Real Managing-Cloud-Security Torrent | PDF Managing-Cloud-Security Cram Exam

P.S. Free & New Managing-Cloud-Security dumps are available on Google Drive shared by itPass4sure: https://drive.google.com/open?id=1oaGsMOxbWFEx2U2YnwBOwB7q-07pHV8j

We pay emphasis on variety of situations and adopt corresponding methods to deal with. More successful cases of passing the Managing-Cloud-Security exam can be found and can prove our powerful strength. As a matter of fact, since the establishment, we have won wonderful feedback and ceaseless business, continuously working on developing our Managing-Cloud-Security Test Prep. We have been specializing Managing-Cloud-Security exam dumps many years and have a great deal of long-term old clients, and we would like to be a reliable cooperator on your learning path and in your further development.

WGU Managing-Cloud-Security Exam Syllabus Topics:

Section	Objectives
Implementing Operational Capabilities, Procedures, and Training	- Security operations workflows • 1. Roles and responsibilities • 2. Security awareness and training
Cloud Security Policies and Procedures	- Cloud application security policies • 1. Data handling standards • 2. Incident response procedures
Risk Analysis and Risk Management	- Business continuity and disaster recovery • 1. Risk mitigation strategies • 2. Threat assessments
Legal, Compliance, and Ethical Concerns	- Compliance and governance • 1. HIPAA • 2. GDPR • 3. SOC 2
Identity and Access Management	- Cloud IAM controls • 1. Privileged access management • 2. Multi-factor authentication

Secure Cloud Service Models	- Cloud architecture security • 1. SaaS security • 2. IaaS security • 3. PaaS security

>> Real Managing-Cloud-Security Torrent <<

Reliable Real Managing-Cloud-Security Torrent & Leading Offer in Qualification Exams & Authorized WGU WGU Managing Cloud Security (JY02)

itPass4sure's web-based WGU Managing-Cloud-Security practice test also contains mock exams just like the desktop practice exam software with some extra features. As this is a web-based software, this is accessible through any browser like Opera, Safari, Chrome, Firefox and MS Edge with a good internet connection. WGU Managing Cloud Security (JY02) (Managing-Cloud-Security) practice test is also customizable so that you can easily set the timings and change the number of questions according to your ease.

WGU Managing Cloud Security (JY02) Sample Questions (Q164-Q169):

NEW QUESTION # 164
A user creates new financial documents that will be stored in the cloud. Which action should the user take before uploading the documents to protect them against threats such as packet capture and on-path attacks?

- A. Hashing
- B. Encryption
- C. Change tracking
- D. Metadata labeling

Answer: B

Explanation:
Before transmitting sensitive financial data to the cloud, the best defense against interception threats like packet capture and man-in-the-middle attacks isencryption. Encryption protects data in transit by converting plain text into cipher text, which can only be deciphered with the correct keys.
Hashing provides integrity verification but does not secure confidentiality. Change tracking monitors modifications but does not prevent interception. Metadata labeling adds context but does not protect against on-path attackers.
Using strong encryption protocols (e.g., TLS) ensures that even if traffic is intercepted, the attacker cannot read the data. Encryption also aligns with compliance requirements such as PCI DSS, which mandates encryption for financial data during transmission. By encrypting before upload, the user ensures end-to-end confidentiality across potentially insecure networks.

NEW QUESTION # 165
Which strategy provides the highest overall cost savings for an organization implementing a business continuity and disaster recovery (BCDR) plan?

- A. Implement cross-site replication.
- B. Deploy a hot cloud site.
- C. Migrate local backups to tape.
- D. Move all services to the cloud.

Answer: D

Explanation:
Moving all services to the cloud provides the highest overall cost savings for organizations implementing BCDR. Managing Cloud guidance explains that cloud-based services reduce capital expenditures, eliminate the need for secondary physical data centers, and leverage on-demand scalability.
Cloud platforms offer built-in redundancy, geographic distribution, and automated recovery capabilities that significantly lower the

cost of maintaining separate disaster recovery infrastructure. Pay-as-you-go pricing ensures organizations only pay for resources when needed, further reducing operational expenses.
Hot sites and cross-site replication incur ongoing costs, while tape backups offer lower cost but do not support rapid recovery. Therefore, migrating services to the cloud delivers the most comprehensive cost savings.

NEW QUESTION # 166
Which description accurately characterizes the movement of applications to the cloud?

- A. In a desktop as a service (DaaS) environment, the customer is responsible for securing the underlying infrastructure.
- B. In a software as a service (SaaS) environment, the CSP is responsible for securing the platform.
- C. In a platform as a service (PaaS) environment, the customer is responsible for securing the underlying infrastructure.
- D. In an infrastructure as a service (IaaS) environment, the CSP is responsible for securing the platform.

Answer: B

Explanation:
In a Software as a Service (SaaS) environment, the cloud service provider (CSP) is responsible for securing the platform. Managing Cloud principles explain that SaaS places the majority of security responsibilities on the provider, including infrastructure, operating systems, middleware, and application security.
Customers primarily manage user access, data usage, and configuration settings, while the provider ensures availability, patching, vulnerability management, and platform protection. This division of responsibility simplifies security management for consumers.
The other options misrepresent shared responsibility boundaries. In IaaS, customers secure the platform, and in PaaS, providers manage infrastructure. Therefore, option D accurately characterizes application movement to the cloud.

NEW QUESTION # 167
A customer requests that a cloud provider physically destroys any drives storing their personal data. What must the provider do with the drives?

- A. It should destroy them only if dedicated hardware disposal is specified in the contract.
- B. It should destroy them only if the contract includes hardware disposal insurance.
- C. It should use cryptographic erasure to securely remove any personal data from the drives.
- D. It should use degaussing tools to securely remove any personal data from the drives.

Answer: A

Explanation:
Cloud providers typically manage multi-tenant infrastructure, where physical hardware is shared among customers. Therefore, drives are not destroyed for each customer unless explicitly required in thecontract. If the customer's agreement specifies dedicated hardware disposal, then the provider must comply by physically destroying the drives.
Cryptographic erasure and degaussing are valid sanitization methods, but they may not meet the specific contractual requirement of physical destruction. Insurance clauses are unrelated to disposal.
This question underscores the importance of negotiating contractual terms in cloud agreements. Customers handling highly sensitive or regulated data may require physical destruction, while others may accept logical erasure. Clear agreements ensure both compliance and alignment of security responsibilities.

NEW QUESTION # 168
A company is interested in tokenization as an alternative to protecting data without encryption. The application will soon store the token. Which step should occur immediately before this action?

- A. The tokenization server generates the token for the application.
- B. Data is sent to the tokenization server.
- C. The tokenization server returns the token to the application.
- D. An authorized application requests the token.

Answer: C

Explanation:
Before an application can store a token, it must first receive the token from the tokenization server.

Managing Cloud guidance outlines that tokenization workflows follow a defined sequence: the application submits sensitive data, the tokenization server generates a token, and then the token is returned to the application.
Only after the token has been successfully returned can the application replace the original sensitive data and store the token instead. This ensures that sensitive data is not retained within the application environment, reducing exposure and simplifying compliance requirements.
The other steps occur earlier in the process. An authorized application must request tokenization, and the sensitive data must be sent to the tokenization server before a token can be generated. Therefore, the immediate step before storing the token is the tokenization server returning the token to the application.

NEW QUESTION # 169
.....

Today, the IT industry is facing fierce competition, you will feel powerless, this is inevitable. All you have to do is to escort your career. Of course, you have many choices. I recommend that you use the itPass4sure WGU Managing-Cloud-Security Exam Questions And Answers, it is a good helper to help your success of IT certification. So what you still waiting for, go to get new itPass4sure WGU Managing-Cloud-Security exam training materials early.

2026 Latest itPass4sure Managing-Cloud-Security PDF Dumps and Managing-Cloud-Security Exam Engine Free Share:

https://drive.google.com/open?id=1oaGsMOxbWFEx2U2YnwBOwB7q-07pHV8j