# CCSP Exam Prep Questions

1. Which of the following is NOT a domain of the Cloud Controls Matrix (CCM)?
   1. Data center security
   2. Budgetary and cost controls
   3. Mobile Security
   4. Human Resources
      1. B
2. What type of data does data rights management (DRM) protect?
   1. PII
   2. Healthcare
   3. Consumer media
   4. Financial
      1. C
3. Which storage type of PaaS would be used for website files or multimedia objects?
   1. Unstructured
   2. Volume
   3. Structured
   4. Object
      1. A
4. What is the official term for the process of determining audit results that deviate from intended configurations and policies?
   1. Findings
   2. Gap analysis
   3. Audit deficiency
   4. Non-compliance
      1. B
5. Which of the following threat types involves an application that does not validate authorization for portions of itself after the initial checks?
   1. Missing function-level access control
   2. Cross-site request forgery
   3. Cross-site scripting
   4. Injection
      1. A
6. Which type of cloud model typically presents the most challenges to a cloud customer during the "destroy" phase of the cloud data lifecycle?
   1. IaaS
   2. DaaS
   3. PaaS
   4. SaaS
      1. D
7. Which ITIL component is focused on proactively putting processes in place to prevent disruptions from ever happening?
   1. Incident management
   2. Problem management
   3. Information security management
   4. Availability management
      1. B
8. What is the biggest benefit to leasing space in a data center versus building or maintain your own?
   1. Control
   2. Costs
   3. Certification
   4. Regulation
      1. B
9. Which of the following is a widely used tool for code development, branching, and collaboration?
   1. Orchestrator
   2. Maestro
   3. GitHub
   4. Conductor
      1. C
10. What is the biggest negative to leasing space in a data center versus building or maintain your own?
    1. Control
    2. Costs
    3. Certification
    4. Regulation
       1. A
11. 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?
    1. Confidentiality
    2. Privacy
    3. Availability
    4. Security
       1. D
12. Which of the following is NOT a criterion for data within the scope of eDiscovery?
    1. Possession
    2. Custody
    3. Control
    4. Archive
       1. D
13. Which of the following service capabilities gives the cloud customer the most control over resources and configurations?
    1. Platform
    2. Desktop
    3. Infrastructure
    4. Software
       1. C
14. What is a potential problem with using object storage versus volume IaaS in regard to availability?
    1. Object storage is its own system, and data consistence depends on replication.
    2. Object storage may have availability issues.
    3. Object storage is dependent on access control from the host server.
    4. Object storage is only optimized for small files.
       1. A
15. Which of the following types of applications are likely to work with application virtualization?
    1. Applications that require shared memory
    2. Applications that require access to system drivers
    3. 32-bit applications
    4. Antivirus software
       1. C
16. Which of the following would NOT be an appropriated limitation to be included as an audit restriction?
    1. Names of auditors
    2. Devices of auditors
    3. Types of invasive testing
    4. Length of audit report
       1. D
17. What is the minimum regularity for testing a BCDR plan to meet best practices?
    1. Once a month
    2. Every six months
    3. Once a year
    4. When the budget allows it
       1. C
18. Which of the following technologies is used to monitor network traffic and notify if any potential threats or attacks are noticed?
    1. IDS
    2. IPS
    3. Firewall
    4. WAF
       1. A
19. Which type of audit report is considered a "restricted use" report for its intended audience?
    1. SOC Type 1
    2. SAS-70
    3. SOC Type 2
    4. SSAE-16
       1. A
20. Which OSI layer does IPsec operate at?
    1. Network
    2. Transport
    3. Presentation
    4. Application
       1. A
21. OpenID is an authentication protocol based on which specifications?
    1. Oauth
    2. XML
    3. SAML
    4. WS-Federation
       1. A
22. Which of the following may unilaterally deem a cloud hosting model inappropriate for a system or application?
    1. Certification
    2. Regulation
    3. Multitenancy
    4. Virtualization
       1. B
23. Which ITIL component is focused on ensuring that services are properly provisioned and secured to meet requirements?
    1. Incident management
    2. Problem management
    3. Information security management
    4. Availability management
       1. D
24. Why does Type 2 hypervisor typically offer less security control than a Type 1 hypervisor?
    1. A Type 2 hypervisor is always exposed to the public Internet for federated identity access.
    2. A Type 2 hypervisor allows users to directly perform some functions with their own access.
    3. A Type 2 hypervisor runs on top of another operations system and is dependent on the security of the OS for its own security.
    4. A Type 2 hypervisor is open source, so attackers can more easily find exploitable vulnerabilities with that access.
       1. C
25. Which of the following is a challenge that is most often overlooked when formulating a BCDR plan?
    1. Availability of staff
    2. Capacity at BCDR site
    3. Change management processes
    4. Restoration of services
       1. D
26. Which type of hypervisor runs directly on the underlying hardware and is coupled tightly with it?
    1. Type 2 hypervisor
    2. Bare-metal hypervisor
    3. Hardware hypervisor
    4. Type 1 hypervisor
       1. D
27. Which if the following is NOT one of the three components of a federated system transaction?
    1. Proxy relay
    2. User
    3. Relying party
    4. Identity provider
       1. A
28. Which of the following would NOT be a reason to activate a BCDR strategy?
    1. Staffing loss
    2. Natural disaster
    3. Terrorism attack
    4. Utility disruptions
       1. A
29. Which term relates to the application of scientific methods and practices to evidence?
    1. Forensics
    2. Theoretical
    3. Measured
    4. Methodical
       1. A
30. Which of the following represents a control on the maximum amount of resources that a single customer, virtual machine, or application can consume within a cloud environment?
    1. Reservation
    2. Limit
    3. Share
    4. Provision
       1. B
31. Which of the following is considered an internal redundancy for a data center?
    1. Generators
    2. Power distribution units
    3. Network circuits
    4. Power substations
       1. B
32. Which of the following is NOT a function performed by the handshake protocol of TLS?
    1. Negotiation of connection
    2. Encryption
    3. Key exchange
    4. Establish session ID
       1. B
33. From the perspective of compliance, what is the most important consideration when it comes to data center location?
    1. Natural disasters
    2. Personnel access
    3. Jurisdiction
    4. Utility access
       1. C
34. Which of the following roles is responsible for peering with other cloud services and providers?
    1. Cloud service developer
    2. Inter-cloud provider
    3. Cloud auditor
    4. Cloud service broker
       1. B
35. What does the management plane typically utilize to perform administrative functions on the hypervisors that has access to?
    1. APIs
    2. Scripts
    3. XML
    4. RDP
       1. A
36. Which protocol allows a system to use block-level storage as if it was a SAN, but over TCP network traffic instead?
    1. TLS
    2. iSCSI
    3. SCSI
    4. SATA
       1. B
37. When is virtual machine susceptible to attacks while a physical server in the same state would not be?
    1. When it is powered off
    2. When it is not patched
    3. When it is behind an IPS
    4. When it is behind a WAF
       1. A
38. What are the four approaches to responding to risk?
    1. Accept, avoid, transfer, mitigate
    2. Accept, dismiss, transfer, mitigate
    3. Accept, deny, mitigate, revise
    4. Accept, deny, transfer, mitigate
       1. A
39. Which of the following would make it more likely that a cloud provider would be unwilling to satisfy specific certification requirements?
    1. Resource pooling
    2. Regulation
    3. Multitenancy
    4. Virtualization
       1. C
40. What is used for local, physical access to hardware within a data center?
    1. VPN
    2. RDP
    3. KVM
    4. SSH
       1. C
41. Which type of masking is implemented between the application and data layers?
    1. Dynamic
    2. Transactional
    3. Static
    4. Transitional
       1. A
42. When limits are allowed to change based on current conditions within the cloud environment, they do not actually change but just temporarily adapt. What is this process called?
    1. Loaning
    2. Borrowing
    3. Adapting
    4. Flexing
       1. B
43. What does GAPP stand for?
    1. Generally Accepted Privacy Principles
    2. Generally Accepted Personal Privacy
    3. General Activities for Personal Privacy
    4. Generally Accepted Privacy Policies
       1. A
44. Which of the following is the biggest concern or challenge with using encryption?
    1. Efficiency
    2. Dependence on keys
    3. Cipher strength
    4. Protocol standards
       1. B
45. Which format is the most commonly used standard for exchanging information within a federated identity system?
    1. SAML
    2. XML
    3. JSON
    4. HTML
       1. A
46. Which technology is NOT commonly used for security with data in transit?
    1. Ipsec
    2. HTTPS
    3. VPN
    4. DNSSEC
       1. D
47. Which of the cloud deployment models involves spanning multiple cloud environments or a mix of cloud hosting models?
    1. Private
    2. Public
    3. Hybrid
    4. Community
       1. C
48. Which of the following publishes the most commonly used standard for data center design in regard to tiers and topologies?
    1. IDCA
    2. BICSI
    3. NFPA
    4. Uptime Institute
       1. D
49. Which of the following is NOT one of the five key principles of the ISO/IEC 27018 standards on privacy with cloud computing?
    1. Consent
    2. Internal audit
    3. Control
    4. Transparency
       1. B
50. Which of the following is considered an external redundancy for a data center?
    1. Power distribution
    2. Generators
    3. Storage systems
    4. Power feeds to racks
       1. B
51. Which aspect of access control involves ensuring users are assigned to the correct roles and levels of access within a system, once they have successfully proven their identity to the system?
    1. Authorization
    2. Authentication
    3. Account provisioning
    4. Privileged access
       1. A
52. Which aspect of cloud computing would make the use of a cloud the most attractive as a BCDR solution?
    1. Portability
    2. Interoperability
    3. Resource pooling
    4. Measured service
       1. D
53. Which of the following is an open source federated identity system that is commonly used in academic institutions?
    1. Shibboleth
    2. OpenID
    3. Puppet
    4. Chef
       1. A
54. Which aspect of cloud computing makes it very difficult to perform repeat audits over time to track changes and compliance?
    1. Resources pooling
    2. Virtualization
    3. Multitenancy
    4. Dynamic optimization
       1. B
55. How many additional DNS queries are needed when DNSSEC integrity checks are added?
    1. One
    2. Zero
    3. Two
    4. Three
       1. B
56. If you're using iSCSI in a cloud environment, what must come from an external protocol or application?
    1. Authentication
    2. Kerberos support
    3. CHAP support
    4. Encryption
       1. D
57. Which of the following storage types is most closely associated with a database-type storage implementation?
    1. Structured
    2. Unstructured
    3. Object
    4. Volume
       1. A
58. Which of the following would NOT be covered by a reservation in a cloud environment?
    1. Starting virtual machines
    2. Auto-scaling
    3. Operating applications
    4. Performing normal business operations
       1. B
59. Which regulatory system pertains to the protection of healthcare data?
    1. HIPAA
    2. HFCA
    3. HAS
    4. HITECH
       1. A
60. As applications mature and new features are added, which concept refers to the process of ensuring new event types are discovered and collected, based on the changes in the application?
    1. Augmentation
    2. Continuous review
    3. Continuous optimization
    4. Continuous compliance
       1. C
61. Which of the following is NOT one of the specialized compliance requirements for highly regulated industries?
    1. HIPPAA
    2. FedRAMP
    3. PCIDSS
    4. GAPP
       1. D
62. Which of the following is NOT one of the official rating categories?
    1. Low
    2. Minimal
    3. Critical
    4. Catastrophic
       1. D
63. What type of host is exposed to the public Internet for a specific reason and hardened to perform only that function for authorized users?
    1. Honeypot
    2. WAF
    3. Proxy
    4. Bastion
       1. D
64. Which of the following would be a reason to undertake a BCDR test?
    1. Change in regulations
    2. Change in staff
    3. Functional change of the application
    4. User interface overhaul of the application
       1. C
65. Which of the following is NOT a factor that is part of a firewall configuration?
    1. Protocol
    2. Source IP
    3. Port
    4. Encryption
       1. D
66. What does dynamic application security testing (DAST) NOT entail?
    1. Probing
    2. Scanning
    3. Discovery
    4. Knowledge of the system
       1. D
67. Which of the following is NOT one of the domains within the ISO/IEC 27001:2013 standards?
    1. Cryptography
    2. Personnel
    3. Compliance
    4. Integrity
       1. D
68. Which of the following roles is responsible for preparing systems for the cloud, administering and monitoring services, and managing inventory and assets?
    1. Cloud service manager
    2. Cloud service business manager
    3. Cloud service operations manager
    4. Cloud service deployment manager
       1. C
69. Which concept pertains to the official record of evidence and data, from its conception through destruction, and what is needed for official legal proceedings?
    1. Nonrepudiation
    2. Authentication
    3. Custodial records
    4. Chain of custody
       1. D
70. Which aspect of access control involves the verification of the identity of a user to establish their credentials within the system?
    1. Authorization
    2. Authentication
    3. Account provisioning
    4. Privileged access
       1. C
71. Which of the following are the storage types associated with PaaS?
    1. Structured and unstructured
    2. Volume and object
    3. Structured and freeform
    4. Database and file system
       1. A
72. Which of the following roles involves overseeing billing, purchasing, and requesting audit reports for an organization within a cloud environment?
    1. Cloud service administrator
    2. Cloud service user
    3. Cloud service integrator
    4. Cloud service business manager
       1. D
73. When two virtual machines are hosted on the same hypervisor, what must network traffic pass through in order to get from one virtual machine to the other?
    1. Firewall
    2. IDS
    3. IPS
    4. They can directly communicate
       1. D
74. What concept does the "A" represent in the DREAD model?
    1. Affected users
    2. Affinity
    3. Authorization
    4. Authentication
       1. A
75. Which certification is a general information security standard that is used internationally and is considered the "gold standard" for information and data security?
    1. ISO/IEC 27001
    2. NIST SP 800-53
    3. PCI DSS
    4. FIPS 140-2
       1. A
76. Which technology can be useful during the "share" phase of the cloud data lifecycle to continue to protect data as it leaves the original system and security controls?
    1. WAF
    2. DLP
    3. IDS
    4. IPS
       1. B
77. With software-defined networking, what aspect of networking is abstracted from the forwarding of traffic?
    1. Filtering
    2. Routing
    3. Firewalling
    4. Session
       1. A
78. Which of the cloud cross-cutting aspects relates to the ability to easily move services and applications between different cloud providers?
    1. Interoperability
    2. Portability
    3. Reversibility
    4. Availability
       1. B
79. 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?
    1. Portability
    2. Interoperability
    3. Resource pooling
    4. Broad network access
       1. D
80. Which of the following could be used as a second component for multifactor authentication if a user also has an RSA token?
    1. Access card
    2. RFID
    3. USB thumb drive
    4. Retinal scan
       1. D
81. Which of the following does NOT fall under the "IT" aspect of quality of service (QoS)?
    1. Key performance indicators (KPIs)
    2. Services
    3. Security
    4. Applications
       1. A
82. Which aspect of cloud computing makes data classification even more vital than in a traditional data center?
    1. Virtualization
    2. Portability
    3. Multitenancy
    4. Interoperability
       1. C
83. What is the biggest concern with hosting a key management system outside of the cloud environment?
    1. Confidentiality
    2. Integrity
    3. Availability
    4. Portability
       1. C
84. Which of the following threat types can occur when baselines are not appropriately applied or unauthorized changes are made?
    1. Security misconfiguration
    2. Insecure direct object references
    3. Sensitive data exposure
    4. Unvalidated redirects and forwards
       1. A
85. What feature of a SIEM solution can simplify an organization's strategy for log retention compliance?
    1. Alerting
    2. Aggregation
    3. Reporting
    4. Dashboards
       1. B
86. Which of the following threat types can occur when encryption is not properly applied or insecure transport mechanisms are used?
    1. Security misconfiguration
    2. Insecure direct object refences
    3. Sensitive data exposure
    4. Unvalidated redirects and forwards
       1. C
87. Which United States law is focused on PII as it relates to the financial industry?
    1. GLBA
    2. HIPAA
    3. Safe Harbor
    4. SOX
       1. A
88. Which type of common threat involves data being exposed to a party that is not authorized to have it?
    1. Data loss
    2. Data breach
    3. Malicious insider
    4. Account hijacking
       1. B
89. Which of the following technologies is used to monitor network traffic and block any potential threats or attacks that match defined signatures and policies?
    1. IDS
    2. IPS
    3. Firewall
    4. WAF
       1. B
90. What process is used within a cloud environment to maintain resource balancing and ensure that resources are available where and when needed?
    1. Dynamic optimization
    2. Dynamic resource scheduling
    3. Dynamic balancing
    4. Dynamic clustering
       1. A
91. Which of the following is NOT a unit that is used to define a limit with a cloud environment?
    1. Virtual machine
    2. Customer
    3. Application
    4. Hypervisor
       1. D
92. Which emerging type of encryption aims to allow the manipulation of data without the need to unencrypt it first?
    1. Elliptic curve
    2. Homomorphic
    3. Dynamic
    4. Transparent
       1. B
93. Which of the following pertains to fire safety standards within a data center, specifically with their enormous electrical consumption?
    1. IDCA
    2. BICSI
    3. NFPA
    4. Uptime Institute
       1. C
94. Which of the cloud deployment models requires the cloud customer to be part of a specific group or organization in order to host cloud services within it?
    1. Private
    2. Public
    3. Hybrid
    4. Community
       1. D
95. Which concept refers to the ability to confirm the origin or authenticity of data?
    1. Repudiation
    2. Nonrepudiation
    3. Authentication
    4. Validation
       1. B
96. Which approach is typically the most efficient method to use for data discovery?
    1. Labels
    2. Metadata
    3. Content analysis
    4. ACLs
       1. B
97. What strategy involves replacing sensitive data with opaque values, usually with a means of mapping it back to the original value?
    1. Anonymization
    2. Masking
    3. Obfuscation
    4. Tokenization
       1. D
98. Which security concept would business continuity and disaster recovery fall under?
    1. Confidentiality
    2. Integrity
    3. Availability
    4. Fault tolerance
       1. C
99. Which of the following roles is responsible for overseeing customer relationships and the processing of financial transactions?
    1. Cloud service manager
    2. Cloud service business manager
    3. Cloud service operations manger
    4. Cloud service deployment manager
       1. B
100. Which publication from the United States National Institute of Standards and Technology pertains to definitions for the various core components of cloud computing?
     1. SP 800-153
     2. SP 800-40
     3. SP 800-145
     4. SP 800-53
        1. C
101. When an organization is considering using multiple cloud providers for BCDR, which of the following concepts is the MOST important?
     1. Portability
     2. Interoperability
     3. Reversibility
     4. Elasticity
        1. A
102. With a SaaS implementation, which types of logs are typically available directly to the cloud customer?
     1. Patching
     2. Billing
     3. Change management
     4. Security
        1. B
103. What is the best source for information about securing a physical asset's BIOS?
     1. Regulations
     2. Manual pages
     3. Vendor documentation
     4. Security policies
        1. C
104. Which technique involves replacing values within a specific data field to protect sensitive data?
     1. Obfuscation
     2. Tokenization
     3. Masking
     4. Anonymization
        1. C
105. The WS-Security standards are built around all of the following standards except which one?
     1. WDSL
     2. SAML
     3. XML
     4. SOAP
        1. B
106. With a cloud environment, who is responsible for the collection of data pursuant to an eDiscovery order?
     1. The cloud provider
     2. The cloud customer
     3. The application owner
     4. Both the cloud provider and cloud customer
        1. D
107. With a federated identify system, where would a user perform their authentication when requesting services or application access?
     1. Their home organization
     2. The application
     3. Third-party authentication system
     4. Cloud provider
        1. A
108. Which of the cloud deployment models offers the most control and input to the cloud customer as to how the overall cloud environment is implemented and configured?
     1. Private
     2. Public
     3. Hybrid
     4. Community
        1. A
109. Which of the following security technologies is commonly used to give administrators access into trust zones within an environment?
     1. HTTPS
     2. IPSec
     3. VPN
     4. WAF
        1. C
110. What changes are necessary to application code in order to implement DNSSEC?
     1. Adding encryption modules
     2. Implementing certificate validations
     3. Additional DNS lookups
     4. No changes are needed
        1. D
111. Which entity requires all collection and storing of data on their citizens to be done on hardware that resides within their borders?
     1. United States
     2. Russia
     3. Germany
     4. France
        1. B
112. Over time, what is a primary concern for data archiving?
     1. Size of archives
     2. Format of archives
     3. Regulatory changes
     4. Recoverability
        1. D
113. What does the "SOC" acronym refer to with audit reports?
     1. Service Organization Control
     2. System Organization Control
     3. Service Origin Confidentiality
     4. System Organization Confidentiality
        1. A
114. Which European Union directive pertains to personal data privacy and individual's control over their personal data?
     1. 95/46/EC
     2. 2000/1/EC
     3. 99/9/EC
     4. 2013/27001/EC
        1. A
115. Which of the following is an example of a direct identifier?
     1. Name
     2. Location
     3. Race
     4. Religion
        1. A

What must SOAP rely on for security?

* 1. TLS
  2. SSL
  3. Encryption
  4. Tokenization
     1. C

1. Where would a DLP solution be implemented within an environment to monitor data in use?
   1. Virtual machine
   2. Client
   3. Network perimeter
   4. Firewalls
      1. B
2. Which value refers to the percentage of production level restoration needed to meet BCDR objectives?
   1. RPO
   2. RSL
   3. RTO
   4. SRE
      1. B
3. 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?
   1. Monitor
   2. Disable
   3. Stop
   4. Remove
      1. D
4. Which international standard is specifically for privacy involving cloud computing?
   1. ISO/IEC 27001
   2. ISO/IEC 18779
   3. ISO/IEC 27018
   4. ISO/IEC 31000
      1. C
5. Which security concept is focused on the trustworthiness of data?
   1. Confidentiality
   2. Integrity
   3. Availability
   4. Nonrepudiation
      1. B
6. Which of the following is NOT something that is maintained with chain of custody records?
   1. Access
   2. Formats
   3. Copyrights
   4. Locations
      1. C
7. Which jurisdiction lacks specific and comprehensive privacy laws at a national or top level of legal authority?
   1. European Union
   2. Russia
   3. United States
   4. Germany
      1. C
8. Which of the cloud cross-cutting aspects relates to the requirements placed on a system or application by law, policy, or requirements from standards?
   1. Auditability
   2. Governance
   3. Regulatory requirements
   4. Service-level agreements
      1. C
9. Which of the following is NOT an example of "something the user has" for a multifactor authentication system?
   1. Fingerprint
   2. USB drive
   3. RSA token
   4. Access card
      1. A
10. Which of the following free tools from VMware can be used for patch management on both hosts and virtual machines?
    1. vSphere Patch Manager
    2. vSphere Patch Update utility
    3. vSphere Update Service
    4. vSphere Update Manager
       1. D
11. Where is an XML firewall most commonly deployed in the environment?
    1. Between the firewall and application
    2. Between the presentation and application layers
    3. Between the IPS and firewall
    4. Between the application and data layers
       1. A
12. Which of the following can be useful for protection cloud customers from a denial-of-service (DoS) attack against another customer hosted in the same cloud?
    1. Limits
    2. Shares
    3. Measured service
    4. Reservations
       1. D
13. Which of the following is NOT a function performed by an SIEM solution?
    1. Searching
    2. Alerting
    3. Tracking
    4. Reporting
       1. C
14. Which of the following free tools from Microsoft can be used for patch management on Windows systems?
    1. Windows patch management tool
    2. Windows Server Update Service
    3. Windows Patch Update Service
    4. Windows Service Manager
       1. B
15. What controls the formatting and security of a volume storage system within a cloud environment?
    1. Hypervisor
    2. Management plane
    3. SAN host controller
    4. Operating system of the host
       1. D
16. What must be secured on physical hardware to prevent unauthorized access to systems?
    1. ALOM
    2. BIOS
    3. SSH
    4. RDP
       1. B
17. Which United States program was designed to enable organizations to bridge the gap between privacy laws and requirements of the United States and the European Union?
    1. GLBA
    2. HIPAA
    3. Safe Harbor
    4. SOX
       1. C
18. Which of the following would NOT be included in the criteria for audit deliverables?
    1. Format
    2. Length
    3. Audience
    4. Structure
       1. B
19. How is an object stored within an object storage system?
    1. Key value
    2. Tree structure
    3. Database
    4. LDAP
       1. A
20. What type of security threats is DNSSEC designed to prevent?
    1. Spoofing
    2. Snooping
    3. Injection
    4. Account hijacking
       1. A
21. Which of the following service capabilities gives the cloud customer the least amount of control over configurations and deployments?
    1. Platform
    2. Desktop
    3. Infrastructure
    4. Software
       1. D
22. When an organization uses a cloud provider for BCDR, where services are only enabled if needed in the event of an incident, which would be the most important consideration while bringing up services?
    1. Broad network access
    2. Resource pooling
    3. Measured service
    4. Rapid elasticity
       1. D
23. Which of the following cloud aspects complicates eDiscovery?
    1. Resource pooling
    2. Measured service
    3. Multitenancy
    4. On-demand self-service
       1. C
24. Which of the following concepts involves the ability to detect problems and automatically switch to redundant systems, based on the nature of the problem?
    1. High availability
    2. Elasticity
    3. Fault tolerance
    4. Orchestration
       1. C
25. Which of the following service categories entails the least amount of support needed on the part of the cloud customer?
    1. IaaS
    2. PaaS
    3. DaaS
    4. SaaS
       1. D
26. What does a cloud system use from a technical perspective to make decisions on the allocation of resources with shares?
    1. Size of the customer
    2. Cost of the resources
    3. Prioritization weighting
    4. Owner of the cloud provider
       1. C
27. Which security concept, if implemented correctly, will protect the data on a system, even if a malicious actor gains access to the actual system?
    1. Sandboxing
    2. Firewalls
    3. Encryption
    4. Access control
       1. C
28. What is the concept of segregating information or processes, within the same system or application, for security reasons?
    1. Cellblocking
    2. Sandboxing
    3. Pooling
    4. Fencing
       1. B
29. Which of the following security measures done at the network layer in a traditional data center are also applicable to a cloud environment?
    1. Dedicated switches
    2. Trust zones
    3. Direct connections
    4. Redundant network circuits
       1. B
30. What is an often overlooked concept that is essential to protecting the confidentiality of data?
    1. Security controls
    2. Policies
    3. Strong passwords
    4. Training
       1. D
31. Which approach to media sanitation involves the zeroing of data on a system to ensure that it cannot be put back together or recovered later?
    1. Cryptographic erasure
    2. Encryption
    3. Overwriting
    4. Nullification
       1. C
32. Unlike SOC Type 1 reports, which are based on a specific point in time, SOC Type 2 reports are done over a period of time. What is the minimum span of time for a SOC Type 2 report?
    1. One month
    2. One year
    3. Six months
    4. One week
       1. C
33. Where would a DLP solution be implemented within an environment to monitor data in transit?
    1. Virtual machine
    2. Client
    3. Network perimeter
    4. Firewalls
       1. C
34. What is the biggest challenge to data discovery in a cloud environment?
    1. Format
    2. Location
    3. Ownership
    4. Multitenancy
       1. B
35. Which of the following is the optimal temperature for a data center, per the guidelines established by the America Society of Heating, Refrigeration, and Air Conditioning Engineers (ASHRAE)?
    1. 51.8-66.2°F (11-19°C)
    2. 44.6-60.8°F (7-16°C)
    3. 64.4-80.6°F (18-27°C)
    4. 69.8-86.0°F (21-30°C)
       1. C
36. Which data format is the SAML standard based on?
    1. Oauth
    2. XML
    3. JSON
    4. HTML
       1. B
37. Which ITIL component is focused on reacting to disruptions to production services and ensuring they are restored as quickly as possible to their normal state?
    1. Incident management
    2. Problem management
    3. Information security management
    4. Availability management
       1. A
38. What does the REST API use to protect data transmissions?
    1. TLS
    2. NetBIOS
    3. Encapsulation
    4. VPN
       1. A
39. What concept does the "R" represent with the DREAD model?
    1. Repudiation
    2. Reproducibility
    3. Risk
    4. Residual
       1. B
40. Which of the following will have the biggest impact on the availability within a cloud environment?
    1. Cloud deployment model
    2. Cloud service model
    3. Cloud service category
    4. Cloud cross-cutting aspect
       1. B
41. Which type of testing uses the same strategies and toolsets that hackers would use?
    1. Penetration
    2. Static
    3. Dynamic
    4. Malicious
       1. A
42. Within a federated identity system, to whom does the identity provider send information after a successful authentication?
    1. Service relay
    2. Relaying party
    3. Relying party
    4. Service originator
       1. C
43. Which of the following represents a minimum guaranteed resource within a cloud environment for the cloud customer?
    1. Reservation
    2. Limit
    3. Share
    4. Provision
       1. A
44. What are the two protocols that TLS uses?
    1. Handshake and record
    2. Handshake and transport
    3. Transport and initiate
    4. Record and transmit
       1. A
45. Which concept BEST describes the capability for a cloud environment to automatically scale a system or application, based on its current resource demands?
    1. Rapid elasticity
    2. Measured service
    3. On-demand self-service
    4. Resource pooling
       1. A
46. What is the concept of isolating an application from the underlying operating system for testing purposes?
    1. Abstracting
    2. Application virtualization
    3. Sandboxing
    4. Hosting
       1. B
47. Which aspect of archiving must be tested regularly for the duration of retention requirements?
    1. Portability
    2. Auditability
    3. Recoverability
    4. Availability
       1. C
48. What concept does the "D" represent with the STRIDE threat model?
    1. Data loss
    2. Distributed
    3. Denial of service
    4. Data breach
       1. C
49. Which of the following roles involves the provisioning and delivery of cloud services?
    1. Cloud service manager
    2. Cloud service business
    3. Cloud service operations manager
    4. Cloud service deployment manger
       1. A
50. Which type of common threat involves an organization not taking proper precautions or planning to mitigate threats to their system or applications?
    1. Insufficient due diligence
    2. System vulnerability
    3. Malicious insider
    4. Account hijacking
       1. A
51. Which security concept is based on preventing unauthorized access to data while also ensuring that it is accessible to those authorized to use it?
    1. Confidentiality
    2. Integrity
    3. Availability
    4. Nonrepudiation
       1. A
52. Which aspect of cloud computing will be most negatively impacted by vendor lock-in?
    1. Interoperability
    2. Portability
    3. Reversibility
    4. Elasticity
       1. B
53. What are the two types of physical storage systems typically used in a cloud environment?
    1. RAID and SCSI
    2. iSCSI and SDD
    3. SAN and SDD
    4. RAID and SAN
       1. D
54. Which of the following actions will NOT make data part of the "create" phase of the cloud data lifecycle?
    1. Importing data
    2. Modifying data
    3. Modifying metadata
    4. Constructing new data
       1. C
55. Which of the following is NOT part of a retention policy?
    1. Format
    2. Duration
    3. Accessibility
    4. Costs
       1. D
56. Which certification pertains to the accreditation of cryptographic modules?
    1. ISO/IEC 27001
    2. NIST SP 800-53
    3. PCI DSS
    4. FIPS 140-2
       1. D
57. Which of the cloud deployment models is used by popular services such as iCloud, Dropbox, and OneDrive?
    1. Private
    2. Public
    3. Hybrid
    4. Community
       1. B
58. From a security perspective, which of the following is a major concern when evaluating possible BCDR solutions?
    1. Access provisioning
    2. Jurisdictions
    3. Authorization
    4. Auditing
       1. B
59. Which of the following roles is responsible for creating cloud components and the testing and validation of services?
    1. Cloud service developer
    2. Inter-cloud provider
    3. Cloud auditor
    4. Cloud service broker
       1. A
60. Why does a Type 1 hypervisor typically offer tighter security controls than a Type 2 hypervisor?
    1. A Type 1 hypervisor only hosts virtual machines with the same operating systems as the hypervisor.
    2. A Type 1 hypervisor is tied directly to the bare metal and only runs with code necessary to perform its specific mission.
    3. A Type 1 hypervisor also controls patching of its hosted virtual machines to ensure they are always secure.
    4. A Type 1 hypervisor performs hardware-level encryption for tighter security and efficiency.
       1. B
61. From a storage perspective, what is the partition allocated to a virtual machine for volume storage referred to?
    1. LAN
    2. Partition
    3. LUN
    4. HDD
       1. C
62. From a legal perspective, what is the most important first step after an eDiscovery order has been received by the cloud provider?
    1. Data collection
    2. Key identification
    3. Notification
    4. Virtual image snapshots
       1. C
63. Which of the following is NOT a regulatory system from the United States federal government?
    1. SOX
    2. PCI DSS
    3. HIPPA
    4. FISMA
       1. B
64. Which of the following threat types involves an application developer leaving references to internal information and configurations in code that is exposed to the client?
    1. Security misconfiguration
    2. Insecure direct object references
    3. Sensitive data exposure
    4. Unvalidated redirects and forwards
       1. B
65. When establishing a baseline, what should you do immediately after a fresh operating system install?
    1. Apply patching
    2. Remove unnecessary software
    3. Apply configurations
    4. Create documentation
       1. B
66. Which of the cloud cross-cutting aspects relates to the oversight of processes and systems, as well as to ensuring their compliance with specific policies and regulations?
    1. Auditability
    2. Governance
    3. Regulatory requirements
    4. Service-level agreements
       1. A
67. Which process serves to prove the identity and credentials of a user requesting access to an application or data?
    1. Authorization
    2. Repudiation
    3. Identification
    4. Authentication
       1. D
68. Which of the following approaches would NOT be considered sufficient to meet the requirements of secure data destruction within a cloud environment?
    1. Deletion
    2. Cryptographic erasure
    3. Overwriting
    4. Zeroing
       1. A
69. Which value refers to the amount of data an organization would need to recover in the event of a BCDR situation in order to reach an acceptable level of operations?
    1. RPO
    2. RSL
    3. RTO
    4. SRE
       1. A
70. What is a major challenge with forensic data collection within a cloud environment?
    1. Size of data
    2. Classification of data
    3. Ownership of data
    4. Format of data
       1. C
71. Which type of common threat involves leveraging access to an environment to snoop on other systems within it?
    1. Insufficient due diligence
    2. System vulnerability
    3. Malicious insider
    4. Account hijacking
       1. D
72. What type of masking strategy involves making a separate and distinct copy of data with masking in place?
    1. Static
    2. Replication
    3. Duplication
    4. Dynamic
       1. A
73. Which of the following is NOT a focus or consideration of an internal audit?
    1. Operational efficiency
    2. Costs
    3. Design
    4. Certification
       1. D
74. Which of the cloud cross-cutting aspects relates to the ability to reuse or move components of an application or service?
    1. Interoperability
    2. Portability
    3. Reversibility
    4. Availability
       1. A
75. Which of the following is NOT one of the three methods of data discovery?
    1. Metadata
    2. Labels
    3. Content analysis
    4. Heuristics
       1. D
76. Which United States law is focused on data related to health records and privacy?
    1. GLBA
    2. HIPAA
    3. Safe Harbor
    4. SOX
       1. B
77. Which of the following features is a main benefit of PaaS over IaaS?
    1. Auto-scaling
    2. High-availability
    3. Location independence
    4. Physical security requirements
       1. A
78. Which of the following is NOT one of the official risk rating categories?
    1. Low
    2. Minimal
    3. Critical
    4. Catastrophic
       1. D
79. What does static application security testing (SAST) offer as a tool to the testers?
    1. Live testing
    2. Production system scanning
    3. Source code access
    4. Injection attempts
       1. C
80. What is essential to change immediately upon the installation of new software components?
    1. Default credentials
    2. Certificates
    3. Open ports
    4. Firewalls
       1. A
81. Which data point that auditors always desire is very difficult to provide within a cloud environment?
    1. Access policy
    2. Privacy statement
    3. Systems architecture
    4. Baselines
       1. C
82. What is a serious complication an organization face from the perspective of compliance with international operations?
    1. Multiple jurisdictions
    2. Different certifications
    3. Different capabilities
    4. Different operational procedures
       1. A
83. What process is used within a clustered system to provide high availability and load balancing?
    1. Dynamic optimization
    2. Dynamic resource scheduling
    3. Dynamic balancing
    4. Dynamic clustering
       1. B
84. Which of the following roles involves the connection and integration of existing systems and services to a cloud environment?
    1. Cloud service administrator
    2. Cloud service user
    3. Cloud service integrator
    4. Cloud service business manager
       1. C
85. Which of the following attempts to establish an international standard for eDiscovery processes and best practices?
    1. ISO/IEC 27001
    2. ISO/IEC 19888
    3. ISO/IEC 31000
    4. ISO/IEC 27050
       1. D
86. Which crucial aspect of cloud computing can be most threatened by insecure APIs?
    1. Automation
    2. Resource pooling
    3. Elasticity
    4. Redundancy
       1. A
87. Which networking concept in a cloud environment allows for network segregation and isolation of IP spaces?
    1. VLAN
    2. LAN
    3. WAN
    4. PLAN
       1. A
88. Which ITIL component is focused on ensuring that changes made to a production environment are properly executed and validated?
    1. Change management
    2. Configuration management
    3. Deployment management
    4. Release management
       1. C
89. Which concept refers to the programmatic handling of resource allocation and configuration within a cloud environment?
    1. Automation
    2. Orchestration
    3. Provisioning
    4. Allocation
       1. B
90. What type of technology/system is typically used for log aggregation and storage at an enterprise level?
    1. LSS
    2. SIM
    3. SIEM
    4. SEM
       1. C
91. Which of the following is NOT one of the five principles of SOC Type 2 audits?
    1. Security
    2. Processing integrity
    3. Privacy
    4. Financial
       1. D
92. Which state of data involves data that is stored on a file system or storage device?
    1. Data in use
    2. Data in transit
    3. Data in storage
    4. Data at rest
       1. D
93. Which of the cloud cross-cutting aspects relates to the assigning of jobs, tasks, and roles, as well to ensuring they are successful and properly performed?
    1. Auditability
    2. Governance
    3. Regulatory requirements
    4. Service-level agreements
       1. B
94. Under SOC Type 2 audits, the security principle contains seven separate categories. Which of the following is NOT one of the seven categories?
    1. Change management
    2. Communications
    3. System operations
    4. Incident management
       1. D
95. Which is the appropriate phase of the cloud data lifecycle for determining the data's classifications?
    1. Create
    2. Use
    3. Store
    4. Share
       1. A
96. What is the primary reason that makes resolving jurisdictional conflicts complicated?
    1. Costs
    2. Lack of international authority
    3. Language barriers
    4. Differing technology standards
       1. B
97. Which United States law is focused on accounting and financial practices of organizations?
    1. GLBA
    2. HIPAA
    3. Safe Harbor
    4. SOX
       1. D
98. Which of the following roles is responsible for gathering metrics on cloud services and managing cloud deployments and the deployment processes?
    1. Cloud service manager
    2. Cloud service business manager
    3. Cloud service operations manager
    4. Cloud service deployment
       1. D
99. Which of the following does NOT relate to the hiding of sensitive data from data sets?
    1. Obfuscation
    2. Federation
    3. Masking
    4. Anonymization
       1. B
100. Which type of common threat involves trusted and approved users of a system leveraging their legitimate access for unauthorized purposes?
     1. Insufficient due diligence
     2. Data breach
     3. Malicious insider
     4. Account hijacking
        1. C
101. Which of the following is a restriction that can be enforced by information rights management (IRM) that is not possible for traditional file system controls?
     1. Read
     2. Delete
     3. Print
     4. Modify
        1. C
102. Which of the following APIs are most commonly used within a cloud environment?
     1. XML and SAML
     2. REST and SAML
     3. SOAP and REST
     4. REST and XML
        1. C
103. What provides the information to an application to make decisions about the authorization level appropriate when granting access?
     1. User
     2. Identity provider
     3. Relying party
     4. Federation
        1. B
104. Which security concept does encryption apply to?
     1. Confidentiality
     2. Integrity
     3. Availability
     4. Compliance
        1. A
105. Which of the following roles is responsible for obtaining new customers and securing contracts and agreements?
     1. Cloud service developer
     2. Inter-cloud provider
     3. Cloud auditor
     4. Cloud service broker
        1. D
106. Which type of audit reports are intended for broad or public release?
     1. SAS-70
     2. SOC Type 1
     3. SOC Type 2
     4. SOC Type 3
        1. D
107. Which of the following shows the correct order for the steps in BCDR planning?
     1. Define scope, gather requirements, assess risk, implement
     2. Gather requirements, define scope, assess risk, implement
     3. Define scope, gather requirements, implement, assess risk
     4. Gather requirements, define scope, implement, assess risk
        1. A
108. Which of the following would NOT be a potential impact of changing the location of services during a BCDR incident?
     1. Network latency
     2. Regulations
     3. Authentication methods
     4. Administrative access
        1. C
109. Which step in the cloud secure data lifecycle comes immediately after "create"?
     1. Use
     2. Share
     3. Store
     4. Secure
        1. C
110. What is the only data format permitted with SOAP API?
     1. HTML
     2. XSML
     3. XML
     4. SAML
        1. C
111. From a security perspective, what must be defined for an audit before any testing or collection is performed?
     1. Classification
     2. Reports
     3. Audience for reports
     4. Debriefing schedule
        1. A
112. Which of the following is the sole responsibility of the cloud customer, regardless of which cloud model is used?
     1. Infrastructure
     2. Application
     3. Governance
     4. Platform
        1. C
113. Which of the following is the sole responsibility of the cloud provider, regardless of which cloud model is used?
     1. Infrastructure
     2. Data
     3. Physical environment
     4. Platform
        1. C
114. Which of the following is the sole responsibility of the cloud customer, regardless of which cloud model is used?
     1. Infrastructure
     2. Data
     3. Application
     4. Platform
        1. B
115. What feature of a SIEM solution enables the discovery of similar events throughout the enterprise?
     1. Alerting
     2. Correlation
     3. Reporting
     4. Dashboards
        1. B
116. From a security perspective, what advantage does a network-based IDS have over a host-based IDS?
     1. System load
     2. Dedicated appliance
     3. Separately maintained from the host
     4. Removed from patching cycles
        1. C
117. Which of the following is the MOST important requirement and guidance for testing during an audit?
     1. Management
     2. Stakeholders
     3. Regulations
     4. Shareholders
        1. C
118. Which of the cloud cross-cutting aspects relates to the ability for a cloud customer to easily remove their applications and data from a cloud environment?
     1. Interoperability
     2. Portability
     3. Reversibility
     4. Availability
        1. C
119. What type of PII is regulated based on the type of application or per the conditions of the specific hosting agreement?
     1. Regulated
     2. Contractual
     3. Jurisdictional
     4. Specific
        1. B
120. Which attribute of data poses the biggest challenge for data discovery?
     1. Format
     2. Volume
     3. Labels
     4. Quality
        1. D
121. Which approach to data removal involves the destruction of keys rather than the actual deletion of data?
     1. Cryptographic erasure
     2. Encryption
     3. Overwriting
     4. Nullification
        1. A
122. Which of the following threat types involves the sending of untrusted data to a user's browser to be executed with their own credentials and access?
     1. Missing function level access control
     2. Cross-site request forgery
     3. Cross-site scripting
     4. Injection
        1. C
123. With an IaaS implementation, which logs will be available directly to the cloud customer without needing the cloud provider to supply them?
     1. Operating system
     2. DNS
     3. Network perimeter
     4. Hypervisor
        1. A
124. Which of the following concepts refers to a cloud customer paying only for the resources and offerings they use within a cloud environment, and only for the duration that they are consuming them?
     1. Metered service
     2. Billable service
     3. Consumable service
     4. Measured service
        1. D
125. What is a standard configuration and policy set that is applied to systems and virtual machines called?
     1. Baseline
     2. Redline
     3. Hardening
     4. Standardization
        1. A
126. At which stage of the BCDR plan creation phase should security be included in discussions?
     1. Gather requirements
     2. Analyze
     3. Assess risk
     4. Define scope
        1. D
127. Which of the following is an example of an indirect identifier?
     1. Name
     2. Location
     3. Date of birth
     4. National ID number
        1. B
128. Which of the following is NOT something that an HIDS will monitor?
     1. Network traffic
     2. Critical system files
     3. User logins
     4. Configurations
        1. C
129. Which of the following standards primarily pertains to cabling designs and setups in a data center?
     1. IDCA
     2. BICSI
     3. NFPA
     4. Uptime Institute
        1. B
130. Which value refers to the amount of time it takes to recover operations in a BCDR situation to meet management's objectives?
     1. RPO
     2. RSL
     3. RTO
     4. SRE
        1. C
131. What type of segregation and separation of resources is needed within a cloud environment for multitenancy purposes versus a traditional data center model?
     1. Virtual
     2. Logical
     3. Physical
     4. Security
        1. B
132. Which of the following statements accurately describes VLANs?
     1. They are restricted to the same racks and data centers.
     2. They are not restricted to the same rack but restricted to the same data center.
     3. They are not restricted to the same data center or the same racks.
     4. They are not restricted to the same rack but restricted to same switches.
        1. C
133. Which aspect of access control involves users having administrative access to a system, or higher levels of access and permissions than normal users would have?
     1. Authorization
     2. Authentication
     3. Account provisioning
     4. Privileged access
        1. D
134. What strategy involves hiding data in a data set to prevent someone from identifying specific individuals based on other data fields present?
     1. Anonymization
     2. Masking
     3. Obfuscation
     4. Tokenization
        1. A
135. Which data formats are most commonly used with the REST API?
     1. XML and JSON
     2. JSON and SAML
     3. XML and SAML
     4. SAML and HTML
        1. A
136. Which of the following service capabilities gives the cloud customer an established and maintained framework to deploy code and applications?
     1. Platform
     2. Desktop
     3. Infrastructure
     4. Software
        1. A
137. Which type of key management service involves a system that is provided by the cloud provider but hosted and maintained by the cloud customer?
     1. Remote key management service
     2. Client-side key management service
     3. External key management service
     4. Customer key management service
        1. B
138. Which of the following regulatory systems contains provisions that require a minimum length of time that financial records must be retained?
     1. HIPAA
     2. FedRAMP
     3. PCI DSS
     4. SOX
        1. D
139. Which type of audit report does many cloud providers use to instill confidence in their policies, practices, and procedures to current and potential customers?
     1. SOC 2
     2. SOC 1
     3. SAS-70
     4. SOX
        1. A
140. Which ITIL component is focused on structured and methodical modifications to systems or applications?
     1. Change management
     2. Configuration management
     3. Deployment management
     4. Release management
        1. A
141. What type of network model combines the storage and IP-based traffic into a single virtualized design?
     1. Converged
     2. Concurrent
     3. Combined
     4. Cooperative
        1. A
142. The European Union passed the first major regulation declaring data privacy to be a human right. In what year did it go into effect?
     1. 2010
     2. 2000
     3. 1995
     4. 1990
        1. C
143. What does a single sign-on system pass between services to validate authentication?
     1. Tokens
     2. Tickets
     3. Certificates
     4. Keys
        1. A
144. What concept does the "I" represent with the STRIDE threat model?
     1. Integrity
     2. Information disclosure
     3. IT security
     4. Insider threat
        1. B
145. Which aspect of access control involves ensuring users are assigned to the correct roles and levels of access within a system, once they have successfully proven their identity to the system?
     1. Authorization
     2. Authentication
     3. Account provisioning
     4. Privileged access
        1. A
146. What expectation of data custodians is made much more challenging by a cloud implementation, especially with PaaS or SaaS?
     1. Access to data
     2. Knowledge of systems
     3. Data classification
     4. Encryption requirements
        1. B
147. Which of the following are the storage types associated with IaaS?
     1. Volume and label
     2. Object and target
     3. Volume and object
     4. Volume and container
        1. C
148. Which of the following is NOT an application or utility to apply and enforce baselines on a system?
     1. Chef
     2. GitHub
     3. Puppet
     4. Active Directory
        1. B
149. Which audit type has been largely replaced by newer approaches since 2011?
     1. SOC Type 1
     2. SAS-70
     3. SOC Type 2
     4. SSAE-16
        1. B
150. Which process is used to prevent the aggregation of indirect identifiers from directly identifying an individual?
     1. Tokenization
     2. Masking
     3. Obfuscation
     4. Anonymization
        1. D
151. Which of the following is the optimal humidity level for a data center, per the guidelines established by the America Society of Heating, Refrigeration, and Air Conditioning Engineers (ASHRAE)?
     1. 40-60 percent relative humidity
     2. 30-50 percent relative humidity
     3. 50-70 percent relative humidity
     4. 20-40 percent relative humidity
        1. A
152. Which of the following roles involves testing, monitoring, and securing cloud services for an organization?
     1. Cloud service administrator
     2. Cloud service user
     3. Cloud service integrator
     4. Cloud service business manager
        1. A
153. Which of the following threat types involves the sending of commands or arbitrary data through input fields in an application in an attempt to get them executed as part of normal processing?
     1. Missing function-level access control
     2. Cross-site request forgery
     3. Cross-site scripting
     4. Injection
        1. D
154. Which of the following should NOT be part of the requirement analysis phase of the software development lifecycle?
     1. Programming languages
     2. Security requirements
     3. Software platform
     4. Functionality
        1. B
155. Which of the cloud deployment models offers the easiest initial setup and access for the cloud customer?
     1. Private
     2. Public
     3. Hybrid
     4. Community
        1. B
156. What network provisioning protocol is essential for automation and orchestration within a cloud environment?
     1. DNS
     2. DNSSEC
     3. DHCP
     4. DDoS
        1. C
157. Which of the following pertains to a macro level approach to data center design rather than the traditional tiered approach to data centers?
     1. IDCA
     2. BICSI
     3. NFPA
     4. Uptime Institute
        1. A
158. When can risk be fully mitigated?
     1. With risk transference
     2. Never
     3. With risk avoidance
     4. When using a private cloud
        1. B
159. Which of the following is NOT a function performed by the record protocol of TLS?
     1. Compression
     2. Authentication
     3. Encryption
     4. Acceleration
        1. D
160. Which cloud service model entails patching responsibility for the cloud customer?
     1. DaaS
     2. PaaS
     3. IaaS
     4. SaaS
        1. C
161. What does SDN stand for within a cloud environment?
     1. Software-dependent networking
     2. System-dynamic nodes
     3. Software-dynamic networking
     4. Software-defined networking
        1. D
162. Which of the following threat types can occur when an application does not properly validate input and can be leveraged to send users to malicious sites that appear to be legitimate?
     1. Security misconfiguration
     2. Insecure direct object references
     3. Sensitive data exposure
     4. Unvalidated redirects and forwards
        1. D
163. With an application hosted in a cloud environment, who could be the recipient of an eDiscovery order?
     1. The cloud provider
     2. The cloud customer
     3. Users
     4. Both the cloud provider and cloud customer
        1. D
164. Which of the cloud cross-cutting aspects relates to the requirements placed on the cloud provider by the cloud customer for minimum performance standards and requirements that must be met?
     1. Auditability
     2. Governance
     3. Regulatory requirements
     4. SLAs
        1. D
165. Which protocol does the REST API depend on?
     1. XML
     2. SAML
     3. SSH
     4. HTTP
        1. D
166. Which ITIL component is focused on maintaining detailed information about all components and services within an organization?
     1. Change management
     2. Configuration management
     3. Deployment management
     4. Release management
        1. B
167. Which ITIL component is focused on ensuring that services are configured and monitored for confidentiality, integrity, and availability?
     1. Incident management
     2. Problem management
     3. Information security management
     4. Availability management
        1. C
168. Which of the following would NOT be an appropriate limitation to be included as an audit restriction?
     1. Names of auditors
     2. Devices of auditors
     3. Types of invasive testing
     4. Length of audit report
        1. D
169. Which of the following storage types is most closely associated with a traditional file system and tree structure?
     1. Structured
     2. Unstructured
     3. Object
     4. Volume
        1. D
170. Which of the following would NOT be considered part of resource pooling with an Infrastructure as a Service implementation?
     1. CPU
     2. Memory
     3. Storage
     4. Application
        1. D
171. Which certification and standard is published by the United States federal government and pertains to information security requirements for federal agencies and government contractors?
     1. ISO/IEC 27001
     2. NIST SP 800-53
     3. PCI DSS
     4. FIPS 140-2
        1. B
172. Which of the following technologies is used to monitor network traffic and block any potential threats or attacks that match defined signatures and policies?
     1. IDS
     2. IPS
     3. Firewall
     4. WAF
        1. B
173. Which of the following is NOT a key area for performance monitoring as far as an SLA is concerned?
     1. Users
     2. Memory
     3. CPU
     4. Network
        1. A
174. Which certification and standard is published by the credit card industry for specific IT security controls and practices for any vendors that accept their cards?
     1. ISO/IEC 27001
     2. NIST SP 800-53
     3. PCI DSS
     4. FIPS 140-2
        1. C
175. Who would be responsible for implementing IPsec to secure communications for an application?
     1. Cloud customer
     2. Developers
     3. Auditors
     4. Systems staff
        1. D
176. What concept does the "T" represent in the STRIDE threat model?
     1. TLS
     2. Transport
     3. Tampering with data
     4. Testing
        1. C
177. What type of PII is controlled based on laws and carries legal penalties for noncompliance with requirements?
     1. Regulated
     2. Contractual
     3. Jurisdictional
     4. Specific
        1. A
178. Which type of key management service involves storing and maintaining keys by the customer at their own location?
     1. Remote key management service
     2. Client-side key management service
     3. External key management service
     4. Customer key management service
        1. A
179. Which aspect of security is DNSSEC designed to ensure?
     1. Confidentiality
     2. Integrity
     3. Availability
     4. Authentication
        1. B
180. Which of the following represents a prioritization of applications or cloud customers for the allocation requested resources when there is a limitation on available resources?
     1. Reservation
     2. Limit
     3. Share
     4. Provision
        1. C
181. Which of the following is NOT one of the components of multifactor authentication?
     1. Something the user knows
     2. Something the user has
     3. Something the user is
     4. Something the user sends
        1. D
182. Which of the following is NOT one of the four official steps of an audit plan?
     1. Define objectives
     2. Define scope
     3. Lessons learned
     4. Billing and compensation
        1. D
183. Which of the following threat types involves the sending of invalid and manipulated requests through a user's client to execute commands on an application under the user's own credentials?
     1. Missing function level access control
     2. Cross-site request forgery
     3. Cross-site scripting
     4. Injection
        1. B
184. What is the data encapsulation used with the SOAP protocol referred to?
     1. Object
     2. Envelope
     3. Packet
     4. Payload
        1. B
185. When an Infrastructure as a Service model, which of the following would NOT be measured service?
     1. Storage
     2. CPU
     3. Number of users
     4. Memory
        1. C
186. What does the REST API support that SOAP does NOT support?
     1. Encryption
     2. Acceleration
     3. Caching
     4. Redundancy
        1. C
187. What type of masking strategy involves replacing data on a system while it passes between the data and application layers?
     1. Static
     2. Replication
     3. Duplication
     4. Dynamic
        1. D
188. What is the first stage of the cloud data lifecycle where security controls can be implemented?
     1. Create
     2. Use
     3. Store
     4. Share
        1. C
189. Which of the following defines what systems and applications are included with an audit?
     1. Scope
     2. Purpose
     3. Audience
     4. Limitations
        1. A
190. Which type of controls are the SOC Type 1 reports specifically focused on?
     1. PII
     2. Financial
     3. Privacy
     4. Integrity
        1. B
191. Which of the following is a commonly used tool for maintaining system configurations?
     1. Orchestrator
     2. Maestro
     3. Puppet
     4. Conductor
        1. C