Download WGU Managing-Cloud-Security Exam Dumps Free

Shared by Holmes on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An organization that primarily uses a remote work model is reviewing the documentation of various insurance providers to become eligible for cybersecurity insurance. Competitive insurance providers require the organization to implement security controls to ensure only authorized personnel can access the network, data, emails, and other administrative information. Which commonly required control should the organization implement before applying for cybersecurity insurance from these competitive insurance providers?

Options:

A- Network segmentation
B- Application whitelisting
C- Multifactor authentication (MFA)
D- Trusted platform module (TPM)

Answer:

C

Explanation:

Multifactor Authentication (MFA) is a commonly mandated control for obtaining cybersecurity insurance. MFA requires users to present at least two independent factors---something they know (password), something they have (token), or something they are (biometrics). This significantly reduces the risk of unauthorized access due to stolen or weak credentials.

Network segmentation and application whitelisting are valuable, but they are not universal insurance requirements. TPM is a hardware component for securing local devices but does not protect remote access in distributed work models.

By enforcing MFA across VPNs, cloud services, email, and administrative interfaces, organizations demonstrate strong access control measures. Insurance providers recognize MFA as a foundational safeguard, reducing claims risk from credential-based breaches. This makes MFA both a compliance requirement and a best practice.

Question 2

Question Type: MultipleChoice

Which privacy issue does the Clarifying Lawful Overseas Use of Data (CLOUD) Act address?

Options:

A- Conflicting regulations in different jurisdictions
B- Collection and use of genetic information
C- Data breach notification requirements
D- Use of digital surveillance by multinational employers

Answer:

A

Explanation:

The CLOUD Act addresses conflicts that arise when law enforcement in one jurisdiction seeks access to data stored in another country. It clarifies how U.S. authorities can compel cloud providers to produce data, even if stored overseas, and establishes a framework for resolving jurisdictional conflicts through bilateral agreements.

The Act does not regulate genetic data, breach notifications, or employer surveillance. Its central purpose is to handle the challenge of cross-border data access in the era of globalized cloud computing.

For organizations, this means carefully evaluating how and where data is stored, and ensuring contracts and compliance strategies account for potential conflicts between U.S. law and foreign privacy regulations like GDPR. Awareness of CLOUD Act obligations is crucial in multinational cloud deployments.

Question 3

Question Type: MultipleChoice

An organization is reviewing a contract from a cloud service provider and wants to ensure that all aspects of the contract are adhered to by the cloud service provider. Which control will allow the organization to verify that the cloud provider is meeting its obligations?

Options:

A- Continuous monitoring
B- Confidential computing
C- Regulatory oversight
D- Incident management

Answer:

A

Explanation:

Continuous monitoring is the control that allows organizations to actively verify that a cloud provider is fulfilling contractual and compliance obligations. This involves automated collection and analysis of operational, security, and performance data. It enables organizations to ensure that service-level agreements (SLAs) are being honored and that compliance requirements are being met in real time.

While regulatory oversight is provided by external authorities and incident management is reactive in nature, continuous monitoring is a proactive approach. It allows customers to maintain visibility into provider operations. Confidential computing focuses on data protection but does not verify contract adherence.

By employing continuous monitoring, organizations establish transparency and accountability. It also supports audit processes by providing evidence that controls remain effective over time. This reduces risk associated with outsourcing critical functions to a cloud provider and ensures resilience against potential provider-side failures.

Question 4

Question Type: MultipleChoice

Which testing standard is currently used to guide Service Organization Control (SOC) audits outside the United States?

Options:

A- The Statement on Standards for Attestation Engagements (SSAE) 18
B- The International Standard on Review Engagements (ISRE) 2400
C- The Statement on Standards for Accounting and Review Services (SSARS) 25
D- The International Standard on Assurance Engagements (ISAE) 3402

Answer:

D

Explanation:

Outside the United States, ISAE 3402 (International Standard on Assurance Engagements 3402) is the standard used for audits equivalent to SOC reports. It ensures that service organizations demonstrate adequate internal controls over financial reporting and operational processes.

SSAE 18 is the U.S. standard governing SOC audits. ISRE 2400 and SSARS 25 focus on accounting and review services, not assurance over service organizations.

ISAE 3402 provides assurance to international customers that cloud providers or service organizations meet rigorous standards for security, availability, processing integrity, confidentiality, and privacy. This builds global trust and interoperability in compliance frameworks.

Question 5

Question Type: MultipleChoice

An organization is sharing personal information that is defined in its privacy policy with a trusted third party. What else should the organization communicate to the trusted third party about the personal information?

Options:

A- The results of the organization's most recent privacy audit
B- A notice of any contractual obligations that do not align with the privacy policy
C- A copy of federal privacy laws regarding unauthorized data disclosure
D- The organization's privacy policy and handling practices

Answer:

D

Explanation:

When sharing personal data with a trusted third party, organizations must ensure that the recipient understands and adheres to the organization's privacy policy and handling practices.

This ensures consistent treatment of personal information across entities and aligns with consent provided by individuals.

Audit results and contractual notices are internal matters, while federal laws define obligations but do not substitute for organizational policies. By explicitly sharing policies and practices, organizations reinforce accountability and ensure compliance with privacy regulations such as GDPR, HIPAA, or CCPA.

This communication sets expectations for data use, retention, and disclosure. It also provides a defensible framework in case of regulatory inquiries, showing that due diligence was performed when transferring data to third parties.

Question 6

Question Type: MultipleChoice

Which release management term describes the process from code implementation to code review and approval to automated testing and then to production deployment?

Options:

A- Iteration
B- Baseline
C- Pipeline
D- Framework

Answer:

C

Explanation:

A pipeline refers to the structured process of moving code from development to production, encompassing implementation, review, automated testing, and deployment. In DevOps, this is known as a CI/CD pipeline (Continuous Integration/Continuous Deployment).

An iteration refers to a development cycle, a baseline represents a stable reference configuration, and a framework provides structure but not a deployment sequence. Only pipeline accurately captures the sequential, automated flow of code into production.

Pipelines enhance efficiency, consistency, and quality assurance by automating repetitive tasks, reducing human error, and ensuring that code changes are validated before reaching production.

They are essential for modern cloud-native applications where rapid deployment is expected.

Question 7

Question Type: MultipleChoice

An organization needs to provide space where security administrators can centrally monitor network traffic and events and respond to threats or outages. What should the organization create?

Options:

A- Emergency response team (ERT)
B- Security operations center (SOC)
C- Disaster response team (DRT)
D- Network operations center (NOC)

Answer:

B

Explanation:

A Security Operations Center (SOC) is a centralized facility that allows administrators to monitor, detect, investigate, and respond to cybersecurity events in real time. SOC teams leverage tools such as SIEM (Security Information and Event Management), threat intelligence, and incident response playbooks.

ERTs and DRTs are teams focused on emergencies and disaster recovery, respectively, but they do not provide continuous monitoring. A NOC focuses on performance and availability of IT infrastructure but not on security threats.

By establishing a SOC, organizations ensure 24/7 visibility into security events, coordinated incident handling, and compliance with standards such as ISO 27001 and SOC 2. SOCs are essential in cloud environments where threats evolve rapidly, and centralized expertise is needed to minimize impact.

Question 8

Question Type: MultipleChoice

Which action should a customer take to add an extra layer of protection to the data stored in a public cloud environment?

Options:

A- Use additional encryption for sensitive files and folders
B- Use web application firewalls (WAFs)
C- Use database activity monitoring (DAM)
D- Use block storage instead of file storage

Answer:

A

Explanation:

While cloud providers typically offer built-in encryption, customers should apply additional encryption for sensitive data to maintain defense-in-depth. Encrypting files and folders before uploading them ensures that even if provider-side protections fail, data remains confidential.

WAFs protect applications from web threats, DAM tools monitor database use, and block storage versus file storage is an architecture choice. None of these directly provide an extra protective layer for stored data.

By maintaining control of their encryption keys, customers ensure compliance with data protection standards such as GDPR, HIPAA, or PCI DSS. This practice also mitigates insider threats within the provider's environment and supports secure multi-cloud strategies. Encryption remains the strongest safeguard for protecting sensitive files in public cloud storage.

Question 9

Question Type: MultipleChoice

Which setting ensures that an attacker cannot read the information stored temporarily for use by another virtual machine (VM)?

Options:

A- Encrypted network protocols
B- Encrypted file system
C- Dedicated processor
D- Dedicated memory

Answer:

D

Explanation:

Dedicated memory allocation ensures isolation between virtual machines in a shared environment. Without memory isolation, remnants of one VM's operations might remain in physical memory and be accessible to another VM, leading to cross-tenant data leakage. Assigning dedicated memory prevents attackers from exploiting memory-sharing vulnerabilities.

Encrypted network protocols protect data in transit, not memory. Encrypted file systems safeguard storage, not volatile memory. A dedicated processor helps with performance and isolation of compute tasks but does not secure temporary memory contents.

Cloud environments are multi-tenant, which makes memory isolation a critical safeguard. By dedicating memory or enforcing strict hypervisor-level isolation, providers prevent data exposure between customers. This aligns with best practices for virtualization security and the ''resource pooling'' characteristic of cloud computing, ensuring that shared infrastructure does not compromise confidentiality.

Question 10

Question Type: MultipleChoice

Which U.S. law requires all publicly traded corporations in the United States to provide information about their financial status and implements controls to ensure the accuracy of the disclosed information?

Options:

A- The Gramm-Leach-Bliley Act (GLBA)
B- The General Data Protection Regulation (GDPR)
C- The Sarbanes-Oxley (SOX) Act

D- The Clarifying Lawful Overseas Use of Data (CLOUD) Act

Answer:

C

Explanation:

The Sarbanes-Oxley (SOX) Act of 2002 was enacted to restore investor confidence after major corporate accounting scandals. It requires publicly traded corporations to maintain accurate financial reporting and implement internal controls to safeguard the integrity of disclosed information.

GLBA focuses on protecting consumer financial data, GDPR is a European regulation governing privacy, and the CLOUD Act addresses cross-border law enforcement access to data. Only SOX directly mandates financial disclosure and corporate accountability.

SOX compliance includes maintaining audit trails, securing data integrity, and ensuring that executives certify financial statements. Failure to comply carries severe penalties, both civil and criminal. For cloud environments, SOX compliance extends to ensuring IT systems used for financial data are secure, monitored, and auditable.

Question 11

Question Type: MultipleChoice

An organization's leadership team gathered managers and key team members in each division to help create a disaster recovery plan. They realize they lack a complete understanding of the infrastructure and software needed to formulate the plan. Which action should they take to correct this issue?

Options:

A- They should create a checklist of the necessary tasks.
B- They should determine the criteria of a disaster.
C- They should identify the key roles in a disaster.
D- They should perform an inventory of assets.

Answer:

D

Explanation:

Without a clear understanding of infrastructure and software, the leadership team must first conduct an inventory of assets. An asset inventory provides a comprehensive list of hardware, software, and services that support business operations.

Creating checklists, defining criteria, and assigning roles are important, but they rely on knowing what assets exist. Without an inventory, the disaster recovery plan would miss critical dependencies, making recovery incomplete or impossible.

Performing an inventory supports business impact analysis, risk assessments, and recovery prioritization. It ensures that all critical systems are accounted for and appropriate recovery strategies can be designed. Asset inventories are a foundational best practice for disaster recovery and continuity planning.