1. You are the security policy lead for your organization, which is considering migrating from your on-premises, legacy environment into the cloud. You are reviewing the Cloud Security Alliance Cloud Controls Matrix (CSA CCM) as a tool for your organization. Which of the following benefits will the CSA CCM offer your organization? Response:
   A. Simplifying regulatory compliance
   B. Collecting multiple data streams from your log files
   C. Ensuring that the baseline configuration is applied to all systems
   D. Enforcing contract terms between your organization and the cloud provider

2. When an organization implements an SIEM solution and begins aggregating event data, the configured event sources are only valid at the time it was configured. Application modifications, patching, and other upgrades will change the events generated and how they are represented over time. What process is necessary to ensure events are collected and processed with this in mind?
   A. Continual review
   B. Continuous optimization
   C. Aggregation updates
   D. Event elasticity

3. You work for a government research facility. Your organization often shares data with other government research organizations. You would like to create a single sign-on experience across the organizations, where users at each organization can sign in with the user ID/authentication issued by that organization, then access research data in all the other organizations. Instead of replicating the data stores of each organization at every other organization (which is one way of accomplishing this goal), you instead want every user to have access to each organization's specific storage resources. If you don't use cross-certification, what other model can you implement for this purpose? Response:
   A. Third-party identity broker
   B. Cloud reseller
   C. Intractable nuanced variance
   D. Mandatory access control (MAC)

4. Which of the following tools might be useful in data discovery efforts that are based on content analysis?
   A. DLP
   B. Digital Rights Management (DRM)
   C. iSCSI
   D. Fibre Channel over Ethernet (FCoE)

5. You are performing an audit of the security controls used in a cloud environment. Which of the following would best serve your purpose?

Response:
A. The business impact analysis (BIA)
B. A copy of the VM baseline configuration
C. The latest version of the company's financial records
D. A SOC 3 report from another (external) auditor

6. Which of the following is the recommended operating range for temperature and humidity in a data center?
   Response:
   A. Between 62 °F - 81 °F and 40% and 65% relative humidity
   B. Between 64 °F - 81 °F and 40% and 60% relative humidity
   C. Between 64 °F - 84 °F and 30% and 60% relative humidity
   D. Between 60 °F - 85 °F and 40% and 60% relative humidity

7. When a data center is configured such that the backs of the devices face each other and the ambient temperature in the work area is cool, it is called ______.
Response:
A. Hot aisle containment
B. Cold aisle containment
C. Thermo-optimized
D. HVAC modulated

A

8. One of the security challenges of operating in the cloud is that additional controls must be placed on file storage systems because ______ .
Response:
A. File stores are always kept in plain text in the cloud
B. There is no way to sanitize file storage space in the cloud
C. Virtualization necessarily prevents the use of application-based security controls
D. Virtual machines are stored as snapshotted files when not in use

9. Each of the following are dependencies that must be considered when reviewing the BIA after cloud migration except:
Response:
A. The cloud provider's suppliers
B. The cloud provider's vendors
C. The cloud provider's utilities
D. The cloud provider's resellers

10. Which ISO standard refers to addressing security risks in a supply chain?
A. ISO 27001
B. ISO/IEC 28000:2007
C. ISO 18799
D. ISO 31000:2009

11. What is the amount of fuel that should be on hand to power generators for backup datacenter power, in all tiers, according to the Uptime Institute?
A. 1
B. 1,000 gallons
C. 12 hours
D. As much as needed to ensure all systems may be gracefully shut down and data securely stored

12. Impact resulting from risk being realized is often measured in terms of ______.
A. Amount of data lost
B. Money
C. Amount of property lost
D. Number of people affected

13. Which type of cloud service category would having a vendor-neutral encryption scheme for data at rest (DAR) be the MOST important?
Response:
A. Public
B. Hybrid
C. Private
D. Community

14. Which one of the following is not one of the three common threat modeling techniques? Response:

A. Focused on assets
B. Focused on attackers
C. Focused on software
D. Focused on social engineering

15. You are the IT security manager for a video game software development company. Which of the following is most likely to be your primary concern on a daily
basis?

Response:
A. Health and human safety
B. Security flaws in your products
C. Security flaws in your organization
D. Regulatory compliance

16. A cloud data encryption situation where the cloud customer retains control of the encryption keys and the cloud provider only processes and stores the data could
be considered a ______.

Response:
A. Threat
B. Risk
C. Hybrid cloud deployment model
D. Case of infringing on the rights of the provider

17. According to OWASP recommendations, active software security testing should include all of the following except ______ .
Response:

A. Session initiation testing
B. Input validation testing
C. Testing for error handling
D. Testing for weak cryptography

18. All of the following might be used as data discovery characteristics in a content-analysis-based data discovery effort except ______.
Response:
A. Keywords
B. Pattern-matching
C. Frequency
D. Inheritance

19. All of the following methods can be used to attenuate the harm caused by escalation of privilege except: Response:

A. Extensive access control and authentication tools and techniques
B. Analysis and review of all log data by trained, skilled personnel on a frequent basis
C. Periodic and effective use of cryptographic sanitization tools
D. The use of automated analysis tools such as SIM, SIEM, and SEM solutions

20. Of the following, which is probably the most significant risk in a managed cloud environment?
Response:

A. DDoS
B. Management plane breach
C. Guest escape
D. Physical attack on the utility service lines

21. ______ can often be the result of inadvertent activity. Response:

A. DDoS
B. Phishing
C. Sprawl
D. Disasters

22. Which of these characteristics of a virtualized network adds risks to the cloud environment? Response:
A. Redundancy
B. Scalability
C. Pay-per-use
D. Self-service

23. Which network protocol is essential for allowing automation and orchestration within a cloud environment? Response:
A. DNSSEC
B. DHCP
C. IPsec
D. VLANs

24. If bit-splitting is used to store data sets across multiple jurisdictions, how may this enhance security? Response:
A. By making seizure of data by law enforcement more difficult
B. By hiding it from attackers in a specific jurisdiction
C. By ensuring that users can only accidentally disclose data to one geographic area
D. By restricting privilege user access

25. Although indirect identifiers cannot alone point to an individual, the more of them known can lead to a specific identity. Which strategy can be used to avoid such a
connection being made?
Response:
A. Masking
B. Anonymization
C. Obfuscation
D. Encryption

26. Which type of cloud-based storage is IRM typically associated with? Response:
A. Volume
B. Unstructured
C. Structured
D. Object

27. A loosely coupled storage cluster will have performance and capacity limitations based on the ______.
Response:
A. Physical backplane connecting it
B. Total number of nodes in the cluster
C. Amount of usage demanded
D. The performance and capacity in each node

28. Which of the following would NOT be used to determine the classification of data?
Response:
A. Metadata
B. PII
C. Creator

D. Future use

29. You are the security manager for a small retail business involved mainly in direct e-commerce transactions with individual customers (members of the public). The
bulk of your market is in Asia, but you do fulfill orders globally.
Your company has its own data center located within its headquarters building in Hong Kong, but it also uses a public cloud environment for contingency backup
and archiving purposes. Your company has decided to expand its business to include selling and monitoring life-support equipment for medical providers.
What characteristic do you need to ensure is offered by your cloud provider? Response:

A. Full automation of security controls within the cloud data center
B. Tier 4 of the Uptime Institute certifications
C. Global remote access
D. Prevention of ransomware infections

30. Which type of web application monitoring most closely measures actual activity? Response:

A. Synthetic performance monitoring
B. Real-user monitoring (RUM)
C. Security information and event management (SIEM)
D. Database application monitor (DAM)

31. Which of the following is a risk that stems from a virtualized environment? Response:

A. Live virtual machines in the production environment are moved from one host to another in the clear.
B. Cloud data centers can become a single point of failure.
C. It is difficult to find and contract with multiple utility providers of the same type (electric, water, etc.).
D. Modern SLA demands are stringent and very hard to meet.

32. ______ is perhaps the main external factor driving IAM efforts. Response:

A. Regulation
B. Business need
C. The evolving threat landscape
D. Monetary value

33. Which of the following is perhaps the best method for reducing the risk of a specific application not delivering the proper level of functionality and performance
when it is moved from the legacy environment into the cloud?
Response:

A. Remove the application from the organization’s production environment, and replace it with something else.
B. Negotiate and conduct a trial run in the cloud environment for that application before permanently migrating.
C. Make sure the application is fully updated and patched according to all vendor specifications.
D. Run the application in an emulator.

34. Setting thermostat controls by measuring the temperature will result in the ______ highest energy costs. Response:

A. Server inlet
B. Return air
C. Under-floor
D. External ambient

35. Maxwell is developing a Data Loss Prevention (DLP) strategy. He is working with a pharmaceutical company that needs to control their sensitive content, in particular the formulas their chemist have created in Research and Development(R&D). Which component of a DLP solution will great deal of work have to be done to **begin to protect that content**?

A. Discovery

B. Encryption

C. Enforcement

D. Monitoring

Chapter6

36. Carla is assigned to manage her organization’s privacy program and is working to communicate to customers about a change in the organization’s privacy practices. She plans to send an email notifying customers of the change and allowing them to opt out of the use of their data. Which GAPP principle is not described in this scenario?

A. Notice

B. Management

C. Access

D. Choice and Consent

37. You’re a medical student at a private research university in the midwestern United States; you make your tuition payments directly from your bank account via a debit card. Which of the following laws and standards will not be applicable to you, your personal data, or the data you work with as a student?

A. Sarbanes–Oxley Act (SOX)

B. Health Information Portability and Accountability Act (HIPAA)

C. Payment Card Industry Data Security Standards (PCI DSS)

D. Family Educational Rights and Privacy Act (FERPA)

38. Which type of business impact assessment tool is most appropriate when attempting to evaluate the impact of a failure on customer confidence?

A. Quantitative

B. Qualitative

C. Annualized loss expectancy

D. Reduction

39. During an IT audit, the CEO of a cloud provider demands regular updates on the testing process. How should auditors respond to this demand?

A. Refuse to provide the CEO with any information until the conclusion of the audit.

B. Refer the matter to the client’s Board of Directors.

C. Provide the CEO with regular updates.

D. Refer the matter to the audit firm’s partnership review board

40. Belinda is auditing the financial controls of a manufacturing company and learns that the financial systems are run on a major IaaS platform. She would like to gain assurance that the platform has appropriate security controls in place to assure the accuracy of her client’s financial statements. What action should she take?

A. Perform an IT audit of the cloud provider.

B. Obtain a SOC 1 report.

C. Obtain a SOC 2 report.

D. Continue testing only controls at the client and note the use of the cloud provider in her report

41. Tony is developing a business continuity plan and is having trouble prioritizing resources because of the difficulty of combining information about tangible and intangible assets. What would be the most effective risk assessment approach for him to use?

A. Quantitative risk assessment

B. Qualitative risk assessment

C. Neither quantitative nor qualitative risk assessment

D. Combination of quantitative and qualitative risk assessment

42. Which one of the following elements of information is not considered a direct identifier that would trigger most United States (U.S.) state data breach laws?

A. Student identification number

B. Social Security number

C. Driver’s license number

D. Credit card number

43. Fran recently conducted a review of the risk management program in her organization and developed an analysis of all of the risks facing the organization and their quantitative impact. What term best describes this analysis?

A. Risk appetite

B. Risk tolerance

C. Risk controls

D. Risk profile

44. Aaron is concerned about the possibility that a cloud vendor that his organization relies on may go out of business. What term best describes this risk?

A. Vendor lock-in

B. Vendor viability

C. Vendor lockout

D. Vendor diversity

45. Elise is helping her organization prepare to evaluate and adopt a new cloud-based human resource management (HRM) system vendor. What would be the most appropriate minimum security standard for her to require of possible vendors?

A. Compliance with all laws and regulations

B. Handling information in the same manner the organization would

C. Elimination of all identified security risks

D. Compliance with the vendor’s own policies

46. Which of the following statements about SSAE-18 is not correct?

A. It mandates a specific control set.

B. It is an attestation standard.

C. It is used for external audits.

D. It uses a framework, including SOC 1, SOC 2, and SOC 3 reports.

47. Matt works for a telecommunications firm and was approached by a federal agent seeking assistance with wiretapping one of Matt’s clients pursuant to a search warrant. Which one of the following laws requires that communications service providers cooperate with law enforcement requests?

A. ECPA

B. CALEA

C. Privacy Act

D. HITECH Act

48. Which of the following is not an enforceable governmental request?

A. Warrant

B. Subpoena

C. Court order

D. Affidavit

49. Nitesh is conducting a global audit of a multinational cloud service provider and has a question about appropriate testing procedures. Which one of the following documents would be most applicable to his situation?

A. ISAE 3402

B. ISAE 3410

C. SSAE 16

D. SSAE 18

50. Which of the following is probably the most volatile form of data that might serve a forensic purpose in a virtualized environment?

A. Virtual instance RAM

B. Hardware RAM

C. Hypervisor logs

D. Drive storage

51. Wanda is working with one of her organization’s European Union business partners to facilitate the exchange of customer information. Wanda’s organization is located in the United States. What would be the best method for Wanda to use to ensure GDPR compliance?

A. Binding corporate rules

B. Privacy Shield

C. Standard contractual clauses

D. Safe harbor

52. Bella is working to develop a long-term relationship with a consulting firm that will assist in her organization’s cloud migration. She would like to create a contract that may govern the terms of many different projects. What type of document should she create?

A. MSA

B. BPA

C. SOW

D. MOU

53. _________________ is the legal concept whereby a cloud customer is held to a reasonable expectation for providing security of its users’ and clients’ privacy data.

A. Due care

B. Due diligence

C. Liability

D. Reciprocity

54. Chris is worried that the laptops that his organization has recently acquired were modified by a third party to include keyloggers before they were delivered. Where should he focus his efforts to prevent this?

A. His supply chain

B. His vendor contracts

C. His post-purchase build process

D. The original equipment manufacturer (OEM)

55. Greg is evaluating a new vendor that will be supplying networking gear to his organization. Due to the nature of his organization’s work, Greg is concerned that an attacker might attempt a supply chain exploit. Assuming that both Greg’s organization and the vendor operate under reasonable security procedures, which one of the following activities likely poses the greatest supply chain risk to the equipment?

A. Tampering by an unauthorized third party at the vendor’s site

B. Interception of devices in transit

C. Misconfiguration by an administrator after installation

D. Tampering by an unauthorized third party at Greg’s site

56. What is an accounting report on controls at a service organization that replaces older SAS 70 type reports?

A. SOC 1

B. SSAE 16

C. GAAP

D. SOC 2

57. Which one of the following frameworks is a U.S. federal law governing privacy?

A. PCI DSS

B. CCPA

C. GDPR

D. HIPAA

58. Which one of the following individuals is normally responsible for fulfilling the operational data protection responsibilities delegated by senior management, such as validating data integrity, testing backups, and managing security policies?

A. Data custodian

B. Data owner

C. Data user

D. Auditor

59. When an organization uses a cloud service provider to handle protected health information, who is responsible for securing that data?

A. Customer

B. Cloud provider

C. Both the customer and the cloud provider

D. Neither the customer nor the cloud provider

60. What term is used to describe an individual within an organization who has been delegated day-to-day responsibility for decision-making about a category of information?

A. Data owner

B. Data custodian

C. Data processor

D. Data steward

61. Which of the following would normally be considered a supply chain risk? (Choose all that apply.)

A. Adversary tampering with hardware prior to being shipped to the end customer

B. Adversary hacking into a web server run by the organization in an IaaS environment

C. Adversary using social engineering to compromise an employee of an SaaS vendor to gain access to customer accounts

D. Adversary conducting a denial-of-service attack using a botnet

62. Based on the information in this scenario, what is the annualized loss expectancy for a tornado at Atwood Landing's datacenter?

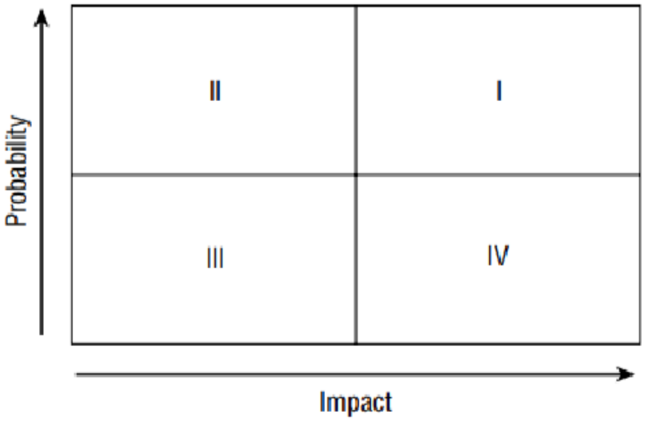
A. $25,000

B. $50,000

C. $250,000

D. $500,000

63. The Domer Industries risk assessment team recently conducted a qualitative risk assessment and developed a matrix similar to the one shown here. Which quadrant contains the risks that require the most immediate attention?



A. I

B. II

C. III

D. IV

64. Which one of the following metrics would not commonly be found in an SLA?

A. Network performance

B. Compute capacity

C. Help desk response time

D. Number of security incidents

65. Which of the following is probably least suited for inclusion in the service-level agreement (SLA) between a cloud customer and cloud provider?

A. Bandwidth

B. Jurisdiction

C. Storage space

D. Availability

66. Which cloud storage type uses an opaque value or descriptor to categorize and organize data?
Response:
A. Volume
B. Object
C. Structured
D. Unstructured

67. Which of the following best describes SAML? Response:
A. A standard for developing secure application management logistics
B. A standard for exchanging authentication and authorization data between security domains
C. A standard for exchanging usernames and passwords across devices
D. A standard used for directory synchronization

68. When considering the option to migrate from an on-premises environment to a hosted cloud service, an organization should weigh the risks of allowing external
entities to access the cloud data for collaborative purposes against ______.
Response:
A. Not securing the data in the legacy environment
B. Disclosing the data publicly
C. Inviting external personnel into the legacy workspace in order to enhance collaboration
D. Sending the data outside the legacy environment for collaborative purposes

69. Very detailed logging should be in place for which of the following?

A. Only specific levels of virtualization structure
B. Each level of virtualization infrastructure, as well as wherever the client accesses the management plane
C. Only access to the hypervisor and the management plane
D. Wherever the client accesses the management plan

70. An engineer has been asked by her supervisor to determine how fast each system must be back up and running after a disaster has occurred to meet BCDR objectives. What has this engineer been asked to determine?

A. RPO
B. RTO
C. RSL
D. MTR

71. A security engineer is implementing mechanisms that are used to allow and deny possible actions on the network. What are these mechanisms called?

A. Security Controls
B. Firewall
C. BCDR
D. Security Regulation

72. A cloud engineer needs to access the cloud environment remotely for administration purposes. The MOST common ways for engineers to get administrative access are via VPN tunnels and which of the following?

A. Jump Server
B. Federated Server
C. Virtual Switches
D. Hypervisors

73. A cloud engineer needs to ensure a seamless transition to the BCDR site in the event of a disaster. What must the engineer have in place to accomplish this?

A. Numerous Hypervisors
B. Redundant internet provider
C. Failover Mechanism
D. Web API

74. Which of the following is NOT one of the main risks that needs to be assessed during the "assess risk" phase of developing a BCDR plan?

A. Load capacity at the BCDR site
B. Legal and Contractual issues
C. Budgetary Restraints
D. Migration of services

75. An engineer working in a data center noticed that the humidity level was 80% relative humidity. What threat could this cause to systems?

A. 80% relative humidity is within the ideal range, so it does not pose any risk to systems
B. Systems may overheat and fry internal Components
C. Excess electrostatic discharge could damage systems
D. Condensation may form causing water damage

76. Which of the following BEST describes the types of applications that create risk in a cloud environment?

A. Full application suites
B. Software with administrator privileges
C. Small utility scripts
D. Every piece of software in the environment

77. During periods of high utilization, cloud providers must prioritize which systems will be given resources in the event that there are not enough resources for all systems.
Which is the term used to describe this concept?
A. Share
B. Reservation
C. Limits
D. Pooling
78. Aden works for a large corporation that maintains its own traditional datacenter. How many computers is this data center likely to house?
A. Tens
B. Hundreds
C. Thousands
D. Hundred Thousand

79. Storage in the cloud typically consists of:
A. NAS and VLANS
B. RAID and VLANS
C. RAID and SANS

D.VLANS and SANs

80. Which of the following is NOT a protection technique for virtualization systems?

A. Standard Configurations
B. Least Privilege
C. Privilege Access
D. Separation of duties

81. Which type of storage system places files in a flat organization of containers and uses IDs to retrieve them?
A. Software Defined Networks
B. Object Storage
C.LUN
D. Volume Storage

82. The recovery point objective can be zero in a cloud environment, with what other technology implemented?

A. Availability Zone
B. Load Balancer
C. Failover
D. Compute resources

83. Which is NOT an overall countermeasure strategy to mitigate risks in the cloud environment?
A. Security by Design
B. User Education
C. Due Diligence
D. Secure Configuration management

84. It's extremely difficult, if not impossible, to find a location for a data center that is not at risk of being hit by some type of natural disaster. Which of the following can be used to help mitigate the threats of natural disasters?

A. Multitenancy
B. Encryption
C. Reinforced walls
D. Rapid Elasticity

85. What is the purpose of hot/cold aisles?
A. Hot aisles are used in colder climates, while cold aisles are mainly used in warmer client
B. To avoid one row of rack pushing hot air directly into another row
C. Servers are placed in cold aisle, while network equipment is placed in hot aisle
D. Some systems require more more cooling than others, so systems are separate into hot and cold flow

86. Of the following examples, which is NOT a risk associated with having a BCDR plan?
A. Maintaining redundancy
B. Location changes
C. Functionality and external services
D. Budget

87. There are many ways to handle risk. However, the usual methods for addressing risk are not all possible in the cloud because ___________________.

A. Cloud data risks cannot be mitigated
B. Migrating into a cloud environment necessarily means you are accepting all risks

C. Some risks cannot be transferred to a cloud provider
D. Cloud providers cannot avoid risk

88. Cloud providers will probably not allow ___________________ as part of a customer's penetration test.
A. Network mapping
B. Vulnerability scanning
C. Reconnaissance
D. Social engineering

89. Which of the following controls would be useful to build into a virtual machine baseline image for a cloud environment?
A. GPS tracking/locator
B. Automated vulnerability scan on system startup
C. Access control list (ACL) of authorized personnel
D. Write protection

90. Where should multiple emergency egress points be included?
A. At the power distribution substation
B. Within the datacenter
C. In every building on the campus
D. In the security operations center

91. Which of the following terms describes a means to centralize logical control of all networked nodes in the environment, abstracted from the physical connections to each?
A. Virtual private network (VPN)
B. Software-defined network (SDN)
C. Access control lists (ACLs)
D. Role-based access control (RBAC)

92. What can hamper the ability of a cloud customer to protect their assets in a managed services arrangement?
A. Prohibitions on port scanning and penetration testing
B. Geographical dispersion
C. Rules against training users
D. Laws that prevent them from doing so

93. Charles is the BC/DR program manager for a cloud service provider. He is assessing the risks facing his program. He believes that the organization has done adequate BC/DR planning but they have never actually activated the plan. Which of the following would most likely pose the most significant risk to the organization?
A. Not having essential BC/DR personnel available during a contingency
B. Not including all BC/DR elements in the cloud contract
C. Returning to normal operations too soon
D. Telecommunications outages

94. Warren is working with a cloud service provider on the terms of a new service that his organization will depend on as a disaster recovery capability. Which one of the following actions will provide Warren with the best assurance that the service will function correctly?
A. Audit all performance functions.
B. Audit all security functions.
C. Perform a full-scale test.
D. Mandate this capability in the contract.

95. What term describes the process of granting users access to resources?
A. Identification

B. Authentication
C. Authorization
D. Federation

96. A Security Assertion Markup Language (SAML) identity assertion token uses the ___________________ protocol.
A. Extensible Markup Language (XML)
B. Hypertext Transfer Protocol (HTTP)
C. Hypertext Markup Language (HTML)
D. American Standard Code for Information Interchange (ASCII)

97. The BC/DR plan/policy should include all of the following except ___________________.
A. Tasking for the office responsible for maintaining/enforcing the plan
B. Contact information for essential entities, including BC/DR personnel and emergency services agencies
C. Copies of the laws/regulations/standards governing specific elements of the plan
D. Checklists for BC/DR personnel to follow

98. Which one of the following audit mechanisms would be able to provide the most accurate reconstruction of user activity?
A. Application logs
B. Security logs
C. Netflow records
D. Packet capture

99. Melissa uses the snapshot capabilities of her cloud service provider to make backup copies of the disk volumes that support her virtual machines. What type of storage is most likely used to store these backups?
A. Dedicated disks
B. Block
C. Encrypted
D. Object

100. Which one of the following services would be least likely described as providing computing capability?
A. Virtual server instances
B. FaaS
C. Object storage
D. Containers

101. You are in charge of creating the business continuity and disaster recovery (BC/DR) plan and procedures for your organization. Your organization has its production environment hosted by a cloud provider, and you have appropriate protections in place. Which of the following is a significant consideration for your BC/DR backup?

A. Enough personnel at the BC/DR recovery site to ensure proper operations
B. Good cryptographic key management
C. Access to the servers where the BC/DR backup is stored
D. Forensic analysis capabilities

102. You are in charge of creating the business continuity and disaster recovery (BC/DR) plan and procedures for your organization. You decide to have a tabletop test of the BC/DR activity. Which of the following will offer the best value during the test?

A. Have all participants conduct their individual activities via remote meeting technology.

B. Task a moderator well versed in BC/DR actions to supervise and present scenarios to the participants, including randomized special events.
C. Provide copies of the BC/DR policy to all participants.
D. Allow all users in your organization to participate

103. "Return to normal operations" is a phase in BC/DR activity when the emergency is over and regular production can resume. Which of the following can sometimes be the result when the organization uses two different cloud providers for the production and BC/DR environments?

A. Both providers are affected by the emergency, extending the time before return to normal can occur. B. The BC/DR provider becomes the new normal production environment.
C. Regulators will find the organization in violation of compliance guidance.
D. All data is lost irretrievably

104. Ursula is examining several virtual servers that her organization runs in an IaaS service. She discovers that the servers are all running a scheduling service that is no longer used by the organization. What action should she take?
A. Ensure the service is fully patched.
B. Remove the service.
C. Leave the service alone unless it is causing issues.
D. Contact the vendor for instructions.

105. You are designing a cloud datacenter that is expected to meet Tier 2 status according to the Uptime Institute standards. What level of availability must you achieve to meet this standard?
A. 99.422%
B. 99.671%
C. 99.741%
D. 99.995%

106. Risk should always be considered from a business perspective. When a risk is accepted, it should be balanced by a corresponding ___________________.
A. Profit
B. Performance
C. Cost
D. Opportunity

107. Best practice for planning the physical resiliency for a cloud datacenter facility includes ___________________.
A. Having one point of egress for personnel
B. Ensuring that redundant cabling/connectivity enters the facility from different sides of the building/property
C. Ensuring that all parking areas are near generators so that personnel in high-traffic areas are always illuminated by emergency lighting, even when utility power is not available
D. Ensuring that the foundation of the facility is rated to withstand earthquake tremors

108. Jason operates a cloud datacenter and would like to improve the ability of administrators to interact programmatically with backend solutions on the management plane. What technology can he use to best allow this type of automation?
A. CASB
B. API
C. Hypervisor
D. Python

109. Cameron is worried about distributed denial-of-service (DDoS) attacks against his company's primary web application. Which of the following options will provide the most resilience against large-scale DDoS attacks?

A. Implement a CDN.
B. Increase the number of servers in the web application server cluster.
C. Contract for DDoS mitigation services via the company's ISP.
D. Increase the amount of bandwidth available from one or more ISPs.

110. Alyssa's team recently implemented a new system that gathers information from a variety of log sources, analyzes that information, and then triggers automated playbooks in response to security events. What term best describes this technology?
A. SIEM
B. Log repositories
C. IPS
D. SOAR

111. Candace is designing a backup strategy for her organization's file server. She would like to perform a backup every weekday that has the smallest possible storage footprint. What type of backup should she perform?
A. Incremental backup
B. Full backup
C. Differential backup
D. Transaction log backup

112. Carla is developing the design of a cloud infrastructure service offering that she will be reselling to a number of customers. What component of her stack is most directly responsible for performing tenant partitioning of the virtual machines belonging to different customers?
A. Access control lists
B. Network security group
C. Firewall
D. Hypervisor

113. Barry is the CIO of an organization that recently suffered a serious operational issue that required activation of the disaster recovery plan. He would like to conduct a lessons learned session to review the incident. Who would be the best facilitator for this session?
A. Barry, as chief information officer
B. Chief information security officer
C. Disaster recovery team leader
D. External consultant

114. Carolyn is concerned that users on her network may be storing sensitive information, such as Social Security numbers, on their hard drives without proper authorization or security controls. What third-party security service can she implement to best detect this activity?
A. IDS
B. IPS
C. DLP
D. TLS

115. Which of the following is a benefit of using a proprietary or vendor API rather than using an open source API?

A. Ability to change the code
B. Ability to review code
C. Formal Patch management
D. Free to use

116. Organizations such as the Cloud Security Alliance (CSA) and the Open Web Application Security Project (OWASP) publish information about cloud threats and risks. Who is responsible for mitigating these risks in an organization?

A. CSP
B. Security Professional
C. Executive Management
D. Database administrator

117. What is OAuth used for?

A. Authentication
B. Federation
C. Identification
D. Authorization

118. Which API relies on the HTTP protocol to support data formats such as XML an JSON?

A. SOP
B. REST
C. SOAP
D. FTP

119. Which of the following is listed on the Cloud Security Alliance's Treacherous Twelve, but NOT listed on the OWASP Top 10?

A. XML External Entities
B. Denial of Service
C. Injection
D. Broken Access Control

120. An application developer has left references regarding the configuration of the hosting system in his code. An attacker was able to find this information in the code and use it to access the application without needing to go through proper validation.

This is an example of what type of vulnerability?

A. XML External Entities
B. Cross-Site Scripting
C. Broken Access Control
D. Injection

121. A malicious actor created a free trial account for a cloud service using a fake identity. Once the free trial cloud environment was up and running, he used it as a launch pad for several cloud-based attacks. Because he used a fake identity to set up the free trial, it would be difficult (if not impossible) for the attacks to be traced back to him.

What type of cloud-based threat is being described here?

A. Shared Technology Issue
B. Advanced persistence Threat
C. Abuse & nefarious use of cloud services

D. Denial of service

122. Which of the following statements regarding SOAP and REST is TRUE?

A. REST only allows the use of XML formatted data
B. REST is typically only used when technical limitations prevent the use of SOAP
C. SOAP supports wide variety of data formats include both JSON and XML
D. SOAP does not allow for caching, making it less scalable and having lower performance than REST

123. When conducting functional testing, which is NOT an important consideration?
A. Testing must design to exercise all requirements
B. Testing must of sufficient to have reasonable assurance there are no bugs
C. Testing must use limited information about the application
D. Testing must be realistic for all the environments

124. Which of the following types of security tests would be considered a "white-box" test?

A. SAST
B. Vulnerability scanning
C. Penetration Testing
D. DAST

125. Company A needs to have a way for employees within their organization, as well as partners and customers, to authenticate and access data in their cloud

Which of the following authentication mechanisms would be the BEST choice for Company A to implement?

A. SOAP
B. Single Sign On
C. REST
D. Federated Identity management

126. An attacker is trying to steal data regarding a new product that an organization is developing. The attacker has planted malware on the system and has left it on the system for eight months. What is the name of this type of attacker?

A. Insecure API
B. Advanced Persistent Threat
C. Malicious Insider
D. Worm

127. An organization needs to use multiple data formats, including both JSON and XML, in their cloud deployment. Which API type should they use?

A. SAST
B. DAST
C. SOAP
D. REST

128. At the conclusion of which phase of the software development lifecycle (SDLC), will there be formal requirements and specifications ready for the development team to turn into actual software?

A. Analysis
B. Testing
C. Design
D. Requirement gathering and feasibility

129. Securing supply chain management software in the cloud and securely connecting vendors globally through cloud services reduces what type of risk?

A. Cloud-related risk
B. IT-related risk
C. Software related-risk
D. Application related- risk

130. Which of the following would be the BEST way to mitigate the risk of sensitive data exposure on web applications?

A. Session token validation
B. Encryption
C. Anti-Malware
D. Input Validation

131. Which of the following can make it difficult for a software developer using a public cloud to receive a security certification for their application?

A. Many regulation require that application be built in physical data center to be considered secure
B. The cost of auditing a cloud environment is much higher than the cost of auditing a physical data center
C. The cloud provider may not be willing to allow auditors the level of access needed to certify their environment
D. Cloud environment inherently less secure than physical environment

132. Of the following, performing checks against client browsers to ensure they meet security standards can help to mitigate which vulnerability?

A. Insufficient Logging
B. Sensitive Data exposure
C. Injection
D. XML external entities

133. Your current SaaS solution provider uses an independent CSP for some of their storage needs. What type of risk does this introduce to the organization?

A. Privacy Risk
B. Legal Risk
C. Fourth party risk
D. Outsourced Risk

134. What process is oriented around service delivery of the application service produced in modern DevOps / DevSecOps and occurs at all phases to provide continuous improvement and quality tracking?

A. Threat Modeling
B. Software Assurance
C. Software Configuration management
D. Quality Assurance

135. Mikayla wants to validate a component of her software that she has downloaded from GitHub. How can she validate that the underlying software does not have security flaws when it is downloaded and included in her environment as part of her integration process?

A. Validate the checksum of the file.
B. Validate the signature of the file.
C. Validate the hash of the file.
D. Mikayla cannot ensure that there are no security flaws via the options described.

136. Lin wants to allow her users to use existing credentials provided by a third-party identity
provider when they access her service. What element will she have to provide from the following list?

A. User IDs
B. Authentication
C. Authorization
D. Identity proofing

137. Nick wants to avoid common pitfalls in his CI/CD pipeline. Which of the following is a common CI/CD pitfall that can harm cloud development efforts?

A. Automation of processes
B. Use of metrics
C. Using multiple deployment paths
D. Reliance on a version control system

138. The CWE/SANS Top 25 most dangerous software errors includes the use of hard-coded
credentials. What common cloud service component can be used to avoid this problem for
cloud-hosted
software and applications?

A. An MFA token
B. A TPM
C. A KMS
D. An API key

139. The company that Yun works for provides API access to customers. Yun wants to rate-limit API access and gather billing information while using a central authorization and access management system. What type of tool should Yun put in place to meet these requirements?

A. An API gateway
B. An API proxy
C. An API firewall
D. A next-generation API manager

140. What phase of the SDLC is IAST typically associated with?

A. Design
B. Testing
C. Implementation
D. Deployments

141. Lori wants to ensure that the included software components provided by her vendor are
secure. What type of process should she use to conduct an assessment of those packages?

A. A web application vulnerability scan
B. A software composition analysis
C. A vulnerability scan
D. A version number validation process

142. Ian wants to use a cloud-specific list of application issues. Which of the following options should he choose?
A. The OWASP Top 10
B. The NIST Dirty Dozen
C. The SANS Top 25
D. The MITRE ATT&CK-RS

143. Yasmine is working with a software as a service vendor. What part of the environment does Yasmine's company have responsibility for?
A. Applications and data storage.
B. The OS, middleware, and runtime.
C. Storage and networking.
D. The vendor is responsible for the environment.

144. Ramon's organization uses Office 365 but relies on their own Active Directory credentials to log into O365. What is this type of configuration called?
A. Federated identity
B. Structured identity
C. Shared identity
D. Constrained identity
145. Aisha's organization has deployed a cloud application security broker. Which of the following is not a typical purpose for a CASB to be deployed?
A. To control usage-based costs
B. To limit access based on service categories
C. To help limit the potential for sensitive data loss
D. To detect anomalous usage patterns

146. Ian is using a CASB to control usage of cloud services. He wants to ensure that users in his organization only use cloud services that are approved for their role. What two elements should he define in his rules to most effectively accomplish this?
A. Identity and activity
B. Activity and data
C. Identity and service
D. Service and data

147. Jacinda's manager has asked her to set up a sandbox environment to help validate third-party software before it is run. What should Jacinda prepare an environment to handle?
A. Optimizing the production environment by moving processes that are not frequently used into the sandbox
B. Allowing secure remote access for users who need resources in the cloud environment
C. Running malware for analysis purposes
D. Creating secure subnets of the production environment

148. Sandboxing can often be used for ___________________.
A. Testing user awareness and training
B. Testing API security
C. Testing software before putting it into production
D. Testing software to validate its compliance with regulatory requirements

149. Kwame wants to limit the impact of potentially compromised secrets in his environment. What should he do to most effectively limit the issues compromised secrets can cause?
A. Extend secrets lifecycle.
B. Rotate secrets.
C. Replace secrets with tokens.
D. Implement a secret expiration list.

150. Kristen wants to filter her SAML traffic for potential attacks, including rate-limiting requests and validating content. Which of the following solutions is purpose-built for this type of security design?
A. A DAM with OpenID support
B. A SAML compliant IDS
C. An XML firewall
D. A WAF

151. Christina is following a typical SDLC process and has completed the planning phase. What phase typically follows the Planning phase in most SDLCs?
A. Design
B. Deployment
C. Maintenance
D. Requirements Gathering

152. Gabriel’s organization wants to ensure that their open source software is properly licensed. What should they were do?
A. Contact the authors of each component to request permission to use them.
B. Engage a third-party
license management vendor to ensure compliance with the licenses.
C. Pay appropriate licensing fees to the licensing organization for each software component.
D. Review the licenses for each component to ensure they are in compliance.

153. Sofia is preparing a list of the likely attacks against her APIs. Which of the following is not a common attack against APIs?
A. Injection
B. Malware
C. Distributed denial-of- service
D. Credential stuffing

154. James has created monitoring instrumentation for his application and uses the instrumentation to assess performance as well as function during the QA stage of his SDLC. What type of software validation methodology is he using?
A. IAST
B. Interactive DST
C. SCA
D. Structured DST

155. Lisa wants to ensure that the open source software package she has downloaded is legitimate. The software download site provides an SHA2 hash, a cryptographic signature, a file size, and a version number. Which of these options provides the greatest level of certainty?
A. The SHA2 hash
B. The cryptographic signature
C. The file size
D. The version number

156. Michelle is using the SAFECode Fundamental Practices for Secure Software Development as an underlying foundation for her organization’s development practices. She wants to develop an encryption strategy and knows that SAFECode describes how to do so. Which of the following is not a best practice for developing an encryption strategy for applications according to SAFECode?

A. Ensuring encryption algorithms cannot be changed easily
B. Defining what to protect
C. Assessing what encryption mechanisms meet the organization's requirements
D. Deciding on a key management solution

157. In a platform as a service (PaaS) model, who should most likely be responsible for the security of the applications in the production environment?
A. Cloud customer
B. Cloud provider
C. Regulator
D. Programmers

158. Jessica’s quality assurance testing process involves identifying software flaws, including business logic flaws and other coding mistakes. What type of testing should she perform to most effectively identify underlying code quality issues?
A. Static testing
B. Black box testing
C. Dynamic testing
D. Software composition analysis

159. Carmen’s organization wants to provide awareness training using a community-based web application security guide. What community standard is best suited to this type of training?
A. ASVS
B. CVE
C. OWASP
D. NIST

160. Henry uses an IAST process as part of his SLDC. What SDLC phase is IAST most likely to occur in?
A. Planning
B. Building
C. Deployment
D. Testing

161. Where is the BIOS stored?
A. Memory
B. Disk
C. Firmware
D. System Board

162. An engineer is helping to design and build a new data center. She knows that there are many institutions that create standards which govern the physical design of data centers.
Of the following, which is NOT an institution that creates standards governing the physical design of data centers?

A. NFPA
B. ITIL
C. IDCA
D. Uptime Institute

163. Your organization is in the process of migrating to the cloud. Mid-migration you come across details in an agreement that may leave you non-compliant. Who would be the BEST contact to discuss your cloud environment compliance with legal jurisdictions?

A. Regulator
B. Stakeholder
C. Partner
D. Consultant

164. At which point during the incident response process are new security controls implemented?

A. Respond
B. Detect
C. Prepare
D. Post-Incident
E. Recover

165. What is the final step in deploying a newly upgraded application into production?

A. Configuration Management
B. Change management
C. Release Management
D. Service Level Management

166. What is used to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems?

A. DNS Sinkhole
B. Jumpbox
C. IDS
D. Honeypots

167. An engineer needs to create a baseline image. What is the FIRST step this engineer needs to take to create a baseline image?

A. Disable Unnecessary services
B. Perform a clean install of OS
C. Update all drivers
D. Install Updates and service packs

168. Incident classification is determined based on what two criteria?

A. Impact and urgency
B. Incident type and time of day
C. Time of day and urgency
D. Incident Type and impact

169. Which management strategy is focused on the required system resources needed to deliver performance at an acceptable level to meet SLA requirements and in a cost-effective manner?

A. Availability Management
B. Release and Deployment Management
C. Capacity Management
D. Configuration Management

170. Which of the following is NOT one of the tiers documented in the Uptime Institute's Data Center Site Infrastructure Tier Standard Topology?

A. Redundant Capacity components
B. Basic Capability
C. Redundant maintainability
D. Fault Tolerance

171. What management strategy encompasses planning, coordinating, execution, and validation of changes and rollouts to the production environment?

A. Change Management
B. Configuration Management
C. Service Level Management

D. Release Management

172. The cloud administrator created a VM in Azure and accidently removed all network access from it, effectively locking themselves out. What are the other options for the administrator to regain access?

A. Contact Microsoft
B. Console Access
C. RDP
D. Jumpbox
E. None of the options are correct

173. When designing and building out a cloud data center, which component requires the MOST security, as a compromise of this could lead to a compromise of all hosted systems?

A. Hypervisor
B. Virtual router
C. Management plane
D. Virtual Machine

174. To take a snapshot and backup a virtual machine, which of the following backup solutions is typically used?

A. Snapshots
B. All options are correct
C. Agentless
D. Agent-based

175. Which of the following is NOT one of the four key areas of the physical cloud environment?

A. Cabling
B. Network
C. Disk
D. CPU

176. In an infrastructure as a service (IaaS) arrangement, who accepts responsibility for securing cloud-based
applications?
A. The cloud provider
B. The cloud customer
C. The regulator
D. The end user/client

177. Brenda’s company employs a number of application developers who create software to meet many different business needs. She is embarking on a project to validate the use of verified open source software and is concerned about the unknowing use of software libraries by those developers. Which of the following technologies will best assist with identifying these uses?

A. Dynamic application security testing (DAST)
B. Static application security testing (SAST)
C. Software composition analysis (SCA)
D. Interactive application security testing (IAST)

178. Carla works for an infrastructure as a service (IaaS) provider. She is analyzing the security settings for the hypervisors used in a multitenant environment. Who should have access to modify settings on those hypervisors?

A. Only employees of Carla’s company with the appropriate security training and access rights.
B. Employees of Carla’s company and customers with virtual machines running on that specific hypervisor.
C. Employees of Carla’s company and customers with appropriate security training.

D. None of these groups should have hypervisor access.

179. You work for a government research facility. Your organization often shares data with other government research organizations. You would like to create a single sign-on experience across the organizations, where users at each organization can sign in with the user ID/ authentication issued by that organization, then access research data in all the other organizations.Instead of replicating the data stores of each organization at every other organization (which is one way of accomplishing this goal), you instead want every user to have access to each organization's specific storage resources. What is the term for this kind of arrangement?
A. Public-key infrastructure (PKI)
B. Portability
C. Federation
D. Repudiation

180. Rusty is evaluating the security of a web-based SaaS application and wants to verify that the site provides strong encryption between the web server and the client. What is the most common way to achieve this goal?
A. Secure sockets layer (SSL)
B. DNS Security Extensions (DNSSEC)
C. Internet Protocol Secure (IPsec)
D. Transport layer security (TLS)

181. In what cloud computing service model is the customer responsible for installing and maintaining the operating system?
A. IaaS
B. PaaS
C. SaaS
D. FaaS

182. Darcy is an information security risk analyst for Roscommon Cloud Solutions. She is currently trying to decide whether the company should purchase an upgraded fire suppression system for their primary datacenter. The datacenter facility has a replacement cost of $2 million. After consulting with actuaries, datacenter managers, and fire subject matter experts, Darcy determined that a typical fire would likely require the replacement of all equipment inside the building but not cause significant structural damage. Together, they estimated that recovering from the fire would cost $750,000. They also determined that the company can expect a fire of this magnitude once every 50 years.
A. Based on the information in this scenario, what is the exposure factor for the effect of a fire on the Roscommon Cloud Solutions datacenter?
A. 7.5 percent
B. 15.0 percent
C. 27.5 percent
D. 37.5 percent

B. Based on the information in this scenario, what is the annualized rate of occurrence for a fire at the Roscommon Cloud Solutions datacenter?
A. 0.002
B. 0.005
C. 0.02
D. 0.05
C. Based on the information in this scenario, what is the annualized loss expectancy for a fire at the Roscommon Cloud Solutions datacenter?
A. $15,000
B. $25,000
C. $75,000
D. $750,000

183. Which of the following best describes threat modeling?

A. The idea of identifying specific points of vulnerability and then implementing countermeasures to protect or thwart those points from successful exploitation
B. The idea of finding points and then implementing countermeasures to protect or thwart those points from successful exploitation
C. The idea of identifying specific vulnerabilities and then patching them to protect or thwart them from successful exploitation
D. The idea of identifying specific intrusion points and implementing countermeasures to protect or thwart those points from successful intrusion

184. Gabriel's organization maintains a system of voting records. The system uses SHA3 to obscure the contents of sensitive records. What data obfuscation technique is this system using?
A. Hashing
B. Masking
C. Anonymization
D. Shuffling

185. You are the data manager for a retail company; you anticipate a much higher volume of sales activity in the final quarter of each calendar year than the other quarters. In order to handle these increased transactions, and to accommodate the temporary sales personnel you will hire for only that time period, you consider augmenting your internal, on-premises production environment with a cloud capability for a specific duration, and will return to operating fully on-premises after the period of increased activity. Which facet of cloud computing is *most* important for making this possible?
A. Broad network access
B. Rapid elasticity
C. Metered service
D. Resource pooling

186. Brad is assisting with the implementation of a cloud-based SaaS solution where users can post content that is viewed by other users. He is concerned that users might store executable content on the site that then might be executed automatically by the browsers of other site visitors. What type of vulnerability would permit this attack?
A. SQL injection
B. Cross-site scripting
C. Cross-site request forgery
D. Server-side request forgery

187. How does representational state transfer (REST) make web service requests?
A. XML
B. SAML
C. URIs
D. TLS

188. What type of cloud storage is typically used to provide disk volumes for use with virtual server instances that will store important long-term data?
A. Object storage
B. Block storage
C. Ephemeral storage
D. Archival storage

189. Which one of the following fire suppression systems is least likely to damage sensitive electronic equipment in a datacenter?
A. Wet pipe
B. Dry pipe
C. Preaction
D. Inert gas

190. Which one of the following standards is most likely to contain detailed technical requirements for a hardware security module (HSM) used in a cloud environment?

A. FIPS 140-2
B. PCI DSS
C. ISO 27017
D. Common Criteria

191. Which one of the following hash algorithms would *not* trigger this vulnerability?
A. MD4
B. MD5
C. SHA-1
D. SHA-256

192 . What is the most likely result of failing to correct this vulnerability?
A. All users will be able to access the site, but some may see an error message.
B. All users will be able to access the site.
C. Some users will be unable to access the site.
D. All users will be unable to access the site.

193. How can Arlene correct this vulnerability?
A. Reconfigure the VPN server to only use secure hash functions.
B. Request a new certificate.
C. Change the domain name of the server.
D. Implement an intrusion prevention system.

194. You are also concerned about the availability of data stored on servers that support your organization's cloud services. You would like to add technology that would enable continued access to files located on the server even if a hard drive in a server fails. What integrity control allows you to add robustness without adding additional servers?
A. Server clustering
B. Load balancing
C. RAID
D. Scheduled backups

195. MTTR is best described as which of the following?
A. The average cost to repair a device that has failed or is in need of repair
B. The average time it takes to return a defective device to the manufacturer
C. The average time it takes to repair a device that has failed or is in need of repair
D. The time it takes to repair a device that has failed or is in need of repair

196. Which type of hypervisor has an operating system installed on the hardware and then the virtual manager software installed on top of it?
A. Type 1
B. Type 3
C. Type 2
D. Type 4

197. Carla is completing an IT audit that involves very sensitive log records that may later be disputed. She would like to collect a copy of the log records now and then protect them with a technology that will provide nonrepudiation. Which one of the following technologies would best meet her needs?
A. Multifactor authentication
B. Strong encryption
C. Cryptographic hash
D. Digital signature

198. You are the security manager for a small application development company. Your company is considering the migration of your testing environment to the cloud. As part of your testing methodology, you use several third-party
cloud testing vendors.
Which of the following traits of cloud functionality is probably the *most* crucial in terms of deciding which cloud provider you will choose?
A. Portability
B. Interoperability
C. Resiliency
D. Governance

199. Warren is helping his organization build a new datacenter that will support a cloud service they provide to their customers. Which one of the following is a reasonable minimum amount of time to expect the uninterruptible power supply (UPS) to provide power to the systems in the datacenter?
A. 10 minutes
B. 60 minutes
C. 3 hours
D. 12 hours

200. Gary is responsible for managing a large data set from a university research project that is stored with a cloud service provider in their object storage mechanism. He is concerned about managing costs of the service but also wants to make sure that they do not violate any legal obligations. The policies governing this data set specify a retention period of five years but note that litigation holds may override this requirement. Researchers rarely access data after 90 days but occasionally have a need to review older data.

a. Which one of the following actions should Gary take to minimize costs?
A. Set a lifecycle policy that moves data to archival storage after 90 days and destroys it after five years.
B. Set a lifecycle policy that moves data to archival storage after 90 days.
C. Set a lifecycle policy that destroys data after five years.
D. None of these actions are appropriate.

b. Gary receives a litigation hold notice for data related to tests performed in March 2022.
What should he do?
A. Suspend all data deletion.
B. Suspend deletion of data from March 2022 only.
C. Suspend all data archival.
D. None of these actions are necessary.

201. Which one of the following technologies is typically contained within a computer and manages the encryption keys used for full-disk encryption?
A. HSM
B. PKI
C. TPM
D. IPS

202. You are the IT security manager for a video game software development company. In order to test your products for security defects, your firm decides to use a small team of game testers recruited from a public pool of interested gamers who apply for a chance to take part.
This is an example of _______________.
A. Static testing
B. Dynamic testing
C. Code review
D. Open source review

203. Which one of the following principles imposes a standard of care upon an individual that is broad and equivalent to what one would expect from a reasonable person under the circumstances?
A. Due diligence
B. Separation of duties

C. Due care
D. Least privilege

204. Which one of the following storage types is typically the most inexpensive class of storage?
A. Block storage
B. Object storage
C. Archival storage
D. Raw storage

205. Andy is concerned that his organization is not meeting uptime requirements to their cloud service customers. Which one of the following ITIL control categories is least directly impacted?
A. Incident management
B. Change management
C. Availability management
D. Service level management

206. Brenda's organization recently completed the acquisition of a competitor firm. Which one of the following tasks would be *least* likely to be part of the organizational processes addressed during the acquisition?
A. Consolidation of security functions
B. Integration of security tools
C. Protection of intellectual property
D. Documentation of security policies

207. What is the term used to describe loss of access to data because the cloud provider has ceased operation?
A. Tokenization
B. Vendor lockout
C. Vendor lock-in
D. Masking

208. What technology can serve as a connection between the virtual guest operating system and the hypervisor, improving the services provided to the guest?
A. Virtualization sandbox.
B. Virtualization bridge.
C. Virtualization tools.
D. It is not advised to create a connection between the virtual guests and the hypervisor in order to preserve tenant isolation.

209 . Matt needs to revoke a digital certificate that is used as part of his organization's information rights management (IRM) program. Which one of the following options would best meet this need?
A. Update the certificate's OCSP record.
B. Add the certificate to the CRL.
C. Change the public key.
D. Change the private key.

210. You are the IT security subject matter expert for a hobbyist collective that researches and archives old music. Your collective is set up in such a way that the members own various pieces of the network themselves, pool resources and data, and communicate and share files via the internet. This is an example of what cloud model?
A. Hybrid
B. Private
C. Public
D. Community

211. You are the security manager for a small retailer engaged in e-commerce.
A large part of your sales is transacted through the use of credit and debit cards and you need to store these numbers for use in future transactions. You have determined that the costs of maintaining an encrypted storage capability in order to meet compliance requirements are prohibitive. What other technology can you use

instead to meet those regulatory needs?
A. Obfuscation
B. Masking
C. Tokenization
D. Hashing

212. Which one of the following actions might be taken as part of a business continuity plan?
A. Restoring from backup tapes
B. Implementing RAID
C. Relocating to a cold site
D. Restarting business operations

213. Carolyn is using ephemeral storage to process data in a machine learning application using a virtual server instance. Which one of the following best describes this storage?
A. It will remain until Carolyn explicitly deletes it.
B. It will be deleted if the server is rebooted.
C. It will be deleted only if the server is stopped.
D. It will be deleted only if the server is terminated.

214. Helen's organization handles large quantities of highly sensitive information. To help address this risk, she purchased a cyber-liability insurance policy. What type of risk response action is Helen taking?
A. Transfer
B. Avoid
C. Mitigate
D. Accept

215 . Which type of attack occurs when an application receives untrusted data and then sends it to a web browser without proper validation?
A. SQL injection
B. Brute-force
C. Cross-site
scripting (XSS)
D. Man-in-the-middle/on-path

216. The Transport Layer Security (TLS) protocol creates a secure communications channel over public media (such as the internet). In a typical TLS session, what form of cryptography is used for the session key?
A. Symmetric key
B. Asymmetric key pairs
C. Hashing
D. One asymmetric key pair

217. What component of a virtualized environment is responsible for enforcing tenant isolation?
A. Guest operating system
B. Hypervisor
C. Kernel
D. Protection manager

218. Which one of the following entities is dedicated to helping application developers improve software security?
A. ATASM
B. PASTA
C. DREAD
D. SAFEcode

219. Zeke is responsible for sanitizing a set of solid-state
drives (SSDs) removed from servers in his organization's datacenter. The drives will be reused on a different project.
Which one of the following sanitization techniques would be most effective?

A. Cryptographic erasure
B. Physical destruction
C. Degaussing
D. Overwriting

220. Tina would like to use a technology that will allow her to bundle up workloads and easily move them between different operating systems. What technology would best meet this need?
A. Virtual machines
B. Serverless computing
C. Hypervisors
D. Containers

221. Seth is helping his organization move their web server cluster to a cloud provider. The goal of this move is to provide the cluster with the ability to grow and shrink based on changing demand. What characteristic of cloud computing is Seth hoping to achieve?
A. Scalability
B. On-demand self service
C. Elasticity
D. Broad network access

222. Sherry is deploying a zero-trust network architecture for her organization. In this approach, which one of the following characteristics would be least important in validating a login attempt?
A. User identity
B. IP address
C. Geolocation
D. Nature of requested access

223. Which one of the following cybersecurity threats is least likely to directly affect an object storage service?
A. Disk failure
B. User error
C. Ransomware
D. Virus

224. Vince would like to be immediately alerted whenever a user with access to a sensitive cloud service leaves a defined physical area. What type of security control should he implement?
A. Intrusion prevention system
B. Geofencing
C. Firewall rule
D. Geotagging

225. Helen would like to provision a disk volume in the cloud that is mountable from a server. What cloud capability does she want?
A. Virtualized server
B. Object storage
C. Network capacity
D. Block storage

226. Which one of the following cryptographic goals protects against the risks posed when a device is lost or stolen?
A. Nonrepudiation
B. Authentication
C. Integrity
D. Confidentiality

227. Which type of business impact assessment tool is most appropriate when attempting to evaluate the impact of a failure on customer confidence?
A. Quantitative
B. Qualitative
C. Annualized loss expectancy
D. Single loss expectancy

228. What activity are cloud providers able to engage in because not all users will access the full capacity of their service offering simultaneously?
A. Oversubscription
B. Overprovisioning
C. Underprovisioning
D. Undersubscription

229. In an infrastructure as a service (IaaS) environment where a vendor supplies a customer with access to storage services, who is normally responsible for removing sensitive data from drives that are taken out of service?
A. Customer's security team
B. Customer's storage team
C. Customer's vendor management team
D. Vendor

230. Colin is reviewing a system that has been assigned the EAL7 evaluation assurance level under the Common Criteria. What is the highest level of assurance that he may have about the system?
A. It has been functionally tested.
B. It has been methodically tested and checked.
C. It has been methodically designed, tested, and reviewed.
D. It has been formally verified, designed, and tested.

231. Which one of the following systems assurance processes provides an independent third-party evaluation of a system's controls that may be trusted by many different organizations?
A. Planning
B. Definition
C. Verification
D. Accreditation

232 Which one of the following would be considered an example of infrastructure as a service cloud computing?
A. Payroll system managed by a vendor and delivered over the web
B. Application platform managed by a vendor that runs customer code
C. Servers provisioned by customers on a vendor-managed
virtualization platform
D. Web-based
email service provided by a vendor

233. When considering a move from a traditional on-premises
environment to the cloud, organizations often calculate a return on investment. Which one of the following factors should you expect to contribute the most to this calculation?
A. Utility costs
B. Licensing fees
C. Security expenses
D. Executive compensation

234. During a system audit, Casey notices that the private key for her organization's web server has been stored in a public Amazon S3 storage bucket for more than a year. What should she do?
A. Remove the key from the bucket.
B. Notify all customers that their data may have been exposed.
C. Request a new certificate using a new key.

D. Nothing, because the private key should be accessible for validation.

235. Glenda would like to conduct a disaster recovery test and is seeking a test that will allow a review of the plan with no disruption to normal information system activities and as minimal a commitment of time as possible. What type of test should she choose?
A. Tabletop exercise
B. Parallel test
C. Full interruption test
D. Checklist review

236. Darcy's organization is deploying serverless computing technology to better meet the needs of developers and users. In a serverless model, who is normally responsible for configuring operating system security controls?
A. Software developer
B. Cybersecurity professional
C. Cloud architect
D. Vendor

237. Which one of the following statements is correct?
A. Services that are scalable are also elastic.
B. There is no relationship between elasticity and scalability.
C. Services that are elastic are also scalable.
D. Services that are either elastic or scalable are both elastic and scalable.

238. Which one of the following programs provides a general certification process for computing hardware that might be used in a government environment?
A. FedRAMP
B. NIST 800-53
C. Common Criteria
D. FIPS 140-2

239. In a Lightweight Directory Access Protocol (LDAP) environment, each entry in a directory server is identified by a _____________.
A. Domain name (DN)
B. Distinguished name (DN)
C. Directory name (DN)
D. Default name (DN)

240. You are concerned about protecting sensitive data while it is stored in memory on a server. What emerging technology is designed to assist with this work?
A. Quantum computing
B. Confidential computing
C. Edge computing
D. Fog computing

241. Which one of the following disaster recovery approaches is generally the most cost-effective for an organization?
A. Hot site
B. Cloud site
C. Cold site
D. Warm site

242. Will wants to use containerized applications in his cloud-hosted environment. Which of the following is a best practice he should use as he builds them?
A. Package a single application per container.
B. Use default installs wherever possible.
C. Retain all normal tools and utilities.
D. Avoid tagging to reduce complexity.

243. Helen’s organization operates an e-commerce website housed by a cloud service provider. Which of the following compliance standards is she likely to have to comply with?
A. PCI DSS
B. FedRAMP
C. COBIT
D. ITIL

244. Ilya wants to ensure that systems in his cloud environment are properly patched. Which of the following options will give him the most flexibility and control over patching, including when patches are installed and what patches are installed if his organization has a strong emphasis on using prebuilt tools?
A. Automatically install patches using built-in OS tools.
B. Use a patching script developed by the organization.
C. Set up automatic updates for all applications and the OS.
D. Use the cloud provider’s patching tools and patch baselines.

245. Charleen wants to implement multifactor authentication for her organization. Which of the following MFA options is considered the least secure?
A. Application-based code generation
B. Hardware token–based code generation
C. SMS-based code delivery
D. USB hardware tokens

246. Kirk is adopting a platform as a service tool for his organization. Who is responsible for application and data security in PaaS environments?
A. The customer
B. The provider
C. The regulator
D. Both the customer and provider

247. What term is used to describe a cloud service provider that allows customers to create virtual machines, define their own networking using virtual networks, and use storage and other services to create and manage their own infrastructure?
A. IaaS
B. PaaS
C. SaaS
D. CaaS

248 . When Susan logs into her organization’s service portal, she sees customer data that has names and addresses removed. What data obfuscation technique is her organization using?
A. Randomization
B. Data masking
C. Hashing
D. Anonymization

249. The Cloud Security Alliance notes that specific log types may only be available to cloud service providers when conducting forensic investigations. Which of the following log types will not typically be under service provider control in an IaaS environment?
A. Logs from DNS servers
B. Billing records
C. API logs
D. Web server logs

250 . ITIL v4 defines one primary responsibility for availability. What role is key to availability efforts in ITIL?
A. System architect
B. Availability tester
C. Risk manager
D. Availability manager

251. Wayne's organization employs cloud architects who have broad responsibility for the implementation and oversight of their cloud environment. He wants to provide the architects with appropriate rights in his environment. What should he do to provide them with the proper rights?
A. Use the vendor's best practices definitions for cloud architect rights.
B. Use only built-in roles.
C. Define a custom role.
D. Use multifactor authentication to map roles as needed.

252. Jack is considering a cloud service policy as part of his organization's move to the cloud. Which of the following is not a common principle to follow when building a cloud service policy?
A. Obtain input from all relevant stakeholders.
B. Change organizational culture for the cloud.
C. Follow the chain of command.
D. Meet external requirements.

253. Lucca wants to define technical risks to his cloud environment. Which of the following is not a technical risk for his cloud services?
A. Privacy issues
B. Data breaches
C. System outages
D. Denial-of-service attacks

254. Which of the following is not a typical goal of a privacy impact assessment (PIA)?
A. Identifying the cost of privacy efforts
B. Ensuring that the organization meets legal and policy-based privacy requirements
C. Identifying the risks of privacy breaches
D. Identifying privacy controls

255. After a breach has been discovered, what group is most likely to have a legally required time frame to be notified about the breach?
A. Customers
B. Partners
C. Regulators
D. Law enforcement

256. Michelle wants to store and manage cryptographic keys for her cloud environment. What solution should she require her cloud IaaS provider to have if she is selecting a new provider?
A. TPM
B. Cloud HSM
C. PKI
D. SAS 70

257. What is the most common method for allocation of compute power in cloud IaaS environments?
A. Each customer uses a dedicated CPU per instance.
B. Each customer uses a dedicated core per instance.
C. Computation time is virtualized and allocated based on performance.
D. Computation time is virtualized and allocated based on time.

258. Gurvinder want to ensure that his cloud environment is available and reliable. What type of agreement should he ensure his organization receives from the cloud vendor?
A. QSA
B. NDA
C. MSA
D. SLA

259. Rick wants to ensure that his organization will not be held accountable if something goes wrong that his PaaS provider is responsible for. What should he require in his cloud contract?
A. OLA
B. Service-level management
C. SLA
D. Indemnification

260 . Hillary wants to publish an SSAE-18 SOC report to her website for public use. What type of SOC report should she provide if she wants to provide information about her organization's controls over time?
A. An SOC 1 Type 2
B. An SOC 2 Type 2
C. An SOC 3 Type 2
D. An SOC 4 Type 2

261. Jerome wants to implement DevOps for his organization and is considering how security should be designed in. Which practice is best suited to a DevOps CI/CD environment?
A. Automation of security processes
B. Creation of major releases on a yearly cycle
C. Testing for security in production
D. Static code review

262. Michelle wants to consider the legal risks relevant to her cloud environment. What risk should she highlight if she is concerned about how her organization will handle responses to lawsuits?
A. Cybersecurity risks
B. eDiscovery
C. Data security
D. Copyright infringement

263. Amanda wants to ensure that she can identify systems that performed actions in her cloud environment. What information is most critical to log to ensure she can properly identify ephemeral systems?
A. Their public IP address
B. Their private IP address
C. Tags
D. Usernames

264. Ramon wants to use a cloud identity provider for his organization. Which of the following options is most likely to be supported by cloud identity providers?
A. SAML
B. RDP
C. LDAP
D. FedID

265. Henry wants to reduce the risk of secrets being exposed in the event of a breach. What practice should he adopt to help prevent an attacker with access to application source code or the running application from using the secrets they can recover for future access?
A. Use multifactor authentication.
B. Use dynamic secrets.
C. Use strong passwords.
D. Use certificates and passphrases.

266. Lisa wants to audit actions taken in her cloud environment. Which of the following mechanisms is typically not permitted when dealing with cloud service management backplanes?
A. User access logs
B. Packet capture
C. Specialized cloud service logs
D. Configuration review

267 Emily needs to identify the data elements in an existing customer database that match customers in a newly acquired customer database. What process will Emily need to engage in to accomplish this?
A. Data migration
B. Data mining
C. Data consolidation
D. Data mapping

268. Wayne's organization considers their data to be highly sensitive and wants to ensure that the cloud provider itself cannot access the data while it is stored on the provider's large-scale bulk storage. What type of encryption should he select to accomplish this in a secure manner?
A. AES-256
B. MD5
C. SHA-1
D. CRC

269. The North American Electric Reliability Corporation Critical Infrastructure Protection (NERC/CIP) points to what it calls "mutually managed encryption" as a useful model for cloud environments where the cloud service provider and registered entity (covered by NERC/CIP's requirements) share access and management of encryption keys. What advantage does this type of shared responsibility provide?
A. Flexibility and easier operational support
B. Lowered risk of unauthorized disclosure
C. Simpler control structure
D. Guaranteed confidentiality

270. Jason wants to detect common vulnerabilities during his software development life cycle. What type of assessment is most likely to identify business logic issues?
A. Static code analysis
B. Vulnerability scanning
C. Dynamic testing
D. Software composition analysis

271 . Stacey wants to preserve forensics artifacts from a running instance in her cloud environment. What two key steps should she take to ensure she can perform forensic analysis?
A. Create a snapshot of the running instance and make bit-for- bit copies of any mounted volumes.
B. Shut down the instance and tag it for forensic investigation.
C. Shut down the instance and then create a snapshot for forensic investigation.
D. Use the cloud provider's forensic response team and validate their process.

272. Naomi wants to understand what open source components are part of the containerization tool she is considering adopting. What testing process should she use to understand potential risks of the software based on its components?
A. Interactive application security testing
B. Software composition analysis
C. Manual static testing
D. Automated static testing

273. Selah has deployed open source software in her cloud environment and wants to validate the licensing for the software. What concern is most frequently involved in open source software licensing?
A. The cost of licensing
B. The license type
C. The length of the license period
D. Changes to the license for the deployed software

274. Susan knows that serverless technology provides a number of security benefits for her organization. Which of the following isn't a common benefit of serverless computing?
A. Not needing to handle patching

B. Broad privileges available via IAM
C. Ephemeral infrastructure
D. High levels of instrumentation

275. Katie's organization creates their software in an environment hosted in the Azure cloud. They use a continuous integration/continuous delivery (CI/CD) process that focuses on automated testing and deployment. What risk is most likely to make it through an automated security testing process?
A. Business logic risk
B. SQL injection flaws
C. Cross-site scripting flaws
D. Vulnerable components

276. What ports and protocol does DHCP operate on?
A. UDP ports 21 and 22
B. TCP ports 80 and 443
C. TCP ports 3389 and 4780
D. UDP ports 67 and 68

277. Sara wants to operate some of her infrastructure in a datacenter that she controls and some in third-party cloud-hosted environments. What type of cloud deployment model best describes this?
A. Private cloud
B. Hybrid cloud
C. Multicloud
D. Community cloud

278. Isabelle wants to retrieve forensic data from her cloud provider's native logging facility. What technique is most likely to be supported for this type of data access?
A. Transfer to removable media
B. Manual copying
C. API-based
D. Printed copies

279. Ashley's testing process involves approaching software testing like an attacker would. She will attempt to compromise or misuse the software, and report on its responses and any issues she identifies. What type of testing is Ashely conducting?
A. Abuse case testing
B. Interactive application security testing
C. User acceptance testing
D. Static testing

280. Freya wants to revoke a certificate used by her organization. What will happen when she revokes the certificate via her certificate authority?
A. The certificate will no longer work to encrypt data.
B. The certificate will be placed on a certificate revocation list.
C. A message about the revocation will be sent to all users of the certificate.
D. The CA will set the certificate's expiration date to the revocation date.

281. Kathleen is concerned about country-specific privacy regulations because her organization is opening a location in a new country. What should she advise her organization's leadership to do?
A. Follow OWASP-defined best practices.
B. Engage external counsel with appropriate expertise.
C. Identify an appropriate NIST standard to follow.
D. Carefully review the laws and design the new policy based on them.

282. Which of the following is not a typical driver for data retention policies?
A. Business requirements
B. Legal requirements
C. Regulatory requirements
D. Data integrity requirements

283. Megan is accountable for the financial data in her organization, and she delegates responsibility for data-related
actions to others in her organization. What role does she play?
A. Data owner
B. Data custodian
C. Data processor
D. Data steward

284. What makes vendor risk assessment difficult for open source software?
A. There is no vendor for many open source packages.
B. Open source software cannot undergo static code review.
C. Open source software vendors do not offer software support contracts.
D. Risk information about historical issues is not available.

285. ITIL v4 identifies four information management subprocesses related to information security management. What ITIL v4 subprocess includes audits?
A. Design of security controls
B. Security testing
C. Management of security incidents
D. Security review

286. Diana wants to increase the bandwidth available to her cloud infrastructure as a service-hosted system. What would she need to do to increase the speed at which her instance is connecting to the provider's network?
A. Replace the network interface card.
B. Request that the cloud provider upgrade the network card.
C. Increase the instance's network bandwidth.
D. Change the network interface speed setting inside the instance's operating system.

287. What requirement for data breach reporting does the Sarbanes–Oxley Act place on organizations that must comply with it?
A. All impacted customers must be notified.
B. Data breaches must be reported in annual and quarterly reports.
C. Law enforcement must be informed as soon as the breach is discovered.
D. Breach disclosure is required in local news media.

288. Mike wants to use a standards-based rating system to identify, define, and catalog vulnerabilities. Which of the following options should he choose?
A. CVE
B. VulnRank
C. CPE
D. MITRE

289. Olivia's industry requires yearly audits of their business, and she knows that she needs to provide audit artifacts to the auditors about her cloud-hosted services. What should Olivia do to meet her audit requirements?
A. Engage external auditors to audit the cloud provider.
B. Contact the cloud service provider to obtain the required audit artifacts.
C. Engage internal auditors to audit the cloud provider.
D. Contact the cloud service provider and provide the required audit artifacts to them.

290. Sean's company has grown its IT infrastructure and no longer considers the converted closet that its servers have been hosted in sufficient to the organization's needs. If Sean wants to meet an Uptime Institute Level 3 rating, what option will most efficiently and effectively meet his needs?

A. Buy a datacenter.
B. Build a datacenter.
C. Rent space in a datacenter facility.
D. Build a datacenter in an existing building.

291. Cloud customers benefit from standalone hosts and clustered hosts in different ways. What are clustered hosts known to provide?

A. All Options are correct
B. Confidentiality
C. Availability
D. Integrity

292. Which management process is concerned with the management of all changes to configuration items, including the addition of any new devices?

A. Continuity Management
B. Incident Management
C. Deployment Management
D. Change Management

293. TLS is a critical technology for encrypting data while it is in transit. TLS is composed of two protocol layers. What are they?

A. Transport protocol and Record protocol
B. Data Protocol and handshake protocol
C. Record protocol and Data protocol
D. Handshake Protocol and Record Protocol

294. What adds to security and reduces susceptibility to spoofing by providing origin authority, data integrity, and authenticated denial of service?

A. DNSSEC
B. PKI
C. SDP
D. FQDN

295. In log management, what defines which categories of events are and are NOT written into logs?

A. Transparency Level
B. Clipping Level
C. Quality Level
D. Retention Level

296. During which phase of the TLS process is the connection between the two parties negotiated and established?

A. TLS Negotiation Protocol
B. TLS Functional Protocol
C. TLS Record Protocol
D. TLS Handshake Protocol

297. The decisions regarding where traffic is filtered or sent to and the actual forwarding of traffic are separate from each other when which of the following technologies is being used?

A. VLAN
B. SAN
C. SDN
D. VPN

298. What is a KVM used for?

A. To connect Keyboard, mouse, and monitor to a physical server
B. As a method of backing up data within a cloud environment
C. To prevent attacks from gaining unauthorized access to physical servers
D. As a storage method for cloud hosted servers

299. Which of the following is TRUE regarding virtualization?

A. Virtual images are susceptible to attacks whether they are running or not
B. It's important to secure the virtual images than the management plane is a virtualized environment
C. The most important component to secure in a virtualized environment is the hypervisor
D. Virtual images are susceptible to attacks whether they are online and running

300. What type of technology uses iSCSI, Fibre Channel, and Fiber channel over Ethernet (FCoE) to create dedicated networks for data storage and retrieval?

A. SDS
B. SDN
C. SAN
D. CDN

301. What is a grouping of resources with a coordinating software agent that facilitates communication, resource sharing, and routing of tasks?

A. VLAN
B. Storage Controllers
C. Clusters
D. Tenant

302. Which of the following is NOT an accurate statement about Remote Desktop Protocol (RDP)?

A. Client-server Operation
B. GUI access to interact with a remote computer
C. Available to most operating systems
D. Secure means of remotely accessing the machines

303. As cloud service customers, the majority of businesses will get communications from their cloud service providers. What are the primary responsibilities of cloud service customers?

A. Provide IT services
B. Creating support tickets
C. Defining SLA terms
D. Active participating in the shared responsibility model

304. Within LDAP, which of the following acts as the primary key for an object?

A. CN
B. AN
C. HN
D. DN

305. Which of the following areas is always entirely the CSP's responsibility, regardless of the cloud service model used?

A. Virtualization
B. Networking
C. Database
D. Storage

306. An organization has spent quite a significant amount of their budget on vendor-specific investments and now the cost for them to move to a new cloud provider would be far too high to be feasible. What is the term used to describe this type of scenario?

A. Provider Exit
B. Data Sanitation
C. Customer Lock-in
D. Vendor Lock-in

307. A cloud administrator would like to reduce the risk of vendor lock-in. What cloud shared consideration should the administrator be looking for?

A. Interoperability
B. Versioning
C. Availability
D. Reversibility

308. In a SaaS environment, if either SQL injection or cross-site scripting vulnerabilities exist within any SaaS implementation, every customer's data becomes at risk. Of the following, what is the BEST method for preventing this type of security risk?

A. The provider should sign a contract stating that they are liable for a data breach
B. The provider should install upto date anti-virus
C. The provider should have different data stores and try to keep the data isolated as much as possible
D. The provider should ensure that the patches are scheduled in place and adhere to it

309. Of the following, which feature of cloud computing allows data to move between multiple cloud providers seamlessly?

A. Interoperability
B. Reversibility
C. Portability
D. Auditability

310. In the cloud, what are the major cloud performance concerns?

A. Virtualization
B. Security and Encryption
C. Availability and Bandwidth
D. Identity and access

311. Which cloud storage type operates as a web service call or as an API?

A. Volume
B. Object
C. Structured
D. Un-structured

312. There are two main types of storage in SaaS environments. Which SaaS storage type is the classic form of storing data within databases that the application uses and maintains?

A. Content Files and storage
B. Object Storage
C. Information Storage and management
D. Volume storage

313. What is a cloud storage architecture that organizes data into fields based on the properties of individual data elements?

A. File-Based
B. Object-based
C. Database
D. Raw-data

314. The most common and well understood threat to storage is:

A. Unauthorized access to data
B. Accidental deletion of data
C. Improper credentials management
D. Malware that modifies data

315. The process of removing all identifiable characteristics from data is known as:

A. Anonymization
B. Obfuscation
C. Hashing
D. Masking

316. IRM can be used as a means for:

A. Data Classification and deletion
B. Data Control and modification
C. Data Modification and deletion
D. Data Classification and control

317. Data dispersal in cloud settings can have a mixed effect on an organization's security. What are the disadvantages of data dispersion?

A. Availability of data
B. Reconstruction of data
C. Erasure Coding
D. Relocation of data

318. An engineer is working with data that is in the store phase of the cloud data lifecycle. Now that the data is in the store phase, what must the engineer immediately employ on top of security controls?

A. Data Classification
B. Backup methods
C. Sharing permissions
D. Data Destruction Methods

319. Jada is currently vetting the tokenization process of her organization's cloud provider. What is one risk that Jada should ensure is limited during the tokenization process?

A. SLA Modification
B. File Type changes
C. Price changes
D. Vendor Lock-in

320. An engineer has implemented data loss prevention solutions that are installed on each of the systems which house and store data. This includes any servers, workstations, and mobile devices which hold data. These DLP solutions are used to protect data in which state?

A. Data in motion
B. Data in use
C. Data in transit
D. Data in Rest

321. Which of the following can data masking NOT be used for?

A. Remote Access
B. Least Privileges
C. Authentication
D. Sandbox environment

322. As you are drafting your organization's cloud data destruction policy, which of the following is NOT a consideration that may affect the policy?

A. Retention requirements
B. Compliance and governance
C. Data Discovery
D. Business Processes

323. Which one of the following is associated heavily with vendor lock-in?

A. DaaS
B. SaaS
C. IaaS
D. PaaS

324. What has been the key concern for data archiving over time?

A. Recoverability
B. Size of Archive
C. Format of Archives
D. Regulatory Changes

325. Tina would like to use a technology that will allow her to bundle up workloads and easily move them between different operating systems. What technology would best meet this need?

A. Virtual machines
B. Serverless computing
C. Hypervisors
D. Containers

326. Sherry is deploying a zero-trust network architecture for her organization. In this approach, which one of the following characteristics would be least important in validating a login attempt?

A. User identity
B. IP address
C. Geolocation
D. Nature of requested access

327. Which one of the following cybersecurity threats is least likely to directly affect an object storage service?

A. Disk failure
B. User error
C. Ransomware
D. Virus

328. Which one of the following characteristics is not a component of the standard definition of cloud computing?

A. Broad network access
B. Rapid provisioning
C. Multitenancy
D. On-demand self service

329. Which one of the following cryptographic goals protects against the risks posed when a device is lost or stolen?

A. Nonrepudiation
B. Authentication
C. Integrity
D. Confidentiality

330. What activity are cloud providers able to engage in because not all users will access the full capacity of their service offering simultaneously?

A. Oversubscription
B. Overprovisioning
C. Under provisioning
D. Undersubscription

331. Which one of the following would be considered an example of infrastructure as a service cloud computing?

A. Payroll system managed by a vendor and delivered over the web
B. Application platform managed by a vendor that runs customer code

C. Servers provisioned by customers on a vendor-managed virtualization platform
D. Web-based email service provided by a vendor

332. Bianca is preparing for her organization's move to a cloud computing environment. She is concerned that issues may arise during the change and would like to ensure that they can revert back to their on-premises environment in the case of a problem. What consideration is Bianca concerned about?
A. Reversibility
B. Portability
C. Regulatory
D. Resiliency

333. Ben has been tasked with identifying security controls for systems covered by his organization's information classification system. Why might Ben choose to use a security baseline?
A. They apply in all circumstances, allowing consistent security controls.
B. They are approved by industry standards bodies, preventing liability.
C. They provide a good starting point that can be tailored to organizational needs.
D. They ensure that systems are always in a secure state

334. Lisa wants to integrate with a cloud identity provider that uses OAuth 2.0, and she wants to select an appropriate authentication framework. Which of the following best suits her needs?
A. OpenID Connect
B. SAML
C. RADIUS
D. Kerberos

335. Nuno's company is outsourcing its email system to a cloud service provider who will provide web-based email access to employees of Nuno's company. What cloud service category is being used?
A. PaaS
B. IaaS
C. SaaS
D. FaaS

336. Kristen wants to use multiple processing sites for her data, but does not want to pay for a full datacenter. Which of the following options would you recommend as her best option if she wants to be able to quickly migrate portions of her custom application environment to the facilities in multiple countries without having to wait to ship or acquire hardware?
A. A cloud PaaS vendor
B. A hosted datacenter provider
C. A cloud IaaS vendor
D. A datacenter vendor that provides rack, power, and remote hands services

337. You are the security subject matter expert (SME) for an organization considering a transition from a traditional IT enterprise environment into a hosted cloud provider's datacenter. One of the challenges you're facing is whether your current applications in the on-premises environment will function properly with the provider's hosted systems and tools. This is a(n)
_________________ issue.
A. Interoperability
B. Portability
C. Stability
D. Security

338. Which one of the following statements is correct?
A. Services that are scalable are also elastic.
B. There is no relationship between elasticity and scalability.
C. Services that are elastic are also scalable.
D. Services that are either elastic or scalable are both elastic and scalable.

339. __________ is an example of due care, and ___________ is an example of due diligence.
A. Privacy data security policy; auditing the controls dictated by the privacy data security policy

B. The European Union General Data Protection Regulation (GDPR); the Gramm–
Leach–Bliley Act (GLBA)
C. Locks on doors; turnstiles
D. Perimeter defenses; internal defenses

340. You are concerned about protecting sensitive data while it is stored in memory on a server. What emerging technology is designed to assist with this work?
A. Quantum computing
B. Confidential computing
C. Edge computing
D. Fog computing

341. Henry's company has deployed an extensive IoT infrastructure for building monitoring that includes environmental controls, occupancy sensors, and a variety of other sensors and controllers that help manage the building. Which of the following security concerns should Henry report as the most critical in his analysis of the IoT deployment?
A. There is a lack of local storage space for security logs, which is common to IoT devices.
B. The IoT devices may not have a separate administrative interface, allowing anybody on the same network to attempt to log in to them and making brute-force attacks possible.
C. The IoT devices may not support strong encryption for communications, exposing the log and sensor data to interception on the network.
D. The long-term support and patching model for the IoT devices may create security and operational risk for the organization

342. Which one of the following disaster recovery approaches is generally the most cost-effective for an organization?
A. Hot site
B. Cloud site
C. Cold site
D. Warm site

343. Mike and Renee would like to use an asymmetric cryptosystem to communicate with each other. They are located in different parts of the country but have exchanged encryption keys by using digital certificates signed by a mutually trusted certificate authority.
When Mike receives Renee's digital certificate, what key does he use to verify the authenticity of the certificate?
A. Renee's public key
B. Renee's private key
C. CA's public key
D. CA's private key

344. Which one of the following statements is correct?
A. Services that are scalable are also elastic.
B. There is no relationship between elasticity and scalability.
C. Services that are elastic are also scalable.
D. Services that are either elastic or scalable are both elastic and scalable

345. Which of the following threat types involves an application that does not validate authorization for portions of itself once the user accesses it for the first time?
A. Missing Function-level access
B. Cross-Site Request forgery
C. Injection
D. Cross-Site Scripting

346. SOAP must rely on ____________ for security.

A. TLS
B. SSL
C. Tokenization
D. Encryption

347. What is the most serious issue with hosting a key management system outside of the cloud?

A. Availability
B. Confidentiality
C. Integrity
D. Portability

348. Three basic concepts characterize the types of data and information for which an organization is responsible in the context of eDiscovery. Which of the following are the three components of disclosure requirements?

A. Possession, Ownership, Control
B. Possession, Custody, Control
C. Ownership, Use, Creation
D. Control, Custody, Use

349. What is the primary reason that makes resolving jurisdictional conflicts complicated?
A. Different technology standards
B. Costs
C. Language barriers
D. Lack of international authority

350. GAAPs are created and maintained by which organization?
A. ISO/IEC
B. AICPA
C. PCI Council
D. ISO

351. Which of the following threat types can occur when encryption is not properly applied or insecure transport mechanisms are used?
A. Security misconfiguration
B. Insecure direct object references
C. Sensitive data exposure
D. Unvalidated redirects and forwards

352. What is the best approach for dealing with services or utilities that are installed on a system but not needed to perform their desired function?
A. Remove
B. Monitor
C. Disable
D. Stop

353. What type of PII is regulated based on the type of application or per the conditions of the specific hosting agreement?
A. Specific
B. Contractual
C. regulated
D. Jurisdictional

354. If you're using iSCSI in a cloud environment, what must come from an external protocol or application?
A. Kerberos support
B. CHAP support
C. Authentication
D. Encryption

355. Which of the following pertains to a macro level approach to data center design rather than the traditional tiered approach to data centers?
A. IDCA
B. NFPA
C. BICSI
D. Uptime Institute

356.Which technology is NOT commonly used for security with data in transit?
A. DNSSEC
B. IPsec
C. VPN
D. HTTPS

357. What controls the formatting and security settings of a volume storage system within a cloud environment?
A. Management plane
B. SAN host controller

C. Hypervisor
D. Operating system of the host

358. You are the security manager for a small retail business involved mainly in direct e-commerce transactions with individual customers (members of the public). The bulk of your market is in Asia, but you do fulfill orders globally. Your company has its own datacenter located within its headquarters building in Hong Kong, but it also uses a public cloud environment for contingency backup and archiving purposes. Your cloud provider is changing its business model at the end of your contract term, and you have to find a new provider. In choosing providers, which tier of the Uptime Institute rating system should you be looking for, if minimizing cost is your ultimate goal?
A. 1
B. 3
C. 4
D. 8

359. Which of the following is not commonly measured as part of a disk's hardware monitoring?
A. Powered-on time
B. Drive temperature
C. Drive health
D. Used capacity

360. ITIL v4 defines four subprocesses for service-level management. Which of the following is not one of the four subprocesses?
A. Maintenance of the service-level management framework
B. Identification of service requirements
C. Pricing structures and penalties
D. Service-level monitoring and reporting

361. Michelle wants to run an application from low-trust devices. What type of cloud-based solution could help her run the application in a secure way?
A. Use a local virtual machine.
B. Use a bastion host.
C. Use a jumpbox.
D. Use a virtual client

362. Which of the following has the highest impact in determining whether the business continuity and disaster recovery (BC/DR) effort has a chance of being successful?
A. Perform an integrity check on archived data to ensure that the backup process is not corrupting the data.
B. Encrypt all archived data to ensure that it can't be exposed while at rest in the long term.
C. Periodically restores from backups.
D. Train all personnel on BC/DR actions they should take to preserve health and human safety

363. Selah wants to conduct a vulnerability scan of her SaaS provider's service as part of her ongoing security operations responsibility. What should she do?
A. Contact the provider and ask about appropriate scan windows.
B. Request vulnerability scan data from the vendor.
C. Scan the provider on a regular basis whenever she wants to.
D. Consider asking the SaaS provider about their own patching and scanning practices

364. Mike's organization is considering adopting an infrastructure as code (IaC) strategy. What should Mike identify as a potential risk in an IaC environment?
A. IaC decreases consistency.
B. IaC is not easily updated.
C. IaC decreases speed.
D. IaC can cause errors to spread quickly.

365. Jim has deployed a system that appears to be a vulnerable host on a network. The system is instrumented to capture attacker commands and tools. What type of network security control has Jim deployed?
A. A honeypot
B. A darknet
C. A honeynet
D. A bastion host

366. Li’s organization uses a software as a service tool for their productivity work. After a recent compromise of user credentials, Li wants to perform digital forensics. What types of information can Li obtain for forensic analysis in an SaaS environment?
A. Logs
B. Disk images
C. VM snapshots
D. Network packet capture data

367. Chelsea wants to prevent network-based attacks against her cloud-hosted system. Which of the following is not an appropriate solution to stop attacks?
A. Honeypots
B. Firewalls
C. Security groups
D. Intrusion prevention systems

368. Methods for achieving high-availability cloud environments include all of the followling except
A. Using instances running on alternate CPU architectures
B. Multiple system vendors for the same services
C. Explicitly documented business continuity and disaster recovery (BC/DR) functions in the service-level agreement (SLA) or contract
D. Failover capability back to the customer’s on-premises environment

369. Susan’s website is unable to be loaded by her customers due to a system outage. What ITIL practice should Susan invest in to ensure that this does not happen again?
A. Availability management
B. Deployment management
C. Change management
D. Capacity management

370.Kathleen knows that her cloud provider makes a DHCP service available to systems in their IaaS environment. What does she know that her systems will receive from the DHCP server?
A. A default gateway, subnet mask, DNS server, and IP address
B. A default route, a subnet mask, an IP address, and a MAC address
C. An IP address and a MAC address
D. An IP address, a subnet mask, a DNS server, and firewall rule definitions for the local network

371. Ben wants to secure his virtualization environment. Which of the following is not a common security practice used to help protect virtualization infrastructure and systems?
A. Enable secure boot
B. Disable cut and paste between the VM and console.
C. Remove unnecessary hardware.
D. Use the virtual machine console whenever possible

372. Amanda wants to use logging from her IaaS cloud environment to determine if an external user is accessing one of her servers. What type of logging should she enable in her cloud provider’s environment to do so?
A. System logging
B. Performance logging
C. Flow logging
D. Storage bucket logging

373. Which of the following roles is responsible for creating cloud components and the testing and validation of services?
A. Cloud auditor
B. Inter-cloud provider
C. Cloud service broker
D. Cloud service developer

374. What is the best approach for dealing with services or utilities that are installed on a system but not needed to perform their desired function?
A. Remove
B. Monitor
C. Disable
D. Stop

375. Which of the following actions will NOT make data part of the "create" phase of the cloud data lifecycle?
A. Modifying metadata

B. Importing data
C. Modifying data
D. Constructing new data

376. If you're using iSCSI in a cloud environment, what must come from an external protocol or application?
A. Kerberos support
B. CHAP support
C. Authentication
D. Encryption

377. Which technology is NOT commonly used for security with data in transit?
A. DNSSEC
B. IPsec
C. VPN
D. HTTPS

378. What controls the formatting and security settings of a volume storage system within a cloud environment?
A. Management plane
B. SAN host controller
C. Hypervisor
D. Operating system of the host

379. Which entity requires all collection and storing of data on their citizens to be done on hardware that resides within their borders?
A. Russia
B. France
C. Germany
D. United States

380. What type of data does data rights management (DRM) protect?
A. Consumer
B. PII
C. Financial
D. Healthcare

381. What changes are necessary to application code in order to implement DNSSEC?
A. Adding encryption modules
B. Implementing certificate validations
C. Additional DNS lookups
D. No changes are needed.

382. What is the biggest challenge to data discovery in a cloud environment?
A. Format
B. Ownership
C. Location
D. Multitenancy

383.Which aspect of cloud computing makes it very difficult to perform repeat audits over time to track changes and compliance?
A. Virtualization
B. Multitenancy
C. Resource pooling
D. Dynamic optimization

384. Which of the following is NOT an application or utility to apply and enforce baselines on a system?
A. Chef
B. GitHub
C. Puppet
D. Active Directory

385. Which of the following is NOT a function performed by the record protocol of TLS?
A. Encryption
B. Acceleration
C. Authentication
D. Compression

386. The SOC Type 2 reports are divided into five principles. Which of the five principles must also be included when auditing any of the other four principles?
A. Confidentiality
B. Privacy
C. Security
D. Availability

387. How many additional DNS queries are needed when DNSSEC integrity checks are added?
A. Three
B. Zero

C. One
D. Two

388.What strategy involves hiding data in a data set to prevent someone from identifying specific individuals based on other data fields present?
A. Anonymization
B. Tokenization
C. Masking
D. Obfuscation

389. Which data point that auditor always desire is very difficult to provide within a cloud environment?
A. Access policy
B. Systems architecture
C. Baselines
D. Privacy statement

390. What type of host is exposed to the public Internet for a specific reason and hardened to perform only that function for authorized users?
A. Proxy
B. Bastion
C. Honeypot
D. WAF

391. With software-defined networking, what aspect of networking is abstracted from the forwarding of traffic?
A. Routing
B. Session
C. Filtering
D. Firewalling

392. Who would be responsible for implementing IPsec to secure communications for an application?
A. Developers
B. Systems staff
C. Auditors
D. Cloud customer

393.Other than cost savings realized due to measured service, what is another facet of cloud computing that will typically save substantial costs in time and money for an organization in the event of a disaster?
A. Broad network access
B. Interoperability
C. Resource pooling
D. Portability

394. Which of the following is NOT something that an HIDS will monitor?
A. Configurations
B. User logins
C. Critical system files
D. Network traffic

395. Which attribute of data poses the biggest challenge for data discovery?
A. Labels
B. Quality
C. Volume
D. Format

396. Where is a DLP solution generally installed when utilized for monitoring data at rest?
A. Network firewall
B. Host system
C. Application server
D. Database server

397.Within a SaaS environment, what is the responsibility on the part of the cloud customer in regard to procuring the software used?
A. Maintenance
B. Licensing
C. Development
D. Purchasing

398. Different certifications and standards take different approaches to data center design and operations. Although many traditional approaches use a tiered methodology, which of the following utilizes a macro-level approach to data center design?

A. IDCA
B. BICSI
C. Uptime Institute
D. NFPA

399. The European Union is often considered the world leader in regard to the privacy of personal data and has declared privacy to be a "human right."In what year did the EU first assert this principle?

A. 1995
B. 2000
C. 2010
D. 1999

400. What type of storage structure does object storage employ to maintain files?

A. Directory
B. Hierarchical
C. tree
D. Flat

401. If a cloud computing customer wishes to guarantee that a minimum level of resources will always be available, which of the following set of services would compromise the reservation?

A. Memory and networking
B. CPU and software
C. CPU and storage
D. CPU and memory