CCSK v5 Sample Questions

Check your knowledge before taking the exam

Domain 1: Cloud Computing Concepts & Architectures

Q1: Which of the following accurately defines the primary responsibility difference for IaaS, PaaS, and SaaS?

- In PaaS, the user manages the hardware and network infrastructure
- In SaaS, the user is responsible for managing and updating the application itself
- **In IaaS, the user manages applications, data, runtime, and OS**
- In IaaS, the provider manages both the infrastructure and applications

Justification: *In the IaaS model, infrastructure management primarily lies with the user, except for the underlying hardware.*

Q2: What does ISO/IEC 22123-1:2023 define cloud computing as?

- **A scalable and elastic pool of shareable resources**
- A static and local set of dedicated resources
- A fixed and isolated pool of private resources
- A static and flexible collection of isolated resources

Justification: *This definition specifically highlights scalability, elasticity, and resource sharing, which are fundamental aspects of cloud computing as defined by ISO/IEC 22123-1:2023.*

Q3: Which characteristic of cloud computing can potentially increase security risks when compared to traditional on-premises infrastructure?

- Elasticity
- Broad network access
- Resource pooling
- **Multi-tenancy**

Justification: *Multi-tenancy allows multiple users to share the same physical resources, increasing the attack surface and potential for data leaks between tenants.*

Q4: Which of the following best describes the composition of a cloud computing resource?

- **It can include processors, memory, networks, databases, and applications**
- It is limited to only raw infrastructure components like processors and memory
- It solely comprises high-level software resources such as databases and applications
- It consists primarily of physical servers and storage devices

Justification: *Cloud computing resources are flexible and cover a range of components, not limited to just hardware or software.*

Q5: What is the main purpose of abstraction in virtualization?

- Improving encryption protocols for data
- **Creating virtual machines from physical servers**
- Optimizing application software performance
- Increasing physical server storage capacity

Justification: *Abstraction in virtualization simplifies hardware resources into virtualized components.*

Domain 2: Cloud Governance

Q6: What is involved in CSA STAR Attestation?

- Independent audits by third-party firms
- Automated compliance tools
- **Self-assessments against CSA CCM**
- Penetration testing

Justification: *CSA STAR Attestation includes self-assessments conducted using the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM).*

Q7: Why are policies important in a cybersecurity framework?

- They provide a detailed implementation plan for security controls
- They serve as a reference for legal compliances
- They outline technical standards for system architectures
- **They translate guidelines into actionable security requirements**

Justification: *Policies ensure that the high-level guidelines are enforceable and actionable.*

Q8: How does enterprise governance align IT capabilities with business objectives?

- **By ensuring IT initiatives support overall business strategy**
- By centralizing all IT decisions within the IT department
- By isolating IT from business processes to maintain security
- By focusing exclusively on technical efficiency

Justification: *Enterprise governance ensures that IT efforts contribute to the main goals and strategic direction of the organization.*

Q9: What is a key component for ensuring effective cloud governance?

- Using multiple cloud service providers
- Reducing cloud service costs
- **Implementing strong frameworks and policies**
- Focusing solely on compliance

Justification: *Strong frameworks and policies form the foundation of effective cloud governance, as they provide structure and guidelines.*

Domain 3: Risk, Audit & Compliance

Q10: Which risk treatment strategy involves taking proactive steps to reduce the impact or likelihood of a risk?

- Transfer
- **Mitigation**
- Avoid
- Accept

Justification: *Mitigation involves developing actions to reduce the impact or likelihood of a risk.*

Q11: Which of the following actions is most effective in establishing a robust cloud risk profile for your organization?

- Rely solely on vendor certifications and assurances
- Deploy an extensive set of firewall rules
- **Conduct regular risk assessments and security audits**
- Adopt a one-time compliance assessment approach

Justification: *Regular risk assessments and security audits help identify potential risks and vulnerabilities continuously, enabling proactive risk management.*

Q12: Which step in the assessment process involves analyzing the cloud service provider's policies and reports?

- **Review CSP documentation**
- Business requests
- Map to data classification
- Define required and compensating controls

Justification: *This step involves analyzing the cloud service provider's policies and reports to ensure they meet contractual and regulatory requirements.*

Q13: What is a primary reason that effective cloud risk management is critical for an organization?

- To reduce the cost of cloud services
- To enhance employee productivity
- To eliminate the need for internal IT staff
- **To mitigate potential data breaches and ensure regulatory compliance**

Justification: *Effective cloud risk management helps protect sensitive data and ensures the organization adheres to relevant laws and regulations.*

Q14: Which of the following best mitigates the risk of an unauthorized access incident in a cloud environment?

- Relying solely on strong passwords
- **Implementing multi-factor authentication (MFA)**
- Encrypting data at rest
- Regularly updating software

Justification: *MFA requires multiple forms of verification to access an account, which significantly reduces the risk of unauthorized access.*

Domain 4: Organization Management

Q15: What is the primary purpose of implementing centralized logging in a shared security services model?

- **To enable comprehensive monitoring and quick identification of security incidents**
- To reduce the overall cost of log storage
- To improve user authentication processes
- To simplify the deployment of applications

Justification: *Centralized logging gathers logs from various sources to facilitate monitoring and quick incident response.*

Q16: Which tool is best suited for ensuring secure API traffic in a SaaS environment?

- Federated Identity Brokers
- CASBs (Cloud Access Security Brokers)
- **API Gateways**
- IAM (Identity and Access Management)

Justification: *API Gateways act as a management tool that controls the way applications use APIs, ensuring secure API traffic handling.*

Q17: Which of the following is a core security capability provided by Cloud Service Providers (CSPs) to help manage access and permissions?

- Logging and Monitoring
- **IAM (Identity and Access Management)**
- Encryption-at-Rest
- DDoS Protection

Justification: *IAM is a critical security capability that helps manage user identities and their access to resources within the cloud environment.*

Q18: How do organization-level security controls differ from controls in individual deployments?

- They provide granular control for specific applications
- They focus solely on physical security measures
- They are less important compared to individual deployment controls
- **They establish overarching policies and controls for the entire organization**

Justification: *Organization-level security covers broad policies that affect all departments to ensure a standardized security posture.*

Q19: What is the scope level at which policies can be applied within an organization?

- **Organization-wide, group-level, or deployment-level**
- Department-level, project-level, or team-level
- Region-level, unit-level, or task-level
- Enterprise-level, section-level, or role-level

Justification: *The policies can indeed be applied at an organization-wide, group-level, or deployment-level, ensuring flexibility in policy management.*

Domain 5: Identity and Access Management

Q20: Which statement best describes Policy-Based Access Control (PBAC)?

- PBAC grants access based on user roles without any policy document
- **PBAC defines extensive access requirements in a policy document**
- PBAC relies on multi-factor authentication for resource access
- PBAC is a type of encryption algorithm used to secure data

Justification: *PBAC specifies access policies in documents, detailing the conditions under which resources can be accessed.*

Q21: Which of the following is considered a soft token in Multi-Factor Authentication (MFA)?

- A physical USB device that generates a random code
- An SMS message with a one-time password sent to a registered phone
- A fingerprint scan used to unlock a secure application
- **A smartphone app generating a time-based one-time password (TOTP)**

Justification: *Soft tokens are usually software-based and can be implemented as apps on smartphones generating TOTPs.*

Q22: Why is Identity and Access Management (IAM) considered the new perimeter in cloud-native security environments?

- **IAM ensures secure access to resources in a decentralized and dynamic cloud environment**
- IAM is used solely for user authentication in on-premises environments

- IAM replaces traditional network perimeter defenses entirely
- IAM is only relevant for managing large cloud infrastructure

Justification: *IAM controls who has access to what, ensuring that only authorized users can interact with resources, which is crucial in a cloud-native environment.*

Q23: What is the primary benefit of implementing IAM between organizations and cloud providers?

- Increased physical security of data centers
- Reduced need for encryption
- **Centralized access control and management**
- Enhanced performance of cloud services

Justification: *Centralized IAM allows organizations to maintain control over access policies and manage identities efficiently across various platforms.*

Q24: Which primary principle does Attribute-Based Access Control (ABAC) utilize to grant access?

- **Uses specific attributes like user role, environment, and resource**
- Uses the username and password only
- Grants access based on IP address
- Uses predefined group policies

Justification: *ABAC makes decisions based on various attributes like user role, environment conditions, and resources for access control.*

Domain 6: Security Monitoring

Q25: What does Cascading Log Architecture involve in the context of log management?

- Distributed log storage
- Log replication
- **Hierarchical log management**
- Dynamic log partitioning

Justification: *Cascading Log Architecture is designed to streamline and organize logs hierarchically.*

Q26: Why is centralization of logs and configuration crucial for distribution and segregation?

- It reduces the load on server hardware
- **It ensures consistent monitoring and quick detection of anomalies**
- It improves the physical security of data centers
- It eliminates the need for regular security audits

Justification: *Centralization allows for uniform monitoring, making detection and response to anomalies more efficient.*

Q27: Which of the following best describes the primary purpose of Cloud Security Posture Management (CSPM)?

- Managing cloud service subscriptions
- Optimizing cloud service performance
- Providing cloud cost management solutions
- **Continuous monitoring and assessing cloud security**

Justification: *CSPM is designed to continuously monitor and assess cloud security to identify and rectify vulnerabilities.*

Q28: Which type of log contains activities from console, API, or CLI access?

- Data Plane Logs
- Application Logs
- **Management Plane Logs**
- Security Logs

Justification: *Management Plane Logs monitor activities initiated through console, API, or CLI access.*

Q29: Which primary function of logs is vital for ensuring comprehensive monitoring and debugging of system activities?

- Optimizing system performance
- **Providing detailed records of all system activities**
- Blocking unauthorized access attempts
- Automating routine maintenance tasks

Justification: *Logs record every system activity, offering comprehensive monitoring and debugging capabilities.*

Domain 7: Infrastructure & Networking

Q30: Which technology improves security posture by assuming network traffic is untrusted until identity verification?

- **Zero Trust Network Access (ZTNA)**
- Secure Sockets Layer (SSL)
- Virtual Private Network (VPN)
- Firewall

Justification: *ZTNA operates on the principle that no user or device is trusted until proven otherwise, enhancing security by requiring identity verification before granting access.*

Domain 8: Cloud Workload Security

Q31: Which section of a report would you typically find credit given to lead authors and contributors?

- Cloud Workload Security
- Detailed Contents
- Reviewers
- **Acknowledgments**

Justification: *Acknowledgments are typically where credit is given to lead authors, contributors, and reviewers.*

Q32: What is a key practice in securing container orchestration systems?

- **Regularly applying patches and updates**
- Disabling unused ports
- Ignoring CSP tools
- Avoiding security policy implementation

Justification: *Keeping software up-to-date is crucial for mitigating vulnerabilities and ensuring system security.*

Q33: Which principle should be prioritized when managing IAM for serverless applications to minimize security risks?

- Broad permissions
- Static roles

- **Least privilege access**
- Manual access control

Justification: *Least privilege access ensures users and applications only have permissions necessary for their tasks, minimizing potential abuse.*

Q34: Why is the cloud preferred for AI workloads?

- Cloud is more secure for AI workloads
- Cloud reduces the cost of hardware
- Cloud services are always faster
- **Cloud enables dynamic scaling for data and computational needs**

Justification: *AI requires extensive data processing and computing power, both of which are efficiently handled by cloud's dynamic scaling capabilities.*

Domain 9: Data Security

Q35: Which function of Data Loss Prevention (DLP) tools helps secure sensitive data in the cloud?

- **Monitoring and protecting data**
- Encrypting all network traffic
- Managing user access controls
- Blocking all unauthorized websites

Justification: *DLP tools aim to identify, monitor, and protect sensitive data, including in cloud environments.*

Q36: Which method provides security for specific data items by encrypting data at the application layer?

- Network level encryption
- **Application level encryption**
- File system encryption
- Database encryption

Justification: *Application level encryption secures specific data items at the application layer, enhancing data confidentiality.*

Q37: What is one of the main advantages of using non-relational databases (NoSQL) over traditional relational databases?

- Enhanced ACID transaction support for all operations
- **Highly scalable and flexible data storage formats**
- Data is strictly structured in tables and rows
- Better suitability for small-scale applications

Justification: *Non-relational databases (NoSQL) are designed to scale horizontally and accommodate various data formats.*

Q38: Which of the following is NOT a common component of PaaS storage?

- Logging services
- Message queues
- In-memory databases
- **Firewall rules setup**

Justification: *Firewall rules setup is related to security configurations and networking, not storage services in PaaS.*

Q39: Why is data security imperative for an organization?

- **It ensures organizational integrity, confidentiality, customer trust, and regulatory compliance**
- It mainly helps in software development and deployment
- Data security primarily aims to enhance user interfaces
- It prevents internal communication failures

Justification: *The core aspects of data security are essential for maintaining the trust and legal standing of an organization.*

Domain 10: Application Security

Q40: What is a key consideration when managing security in a cloud environment with the shared responsibility model?

- Client-controlled physical hardware must be isolated
- User authentication settings are exclusively client responsibility
- **Provider-controlled libraries must be monitored and audited**
- Network encryption is solely the client's responsibility

Justification: *Ensuring security requires attention to components managed by the provider to prevent vulnerabilities.*

Q41: Which of the following best describes the importance of understanding infrastructure vulnerabilities in scalable applications?

- **To ensure that security measures can handle increased load and complexity**
- To minimize the costs associated with infrastructure upgrades
- To streamline the deployment process regardless of security
- To reduce the number of required compliance audits

Justification: *Understanding vulnerabilities helps in adapting security measures to support application scalability efficiently.*

Q42: Which of the following is crucial for ensuring application security in a cloud computing environment?

- Lowering network latency
- Implementing redundant power supplies
- Prioritizing bandwidth allocation
- **Implementing robust access controls**

Justification: *Robust access controls are essential to secure sensitive data and enforce user authentication in cloud environments.*

Q43: What is a crucial phase in application security that involves addressing vulnerabilities from early design to maintaining live applications?

- Only during initial development
- **All stages from early design to live maintenance**
- Only during testing phase
- Only during post-deployment maintenance

Justification: *Application security must be integrated from the initial design phase through continuous maintenance to ensure comprehensive protection.*

Q44: How can DevOps introduce risk, but also benefit application security?

- DevOps reduces the need for security testing
- DevOps focuses solely on automating deployment processes
- **Faster deployment cycles can improve response times but may introduce untested code**
- DevOps practices inherently guarantee secure applications

Justification: *DevOps enables rapid deployment, which helps respond quickly to threats but may unintentionally introduce vulnerabilities.*

Domain 11: Incident Response & Resilience

Q45: When establishing a cloud incident response program, what access do responders need to to effectively analyze incidents?

- **Persistent read access and controlled write access for critical situations**
- Unlimited write access for all responders at all times
- Full-read access without any approval process
- Access limited to log events for incident analysis

Justification: *It is essential for cloud incident response teams to have persistent read access to all deployments to review resources and configurations involved in an incident.*

Domain 12: Related Technologies & Strategies

Q46: In the context of securing a PaaS model, which of the following is the most critical security control to implement?

- Securing the hardware
- **Securing user access**
- Updating software frequently
- Implementing firewalls

Justification: *User access controls ensure that only authorized individuals can interact with sensitive components of the PaaS, mitigating risks of unauthorized access.*

Q47: Which approach improves consistency and simplification in managing access control across multiple access requests?

- Using multiple access control policies for each request
- Granting administrative privileges by default
- **Implementing unified access control models**
- Applying access control only to sensitive data

Justification: *Unified access control models provide a consistent framework, reducing complexity and enhancing manageability.*

Q48: According to the CISA ZT Maturity Model, what is the highest level of maturity an organization can achieve?

- Advanced
- Initial
- Traditional
- **Optimal**

Justification: *The Optimal stage is the highest in the CISA ZT Maturity Model, indicating complete integration and optimization.*

Q49: Which feature is characteristic of an optimal security stage in automation maturity?

- Manual oversight with automated alerts
- **Fully automated and adaptive functions**
- Semi-automated processes with manual intervention
- Static rule-based automation

Justification: *An optimal stage in automation maturity involves systems that can fully automate processes and adapt to new threats or changes dynamically.*

Q50: Which strategy is crucial to minimizing security risks by ensuring users only have access necessary for their job functions?

- Continuous authentication
- Implemented firewalls
- **Enforcing least privilege principles**
- Strict access controls

Justification: *Least privilege limits user access strictly to what is required, reducing potential misuse or breaches.*