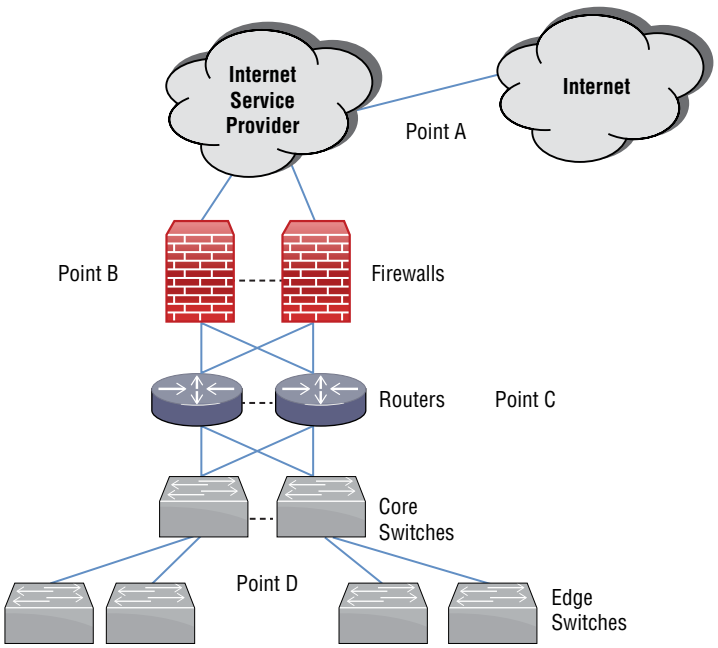
A. A change management policy

B. An incident response policy

C. An asset management policy

D. An acceptable use policy

70. Megan is reviewing her organization's datacenter network diagram as shown in the following image. What should she note for point A on the diagram?



A. A wireless link

B. A redundant connection

C. A wired link

D. A single point of failure

71. Emma is reviewing third-party risks to her organization, and Nate, her organization's procurement officer, notes that purchases of some laptops from the company's hardware vendor have been delayed due to lack of availability of SSDs (solid state drives) and specific CPUs for specific configurations. What type of risk should Emma describe this as?

A. Financial risk

B. A lack of vendor support

C. System integration

D. Supply chain

72. Henry has implemented an intrusion detection system. What category and control type could he list for an IDS?

A. Technical, Detective

B. Administrative, Preventative

C. Technical, Corrective

D. Administrative, Detective

73. Amanda administers Windows 10 workstations for her company and wants to use a secure configuration guide from a trusted source. Which of the following is not a common source for Windows 10 security benchmarks?

A. CIS

B. Microsoft

C. The FTC

D. The NSA

74. Katie has discovered a Windows 2008 web server running in her environment. What security concern should she list for this system?

A. Windows 2008 only runs on 32-bit platforms.

B. Windows 2008 cannot run modern web server software.

C. Windows 2008 has reached its end of life and cannot be patched.

D. All of the above

75. Patching systems immediately after patches are released is an example of what risk management strategy?

A. Acceptance

B. Avoidance

C. Mitigation

D. Transference

76. Charles wants to display information from his organization's risk register in an easy-to-understand and -rank format. What common tool is used to help management quickly understand relative rankings of risk?

A. Risk plots

B. A heat map

C. A qualitative risk assessment

D. A quantitative risk assessment

77. What key element of regulations, like the European Union's (EU's) GDPR, drive organizations to include them in their overall assessment of risk posture?

A. Potential fines

B. Their annual loss expectancy (ALE)

C. Their recovery time objective (RTO)

D. The likelihood of occurrence

78. What phases of handling a disaster are covered by a disaster recovery plan?

A. What to do before the disaster

B. What to do during the disaster

C. What to do after the disaster

D. All of the above

79. Naomi's organization has recently experienced a breach of credit card information. After investigation, it is discovered that her organization was inadvertently not fully compliant with PCI-DSS and is not currently fully compliant. Which of the following penalties is her organization most likely to incur?

A. Criminal charges

B. Fines

C. Termination of the credit card processing agreement

D. All of the above

80. Alaina wants to map a common set of controls for cloud services between standards like COBIT (Control Objectives for Information and Related Technology), FedRAMP (Federal Risk and Authorization Management Program), HIPAA (the Health Insurance Portability and Accountability Act of 1996), and others. What can she use to speed up that process?

A. The CSA's reference architecture

B. ISO 27001

C. The CSA's cloud control matrix

D. ISO 27002

81. Gary has created an application that new staff in his organization are asked to use as part of their training. The application shows them examples of phishing emails and asks the staff members to identify the emails that are suspicious and why. Correct answers receive points, and incorrect answers subtract points. What type of user training technique is this?

A. Capture the flag

B. Gamification

C. Phishing campaigns

D. Role-based training

82. What law or regulation requires a DPO in organizations?

A. FISMA

B. COPPA

C. PCI-DSS

D. GDPR

83. The university that Susan works for conducts top secret research for the U.S. Department of Defense as part of a partnership with its engineering school. A recently discovered breach points to the school being compromised for over a year by an advanced persistent threat actor. What consequence of the breach should Susan be most concerned about?

A. Cost to restore operations

B. Fines

C. Identity theft

D. IP theft

84. What term is used to describe the functions that need to be continued throughout or resumed as quickly as possible after a disaster?

A. Single points of failure

B. Mission-essential functions

C. Recovery time objectives

D. Core recovery functions

85. 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

86. Rick's organization provides a website that allows users to create an account and then upload their art to share with other users. He is concerned about a breach and wants to properly classify the data for their handling process. What data type is most appropriate for Rick to label the data his organization collects and stores?

A. Customer data

B. PII

C. Financial information

D. Health information

87. Jack is conducting a risk assessment, and a staff member notes that the company has specialized, internal AI algorithms that are part of the company's main product. What risk should Jack identify as most likely to impact those algorithms?

A. External

B. Internal

C. IP theft

D. Licensing

88. Dan has written a policy that prohibits employees from sharing their passwords with their coworkers, family members, or others. What type of credential policy has he created?

A. Device credential policy

B. Personnel credential policy

C. A service account policy

D. An administrative account policy

89. Risk severity is calculated using the equation shown here. What information should be substituted for X?

Risk severity = X * Impact

A. Inherent risk

B. MTTR (mean time to repair)

C. Likelihood of occurrence

D. RTO (recovery time objective)

90. How is asset value determined?

A. The original cost of the item

B. The depreciated cost of the item

C. The cost to replace the item

D. Any of the above based on organizational preference

91. What process is used to help identify critical systems?

A. A BIA

B. An MTBF

C. An RTO

D. An ICD

92. Zarmeena wants to transfer the risk for breaches to another organization. Which of the following options should she use to transfer the risk?

A. Explain to her management that breaches will occur.

B. Blame future breaches on competitors.

C. Sell her organization's data to another organization.

D. Purchase cybersecurity insurance.

93. Which of the following is a common security policy for service accounts?

- **A.** Limiting login hours
- **B.** Prohibiting interactive logins
- **C.** Limiting login locations
- **D.** Implementing frequent password expiration

94. The financial cost of a breach is an example of what component of risk calculations?

- **A.** Probability
- **B.** Risk severity
- **C.** Impact
- **D.** All of the above

95. As part of his organization's effort to identify a new headquarters location, Sean reviews the Federal Emergency Management Agency (FEMA) flood maps for the potential location he is reviewing. What process related to disaster recovery planning includes actions like this?

- **A.** Business impact analysis (BIA)
- **B.** Site risk assessment
- **C.** Crime prevention through environmental design
- **D.** Business continuity planning

96. Joanna wants to request an audit report from a vendor she is considering and plans to review the auditor's opinions on the effectiveness of the security and privacy controls the vendor has in place. What type of Standard for Attestation Engagements (SSAE) should she request?

- **A.** SSAE-18 SOC 1, Type 2
- **B.** SSAE-18 SOC 2, Type 1
- **C.** SSAE-18 SOC 1, Type 1
- **D.** SSAE-18 SOC 2, Type 2

97. Jason has created a risk register for his organization and regularly updates it with input from managers and senior leadership throughout the organization. What purpose does this serve?

- **A.** It decreases inherent risk.
- **B.** It increases risk awareness.
- **C.** It decreases residual risk.
- **D.** It increases risk appetite.

98. Laura is aware that her state has laws that guide her organization in the event of a breach of personally identifiable information, including Social Security numbers (SSNs). If she has a breach that involves SSNs, what action is she likely to have to take based on state law?

- **A.** Destroy all Social Security numbers.
- **B.** Reclassify all impacted data.
- **C.** Provide public notification of the breach.
- **D.** Provide a data minimization plan.

99. 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

100. Olivia's cloud service provider claims to provide "five nines of uptime" and Olivia's company wants to take advantage of that service because their website loses thousands of dollars every hour that it is down. What business agreement can Oliva put in place to help ensure that the reliability that the vendor advertises is maintained?

A. An MOU

B. An SLA

C. An MSA

D. A BPA

101. After reviewing systems on his network, Brian has discovered that dozens of them are running copies of a CAD software package that the company has not paid for. What risk type should he identify this as?

A. Internal

B. Legacy systems

C. IP theft

D. Software compliance

102. Gary is beginning his risk assessment for the organization and has not yet begun to implement controls. What risk does his organization face?

A. Residual risk

B. IP theft risk

C. Multiparty risk

D. Inherent risk

103. How is SLE calculated?

A. AV * EF

B. RTO * AV

C. MTTR * EF

D. AV * ARO

104. What type of credential policy is typically created to handle contractors and consultants?

A. A personnel policy

B. A service account policy

C. A third-party policy

D. A root account policy

105. Wayne has estimated the ARO for a risk in his organization to be 3. How often does Wayne think the event will happen?

A. Once every 3 months

B. Three times a year

C. Once every three years

D. Once a year for three years

106. Gurvinder is assessing risks from disasters to his company's facility and wants to properly categorize them in his planning. Which of the following is not a type of natural disaster?

A. Fire

B. Flood

C. Tornado

D. Industrial accidents

107. Madhuri is classifying all of her organization's data and wants to properly classify the information on the main organizational website that is available to anyone who visits the site. What data classification should she use from the following list?

A. Sensitive

B. Confidential

C. Public

D. Critical

108. Elle works for a credit card company that handles credit card transactions for businesses around the world. What data privacy role does her company play?

A. A data controller

B. A data steward

C. A data custodian

D. A data processor

109. The website that Brian is using shows part of his Social Security number, not all of it, and replacing the rest of the digits with asterisks, allowing him to verify the last four digits. What technique is in use on the website?

A. Tokenization

B. Hashing

C. Encryption

D. Data masking

110. Mike wants to look for a common set of tools for security and risk management for his infrastructure as a service (IaaS) environment. Which of the following organizations provides a vendor-neutral reference architecture that he can use to validate his design?

A. The Center for Internet Security (CIS)

B. ISO

C. The Cloud Security Alliance

D. NIST

111. What type of control is a lock?

A. Managerial

B. Technical

C. Physical

D. Corrective

112. Isaac has discovered that his organization's financial accounting software is misconfigured, causing incorrect data to be reported on an ongoing basis. What type of risk is this?

A. Inherent risk

B. Residual risk

C. Control risk

D. Transparent risk

113. Which of the following is not a potential type of person-made disaster?

A. Fires

B. Oil spills

C. Hurricanes

D. War

114. Susan works for the U.S. government and has identified information in her organization that requires some protection. If the information were disclosed without authorization, it would cause identifiable harm to national security. How should she classify the data?

A. Top Secret

B. Secret

C. Confidential

D. Business Sensitive

115. Ed serves as his organization's data steward and wants to classify each data element that is used in their business. How should he classify cell phone numbers?

A. As PHI

B. As financial information

C. As PII

D. As government information

116. Marcus wants to ensure that attackers can't identify his customers if they were to gain a copy of his organization's web application database. He wants to protect their Social Security numbers (SSNs) with an alternate value that he can reference elsewhere when he needs to look up a customer by their SSN. What technique should he use to accomplish this?

A. Encryption

B. Tokenization

C. Data masking

D. Data washing

117. Which of the following is the most common reason to include a privacy notice on a website?

A. To warn attackers about security measures

B. To avoid lawsuits

C. Due to regulations or laws

D. None of the above

118. Nicole determines how her organization processes data that it collects about its customers and also decides how and why personal information should be processed. What role does Nicole play in her organization?

A. Data steward

B. Data custodian

C. Data controller

D. Data consumer

119. The virtual machine cluster that Pat is in charge of has suffered a major failure in its primary controller. The entire organization is offline, and customers cannot get to the organization's website which is its primary business. What type of disaster has Pat's organization experienced?

A. An MRO disaster

B. An internal disaster

C. An RTO disaster

D. An external disaster

120. What important step should be taken early in the information life cycle to ensure that organizations can handle the data they collect?

A. Data retention

B. Data classification

C. Data minimization

D. Data exfiltration

121. Kirk's organization has been experiencing large-scale denial-of-service (DoS) attacks against their primary website. Kirk contracts with his Internet service provider to increase the organization's bandwidth and expands the server pool for the website to handle significantly more traffic than any of the previous DoS attacks. What type of risk management strategy has he employed?

A. Acceptance

B. Avoidance

C. Transfer

D. Mitigation

122. The co-location facility that Joanna contracts to host her organization's servers is in a flood plain in a hurricane zone. What type of risk best describes the risk that Joanna and other customers face?

A. A multiparty risk

B. An internal risk

C. A legacy risk

D. An IP theft risk

123. The cloud service that Natasha's organization has used for the past five years will no longer be available. What phase of the vendor relationship should Natasha plan for with this service?

A. Preparing a service MOU

B. An EOL transition process

C. Creating an NDA

D. A last will and testament

124. Gary wants to use a secure configuration benchmark for his organization for Linux. Which of the following organizations would provide a useful, commonly adopted benchmark that he could use?

A. Microsoft

B. NIST

C. CIS

D. All of the above

125. After Angela left her last organization, she discovered that she still had access to her shared drives and could log in to her email account. What critical process was likely forgotten when she left?

A. An exit interview

B. Job rotation

C. Offboarding

D. Governance

126. Frank knows that businesses can use any classification labels they want, but he also knows that there are a number of common labels in use. Which of the following is not a common data classification label for businesses?

A. Public

B. Sensitive

C. Private

D. Secret

127. Where are privacy notices frequently found?

A. The terms of an agreement for customers

B. A click-through license agreement

C. A website usage agreement

D. All of the above