CCSP Cloud Security Prep

Free Practice Test — 30 Real Exam-Style Questions

with full answer key & explanations

Practice Questions

Try all 30 first, then check the answer key at the back.

1. Which of the following techniques is commonly used to enhance the security and availability of cloud-stored data?

A. Data loss prevention
B. Data masking
C. Data aggregation
D. Data sharding

2. What security challenge is commonly associated with improper disposal practices of cloud resources?

A. Malware
B. Data Leakage
C. Unauthorized Access
D. Denial of Service

3. A CASB (Cloud Access Security Broker) generates an alert for security personnel. This is part of which phase of the CASB process?

A. Discovery
B. Mapping
C. Monitoring
D. Enforcement

4. An IT manager needs to ensure that sensitive customer data stored in an organization's cloud environment is not improperly accessed or leaked. Which technology can be employed to monitor and restrict access to sensitive data stored in cloud repositories?

A. Virtual Private Network (VPN)
B. Encryption
C. Cloud Access Security Broker (CASB)
D. Multi-Factor Authentication (MFA)

5. Which type of cloud storage behaves as if it were a connected external storage drive to a virtual machine?

A. Long-Term
B. Volume
C. Object
D. Ephemeral

6. Annie has been brought into a company to oversee the migration of their existing IT infrastructure to a cloud environment. At what stage in the migration process should security be addressed first?

A. Post-Migration Review
B. Optimization
C. Planning
D. Deployment

7. Maya, a cloud security analyst, has been alerted by her company's Security Operations Center (SOC) to assist in an incident involving unauthorized access to an encryption key management system within their Infrastructure as a Service (IaaS) deployment. She needs to ensure that all evidence collected is protected from tampering or alteration. What crucial process must Maya follow?

A. Chain of custody
B. Due diligence
C. Due care
D. Data masking

8. Which of the following is MOST closely related to the concept of Identity and Access Management (IAM) within cloud computing?

A. Threat Detection
B. Authentication
C. Data Encryption
D. Network Segmentation

9. An organization has adopted a cloud-based management system to ensure administrators cannot inadvertently change operational data or configuration settings. Which security measure has been implemented in this scenario?

A. Separation of system and user functionality
B. Security function isolation
C. Boundary protection
D. Denial of Service (DoS) protection

10. Which of the following NIST controls for access control is MOST closely related to the management of policies such as multi-factor authentication and account lockout settings?

A. Separation of Duties
B. Least Privilege
C. Auditable Events
D. Access Enforcement

11. A malicious script is embedded within a legitimate email sent to multiple recipients. When recipients open the email, their browser executes the script, leading to the theft of login credentials. What type of attack is being described?

A. Cross Site Request Forgery (CSRF)
B. Cross-site scripting (XSS)
C. Structured Query Language (SQL) injection
D. eXternal Markup Language (XML) external entities (XEE)

12. Which of the following organizations developed the Shared Responsibility Model for cloud security?

A. OWASP
B. SANS
C. ISO
D. AWS

13. Which of the following tools is primarily used to identify security vulnerabilities in container images?

A. Dynamic Application Security Testing (DAST)
B. Interactive Application Security Testing (IAST)
C. Container Security Scanner
D. Static Application Security Testing (SAST)

14. During which phase of the SDLC are security requirements identified and documented?

A. Testing
B. Requirements
C. Design
D. Development

15. At what phase of the cloud application lifecycle does the implementation and testing of security controls occur?

A. Testing
B. Planning
C. Deployment
D. Operations & Maintenance

16. A mid-sized retail company decided to migrate its e-commerce platform from one cloud provider to another without experiencing downtime or data loss. What BEST describes the ability to do this?

A. Reversibility to retrieve all assets from the initial provider and portability to migrate data seamlessly.
B. Portability to retrieve all assets from the initial provider and interoperability to migrate data seamlessly.
C. Interoperability to retrieve all assets from the initial provider and migrate data seamlessly.
D. Interoperability between the two cloud providers allows data migration and portability for the data.

17. Which of the following is PRIMARILY a concern when integrating cloud-based applications with on-premises systems?

A. Performance
B. Interoperability
C. Resiliency
D. Availability

18. A multinational corporation intends to integrate their existing HR management system with a cloud-based platform. Their cloud security specialist, Ethan, collaborates with IT admins to make the transition smooth. They plan to maintain their current user authentication methods within their on-premises data centers for a period. Employee data and applications will be hosted in the cloud. Which protocol can they employ for their IAM solution to ensure seamless integration between their on-premises data centers and the cloud?

A. Dynamic Host Configuration Protocol (DHCP)
B. Security Assertion Markup Language (SAML)
C. Lightweight Directory Access Protocol (LDAP)
D. Domain Name Service (DNS)

19. A cloud security architect is advising a company on migrating their applications to a cloud provider. The company wants to ensure they can easily move their applications to another provider if needed, avoiding vendor lock-in. What key cloud concept should they focus on to address this requirement?

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

20. When a company plans to migrate its applications to a cloud provider's Infrastructure as a Service (IaaS) platform, what is the most critical factor to evaluate before signing contracts?

A. Evaluating cost-efficiency
B. Assessing vendor reputation
C. Reviewing service level agreements (SLAs)
D. Ensuring data integrity and security

21. Leah is a cloud security engineer working for a major financial services firm. During a routine audit, she identifies an unusual activity that warrants further investigation. To determine the potential risk and prioritize mitigation steps, what standardized framework could she use to assess the severity of the identified vulnerability?

A. Common Vulnerability Scoring System
B. Common Weakness Enumeration
C. Common Vulnerabilities and Exposures
D. National Vulnerability Database

22. Marie is working in the Cloud Security Operations team for a healthcare organization. She is reviewing security alerts from a tool that can detect unauthorized access attempts to the cloud infrastructure. What tool is likely generating these alerts?

A. Cloud Intrusion Prevention System (CIPS)
B. File Integrity Monitor (FIM)
C. Host-based anti-malware
D. Cloud Intrusion Detection System (CIDS)

23. Maya is configuring her Platform as a Service (PaaS) environment and wants to ensure that application requests are directed to different instances dynamically to improve response times and availability. What is she implementing?

A. High availability
B. Auto-scaling
C. Load balancing
D. Failover

24. In a cloud security operations environment, which group is the LEAST likely to have a Service Level Agreement (SLA) or formal contract with a cloud service provider (CSP)?

A. Suppliers
B. Partners
C. Regulatory Authorities
D. Clients

25. You are a security administrator for a financial institution that has recently transitioned its transactional systems to a cloud-based platform. As part of your duties, you need to establish a comprehensive incident response plan for potential security breaches in the cloud environment. Which of the following aspects need to be included?

A. Detection and analysis, containment, eradication and recovery, financial audit data
B. Detection and analysis, containment, eradication and recovery, post-incident activities
C. Detection and analysis, containment, Maximum Tolerable Downtime, post-incident activities
D. Detection and analysis, response team labeling, eradication and recovery, post-incident activities

26. In a cloud service provider (CSP) context, which of the following entities is MOST likely to receive notifications about service degradations or interruptions to maintain transparency and protect the CSP's reputation?

A. Clients
B. Managed Service Providers
C. Hardware Suppliers
D. Compliance Auditors

27. The Sarbanes-Oxley Act (SOX) specifically applies to which of the following?

A. Financial institutions only
B. Non-profit organizations
C. Publicly traded companies
D. Health care providers

28. A cloud service provider is working with various clients in the healthcare sector and needs to ensure data privacy and security. Which of the following regulations should the provider be primarily concerned with to address the clients' compliance requirements?

A. Health Insurance Portability and Accountability Act (HIPAA)
B. Sarbanes-Oxley Act (SOX)
C. Gramm-Leach-Bliley Act (GLBA)
D. Asia Pacific Economic Cooperation (APEC)

29. In the context of healthcare data management, what role does a hospital's IT department typically play?

A. Data Owner
B. Data Custodian
C. Data Steward
D. Data Processor

30. Michael has been recently hired by a multinational tech company. His first training program is focused on protecting users' personal identifiable information during processing and storage. Which regulation governs this aspect and which region does it apply to?

A. Personal Information Protection and Electronic Documents Act (PIPEDA), Canada
B. Data Protection Act 2018 (DPA 2018), UK
C. General Data Protection Regulation (GDPR), European Union
D. California Consumer Privacy Act (CCPA), USA

Answer Key & Explanations

1. D — Data sharding
Answer: Data sharding Data sharding involves dividing a large dataset into smaller, more manageable pieces (shards) that can be distributed across multiple servers or locations. This not only improves security by isolating data but also enhances availability and performance as the workload is spread across different systems. Data loss prevention (DLP) techniques are used to prevent unauthorized access and transmission of sensitive data. However, DLP primarily focuses on protecting data from being leaked rather than improving availability. Data masking involves hiding or obfuscating data to protect sensitive information, which is crucial for data security but does not directly contribute to availability. Data aggregation refers to the process of collecting and summarizing data, useful for analysis and reporting but not directly linked to improving security and availability.

2. B — Data Leakage
Answer: Data Leakage Improper disposal of cloud resources can lead to the exposure of sensitive information if the data is not properly wiped before disposal. Cloud Service Providers (CSPs) are responsible for ensuring that media is sanitized properly at the end of its lifecycle. However, clients should also implement their own measures by encrypting data to ensure that any remaining data on disposed media remains unreadable. This is crucial because any mishandling can lead to significant security breaches, compliance issues, and loss of reputation. Other potential threats include: Threat Description Unauthorized Access Cloud customers should implement access controls to prevent unauthorized users from accessing data. Data Corruption Data stored in the cloud can be corrupted by various factors including human error, software bugs, or malicious attacks. Malware Ransomware and other malware increasingly target cloud environments, making anti-malware solutions essential.

3. D — Enforcement
Answer: Enforcement Cloud Access Security Brokers (CASBs) are security policy enforcement points that sit between cloud service consumers and cloud service providers to enforce security, compliance, and governance policies. In general, CASB solutions consist of three components: Phase Description Discovery In this phase, the CASB identifies and classifies sensitive data and resources that require protection in the cloud. Monitoring The CASB continuously monitors cloud activities to detect any anomalies or potential threats, such as unauthorized access or data leaks. Enforcement Upon detecting a violation or threat, the CASB enforces security policies by generating alerts, blocking activity, or taking other appropriate actions. Mapping is not a phase of the CASB process.

4. C — Cloud Access Security Broker (CASB)
Answer: Cloud Access Security Broker (CASB) A Cloud Access Security Broker (CASB) is a security policy enforcement point placed between cloud service users and cloud applications to monitor and enforce data security policies. CASBs provide visibility, data security, threat protection, and compliance. Multi-Factor Authentication (MFA) is a security enhancement that requires users to present multiple pieces of evidence (credentials) before being granted access to a system, but it doesn't monitor or restrict access to data. Virtual Private Network (VPN) creates a secure channel over the internet for data transmission, ensuring data privacy

during transit but does not proactively monitor or control access to data. Encryption ensures data privacy by converting it into a secure format that can only be read by authorized users, but it doesn't control or monitor who accesses the data once decrypted.

5. B — Volume
Answer: Volume Cloud-based infrastructure can use different forms of storage, including: Storage Type Description Ephemeral Acts like RAM, intended for short-term storage that is deleted when an instance is terminated. Long-Term Designed for long-term data storage with durability and integrity protections (e.g., Amazon Glacier). Raw Provides direct access to underlying storage of the server rather than a managed storage service. Volume Behaves like a physical hard drive connected to a virtual machine, can be file or block storage. Object Stores data as objects with unique identifiers and associated metadata, usually for unstructured data.

6. C — Planning
Correct answer: Planning Security should be a primary consideration during the planning phase of migrating to a cloud environment. Addressing security at this stage ensures that security protocols and measures are integrated into the overall migration plan from the beginning, thereby avoiding potential vulnerabilities and the need for costly adjustments later on. Security remains an ongoing concern during deployment, post-migration review, and optimization phases, but the foundational decisions should be made upfront in the planning phase.

7. A — Chain of custody
The correct answer is chain of custody. The chain of custody is crucial in maintaining the integrity and reliability of evidence or items of importance. It ensures that the evidence is handled, stored, and transferred in a secure and accountable manner, enabling confidence in its authenticity and validity for legal or investigatory purposes. Due diligence is a comprehensive and systematic process of research, investigation, and analysis conducted by individuals, organizations, or entities to assess and evaluate potential risks and implications associated with a specific transaction, investment, or business relationship. Due care refers to the level of caution, prudence, and diligence that a reasonable person or organization exercises to prevent harm or minimize risks. Data masking is the process of hiding original data with modified content (characters or other data). The purpose is to protect sensitive data while enabling aggregates, snapshots, and results of applications to be shared with others.

8. B — Authentication
Answer: Authentication Within the realm of cloud computing, IAM involves ensuring that only authorized users can authenticate and access resources. This often includes methods such as passwords, multi-factor authentication, and biometrics. Data Encryption concerns encrypting data at rest or in transit, Network Segmentation involves dividing a network into subnets for improved security, and Threat Detection focuses on identifying potential security breaches.

9. A — Separation of system and user functionality
Answer: Separation of system and user functionality Separating system and user functions ensures that operational data and configurations are protected from unauthorized or accidental changes by administrators. This is a key security practice known as separation of duty. Security function isolation involves isolating security mechanisms to limit their exposure but does not specifically prevent administrators from making changes. Boundary protection includes setting up firewalls or network security measures at the edge of a network or subnet but does not control internal administrative functions. Denial of Service (DoS) protection

aims to prevent or mitigate DoS attacks using firewalls, Intrusion Prevention Systems (IPS), or other technologies but does not relate to administrative control over data and settings.

10. D — Access Enforcement
Answer: Access Enforcement NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations defines numerous security controls for access control. Among these are: - **Access Enforcement**: Controls that enforce access restrictions based on organizational policies, such as multi-factor authentication and account lockout settings. - **Separation of Duties**: Ensures that no single individual has complete control over all aspects of any critical function or system. - **Least Privilege**: Grants users only the permissions they need to perform their jobs, reducing exposure to potential breaches. - **Auditable Events**: Ensures that security-relevant events are recorded and can be reviewed to detect and address any unusual activity.

11. B — Cross-site scripting (XSS)
Answer: Cross-site scripting (XSS) Cross-site scripting (XSS) is an attack where malicious scripts are injected into otherwise benign and trusted websites or emails. These scripts can be executed by the browser of any user who views the compromised content, leading to activities like credential theft, hijacking user sessions, or defacing websites. CSRF involves tricking a user into executing unwanted actions on a different site where they are authenticated. For example, transferring funds or changing email addresses. SQL injection is a type of attack that allows an attacker to execute arbitrary SQL code on a database by inserting malicious SQL statements into a vulnerable application's input fields. XEE attacks exploit the XML processing capabilities of a system by embedding external entities in the XML data. This can lead to issues like data theft or denial of service.

12. D — AWS
Answer: AWS Several organizations provide models and frameworks to enhance cloud security understanding: Cloud Security Alliance (CSA): Offers various resources such as the Cloud Control Matrix, which highlights key security concepts and practices. Open Web Application Security Project (OWASP): Focuses on improving web application security by maintaining lists such as the OWASP Top 10 Web Application Security Risks. Sans Institute: Known for its extensive training and certification programs, SANS also maintains essential resources such as the CWE Top 25 Most Dangerous Software Errors. ISO (International Organization for Standardization): Publishes various standards for many areas, including cloud security (e.g., ISO/IEC 27018:2019 for cloud privacy). Amazon Web Services (AWS) is widely recognized for introducing the Shared Responsibility Model. This model delineates the responsibilities between the cloud service provider and its customers regarding security.

13. C — Container Security Scanner
Answer: Container Security Scanner Static Application Security Testing (SAST): SAST tools inspect the source code of an application for vulnerable code patterns. It can be performed early in the software development lifecycle but can’t catch some vulnerabilities, such as those visible only at runtime. Dynamic Application Security Testing (DAST): DAST bombards a running application with anomalous inputs or attempted exploits for known vulnerabilities. It has no knowledge of the application’s internals, so it can miss vulnerabilities. However, it is capable of detecting runtime vulnerabilities and configuration errors (unlike SAST). Interactive Application Security Testing (IAST): IAST places an agent inside an application and monitors its internal state while it is running. This enables it to identify unknown vulnerabilities based on their effects on the application. Container Security Scanner: A Container Security Scanner

identifies vulnerabilities in container images by scanning and analyzing the software components and configurations within the container. This helps ensure that the containerized application's dependencies and setups are secure.

14. B — Requirements
Answer: Requirements The Software Development Lifecycle (SDLC) describes the main phases of software development from initial planning to end-of-life. While definitions of the phases differ, one commonly-used description includes these phases: Phase Description Requirements During the requirements phase, the team identifies the software's role and the applicable requirements. This includes business, functional, and security requirements. Design During this phase, the team creates a plan for the software that fulfills the previously identified requirements. Test cases may also be developed during this phase to verify the software against requirements. Development This phase is when the software is written. Unit testing should be performed regularly through the development phase to verify that individual components meet requirements. Testing After the software has been built, it undergoes more extensive testing to ensure that it fulfills all of the software’s requirements. Deployment During the deployment phase, the software moves from development to release and default configurations are defined and reviewed for security. Operations and Maintenance (O&M) The O&M phase covers the software from release to end-of-life. The software should undergo regular monitoring and testing to ensure that it remains secure and fit for purpose.

15. A — Testing
Answer: Testing The testing phase entails the implementation and rigorous testing of security controls to ensure they function as intended. The planning phase involves identifying security requirements and planning for their incorporation. The deployment phase is when the application is put into use, typically in a production environment. Operations and maintenance involve the ongoing management and patching of security controls to address emerging threats and vulnerabilities.

16. A — Reversibility to retrieve all assets from the initial provider and portability to migrate data seamlessly.
Answer: Reversibility to retrieve all assets from the initial provider and portability to migrate data seamlessly. Reversibility refers to the ability of a cloud customer to retrieve all data, applications, and artifacts from a cloud provider's environment. Portability is the capability of transferring data (or software) from one provider to another without requiring reentry of the data. Interoperability implies using data across different systems. These terms are defined in ISO/IEC 17788.

17. B — Interoperability
Answer: Interoperability Some important cloud considerations have to do with its effects on operations. These include: Availability: The data and applications that an organization hosts in the cloud must be available to provide value to the company. Contracts with cloud providers commonly include service level agreements (SLAs) mandating that the service is available a certain percentage of the time. Resiliency: Resiliency refers to the ability of a system to weather disruptions. Resiliency in the cloud may include the use of redundancy and load balancing to avoid single points of failure. Performance: Cloud contracts also often include SLAs regarding performance. This ensures that the cloud-based services can maintain an acceptable level of operations even under heavy load. Maintenance and Versioning: Maintenance and versioning help to manage the process of changing software and other systems. Updates should only be made via clear, well-defined processes. Reversibility: Reversibility refers to the ability to recover from a change that went wrong. For example, how difficult it is to restore on-site operations after a transition to an outsourced service (like a cloud

provider). Portability: Different cloud providers have different infrastructures and may do things in different ways. If an organization's cloud environment relies too much on a provider's unique implementation or the provider doesn't offer easy export, the company may be stuck with that provider due to vendor lock-in. Interoperability: When integrating cloud-based applications with on-premises systems, it is important to ensure that these platforms and the applications hosted on them are capable of interoperating. Outsourcing: Using cloud environments requires handing over control of a portion of an organization's infrastructure to a third party, which introduces operational and security concerns.

18. C — Lightweight Directory Access Protocol (LDAP)
Correct answer: Lightweight Directory Access Protocol (LDAP) Lightweight Directory Access Protocol (LDAP) is a widely adopted protocol for accessing and managing directory services, which helps to store and organize information about users, groups, devices, and other resources in a hierarchical structure. LDAP can be used as a foundational protocol for cloud-based directory services, allowing organizations to maintain user accounts, groups, and other directory-related information seamlessly. This supports scalability, centralized management, and cross-cloud region availability. Security Assertion Markup Language (SAML) facilitates Single Sign-On (SSO) by enabling the secure exchange of authentication and authorization data between entities. Although important for IAM, it is not typically used within data centers, making LDAP a more suitable choice. Domain Name Service (DNS) translates domain names into IP addresses, operating similarly to a distributed directory service. However, DNS is not designed for IAM. Dynamic Host Configuration Protocol (DHCP) automatically assigns IP addresses and network configurations within local networks. Though useful for network administration, it does not pertain to IAM.

19. D — Portability
Answer: Portability Portability is defined in ISO/IEC 17788 as the "ability to easily transfer data and applications from one cloud service provider to another without requiring significant changes or modification." This is crucial for minimizing vendor lock-in. Interoperability, as defined in ISO/IEC 17788, is the "ability of different systems or applications to communicate and exchange data effectively." While important, it is not directly related to moving applications between providers. Reversibility refers to the "process allowing cloud service customers to retrieve their data and application artifacts, in order to move away from the cloud service provider." Availability is the "property that ensures cloud services are accessible and usable upon demand by authorized entities."

20. D — Ensuring data integrity and security
Answer: Ensuring data integrity and security When migrating applications to an IaaS provider, it is crucial to ensure that the data's integrity and security are preserved. Any compromise on these aspects can lead to data breaches, loss of sensitive information, and potential compliance issues. While cost-efficiency, vendor reputation, and service level agreements are also important, the priority should be on maintaining the integrity and security of the data being transferred to the cloud.

21. A — Common Vulnerability Scoring System
Answer: Common Vulnerability Scoring System The Common Vulnerability Scoring System (CVSS) is a standardized framework used to assess and communicate the severity of security vulnerabilities in computer systems and software. The purpose of CVSS is to provide a consistent and objective way to evaluate the potential impact and exploitability of vulnerabilities, enabling organizations to prioritize their response and allocate resources effectively. The National Vulnerability Database (NVD) is a comprehensive repository of information about known vulnerabilities and security issues in software and hardware products. It is

maintained by the National Institute of Standards and Technology (NIST) in the United States and serves as a central resource for vulnerability management, risk assessment, and cybersecurity research. Common Weakness Enumeration (CWE) is a community-developed list of common software weaknesses and vulnerabilities. It provides a standardized language and taxonomy for describing and categorizing software security weaknesses that can be found in various stages of the software development lifecycle. CWE is maintained by MITRE Corporation (CWE.MITREdotorg). Common Vulnerabilities and Exposures (CVE) is a community-driven dictionary of publicly known information security vulnerabilities and exposures. It provides a standardized naming scheme and unique identifiers for known vulnerabilities, making it easier for organizations and security professionals to track and manage security risks.

22. D — Cloud Intrusion Detection System (CIDS)
Answer: Cloud Intrusion Detection System (CIDS) A CIDS is a cloud intrusion detection system. It will capture and analyze network traffic and events in the cloud to detect potential attacks or unauthorized access attempts. This makes it the tool likely generating the alerts Marie is reviewing. A CIPS would focus on preventing these attempts, not just detecting them. A FIM monitors changes on file systems and is less likely to be used for detecting unauthorized access at the cloud infrastructure level. Host-based anti-malware is designed to detect and prevent malicious activities at the endpoint level, not specifically cloud infrastructure.

23. C — Load balancing
Correct: Load balancing A load balancer distributes incoming application requests across multiple instances to ensure no single instance is overwhelmed, thereby improving response times and availability. This setup helps in improving performance and providing fault tolerance. In this scenario, Maya is setting up load balancing, which is crucial for directing traffic efficiently across different instances. By implementing load balancing, the PaaS environment can handle increased traffic, effectively manage resources, and deliver better service availability. The focus of the question is on distributing application requests dynamically, which is a characteristic of load balancing.

24. C — Regulatory Authorities
Answer: Regulatory Authorities Cloud Service Providers (CSPs) are likely to have SLAs or formal contracts with clients, suppliers, and partners to ensure service quality, availability, and support. However, CSPs rarely have such agreements with regulatory authorities. Regulatory bodies enforce compliance and conduct audits but do not typically engage in contractual relationships with CSPs. Clients will generally have SLAs defining the terms of service and support, while suppliers provide the necessary infrastructure and hardware, bound by detailed contracts. Partners, who may offer additional services or joint solutions, also engage in similar formal agreements. In contrast, regulatory authorities oversee the legal and compliance aspects without necessitating formal contracts, putting the onus on CSPs and clients to adhere to regulations.

25. B — Detection and analysis, containment, eradication and recovery, post-incident activities
Answer: Detection and analysis, containment, eradication and recovery, post-incident activities When planning for an incident response in the cloud, consider the following aspects: Aspect Explanation **Detection and analysis** Identify incidents as quickly as possible using automated tools, and perform a detailed analysis to understand the scope and impact. **Containment** Implement measures to limit further damage and isolate affected systems to prevent the spread of the incident. **Eradication and recovery** Remove the root cause of the incident and restore affected systems to normal operation, ensuring all vulnerabilities are addressed. **Post-incident activities** Review and analyze the incident to improve future incident response efforts, including debriefing the response team and updating procedures. Labeling would involve tagging certain

aspects but is not a critical need that needs to be addressed in incident response plans. Maximum Tolerable Downtime (MTD) pertains to business continuity rather than incident response. Financial audit data can be part of the system data to be secured but is not directly related to incident response strategies.

26. A — Clients
Answer: Clients A Cloud Service Provider's (CSP's) communications strategy must include transparency with their clients. This involves informing clients of any planned or unplanned service interruptions and actions taken to mitigate these issues. This is crucial for maintaining trust and protecting the CSP's reputation. Other entities like Managed Service Providers, Hardware Suppliers, and Compliance Auditors have important roles but are less likely to be primary recipients of service degradation notifications.

27. C — Publicly traded companies
Correct answer: Publicly traded companies. The Sarbanes-Oxley Act (SOX) governs the financial practices and reporting of publicly traded companies to protect investors from fraudulent accounting activities. It does not specifically apply to health care providers, financial institutions only, or non-profit organizations. The collection and storing of protected health information is governed by the Health Insurance Portability and Accountability Act (HIPAA). Financial institutions are regulated under various other laws like the Gramm-Leach-Bliley Act (GLBA). Non-profit organizations adhere to other compliance regulations depending on their activities and geographical locations.

28. A — Health Insurance Portability and Accountability Act (HIPAA)
Answer: Health Insurance Portability and Accountability Act (HIPAA) HIPAA regulates the protection of Protected Health Information (PHI) and sets standards for its privacy and security. Cloud providers working with healthcare clients must comply with HIPAA to ensure the confidentiality, integrity, and availability of PHI. The Sarbanes-Oxley Act (SOX) is concerned with financial and accounting data, not healthcare data. The Gramm-Leach-Bliley Act (GLBA) governs the disclosure of personal information by financial institutions, but it does not directly address healthcare data. Asia Pacific Economic Cooperation (APEC) is an international agreement that promotes free trade and the handling of personal data but does not specifically address healthcare data.

29. D — Data Processor
Answer: Data Processor There are several roles and responsibilities related to data ownership, including: Data Owner: The data owner creates or collects the data and is responsible for it. Data Custodian: A data custodian is responsible for maintaining or administrating the data. This includes securing the data based on instructions from the data owner. Data Steward: The data steward ensures that the data’s context and meaning are understood and that it is used properly. Data Processor: A data processor uses the data, including manipulating, storing, or moving it. Hospital IT departments typically act as data processors.

30. C — General Data Protection Regulation (GDPR), European Union
Answer: General Data Protection Regulation (GDPR), European Union The General Data Protection Regulation (GDPR) is a comprehensive data protection law that applies to all organizations processing personal data of EU residents. It ensures the privacy and protection of personal data. The California Consumer Privacy Act (CCPA) is a state statute intended to enhance privacy rights and consumer protection for residents of California, USA. Personal Information Protection and Electronic Documents Act (PIPEDA) encompasses data privacy for Canadian businesses and residents. Data Protection Act 2018 (DPA 2018) updates and enforces data protection laws in the UK, aligning closely with GDPR principles.

Ready to pass?

Unlock the full CCSP Cloud Security Prep bank, every explanation, and unlimited timed mock exams.

Scan to start practising
https://certs.theorypractice.app/ccsp

Watch the full video walkthrough on YouTube @CertsQuizPrep