



CCSP^{Q&As}

Cloud Security

Pass ISC CCSP Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass4itsure.com/ccsp.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by ISC Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



**QUESTION 1**

At which stage of the BCDR plan creation phase should security be included in discussions?

- A. Define scope
- B. Analyze
- C. Assess risk
- D. Gather requirements

Correct Answer: A

Security should be included in discussions from the very first phase when defining the scope. Adding security later is likely to incur additional costs in time and money, or will result in an incomplete or inadequate plan.

QUESTION 2

Data masking can be used to provide all of the following functionality, except:

- A. Test data in sandboxed environments
- B. Authentication of privileged users
- C. Enforcing least privilege
- D. Secure remote access

Correct Answer: B

Data masking does not support authentication in any way. All the others are excellent use cases for data masking.

QUESTION 3

You need to gain approval to begin moving your company's data and systems into a cloud environment. However, your CEO has mandated the ability to easily remove your IT assets from the cloud provider as a precondition.

Which of the following cloud concepts would this pertain to?

- A. Removability
- B. Extraction
- C. Portability
- D. Reversibility

Correct Answer: D

Reversibility is the cloud concept involving the ability for a cloud customer to remove all of its data and IT assets from a



cloud provider. Also, processes and agreements would be in place with the cloud provider that ensure all removals have been completed fully within the agreed upon timeframe. Portability refers to the ability to easily move between different cloud providers and not be locked into a specific one. Removability and extraction are both provided as terms similar to reversibility, but neither is the official term or concept.

QUESTION 4

Why does a Type 1 hypervisor typically offer tighter security controls than a Type 2 hypervisor?

- A. A Type 1 hypervisor also controls patching of its hosted virtual machines ensure they are always secure.
- B. A Type 1 hypervisor is tied directly to the bare metal and only runs with code necessary to perform its specific mission.
- C. A Type 1 hypervisor performs hardware-level encryption for tighter security and efficiency.
- D. A Type 1 hypervisor only hosts virtual machines with the same operating systems as the hypervisor.

Correct Answer: B

Type 1 hypervisors run directly on top of the bare metal and only contain the code and functions required to perform their purpose. They do not rely on any other systems or contain extra features to secure.

QUESTION 5

Although the REST API supports a wide variety of data formats for communications and exchange, which data formats are the most commonly used?

- A. SAML and HTML
- B. XML and SAML
- C. XML and JSON
- D. JSON and SAML

Correct Answer: C

JavaScript Object Notation (JSON) and Extensible Markup Language (XML) are the most commonly used data formats for the Representational State Transfer (REST) API and are typically implemented with caching for increased scalability and performance. Extensible Markup Language (XML) and Security Assertion Markup Language (SAML) are both standards for exchanging encoded data between two parties, with XML being for more general use and SAML focused on authentication and authorization data. HTML is used for authoring web pages for consumption by web browsers

QUESTION 6

Data center and operations design traditionally takes a tiered, topological approach.

Which of the following standards is focused on that approach and is prevalently used throughout the industry?

- A. IDCA



- B. NFPA
- C. BICSI
- D. Uptime Institute

Correct Answer: D

The Uptime Institute publishes the most widely known and used standard for data center topologies and tiers. The National Fire Protection Association (NFPA) publishes a broad range of fire safety and design standards for many different types of facilities. Building Industry Consulting Services International (BICSI) issues certifications for data center cabling. The International Data Center Authority (IDCA) offers the Infinity Paradigm, which takes a macro-level approach to data center design.

QUESTION 7

Key maintenance and security are paramount within a cloud environment due to the widespread use of encryption for both data and transmissions.

Which of the following key-management systems would provide the most robust control over and ownership of the key-management processes for the cloud customer?

- A. Remote key management service
- B. Local key management service
- C. Client key management service
- D. Internal key management service

Correct Answer: A

A remote key management system resides away from the cloud environment and is owned and controlled by the cloud customer. With the use of a remote service, the cloud customer can avoid being locked into a proprietary system from the cloud provider, but also must ensure that service is compatible with the services offered by the cloud provider. A local key management system resides on the actual servers using the keys, which does not provide optimal security or control over them. Both the terms internal key management service and client key management service are provided as distractors.

QUESTION 8

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?

- A. Community
- B. Hybrid
- C. Private
- D. Public

Correct Answer: A



A community cloud model is where customers that share a certain common bond or group membership come together to offer cloud services to their members, focused on common goals and interests.

QUESTION 9

All of these are methods of data discovery, except:

- A. Label-based
- B. User-based
- C. Content-based
- D. Metadata-based

Correct Answer: B

All the others are valid methods of data discovery; user-based is a red herring with no meaning.

QUESTION 10

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?

- A. Share
- B. Reservation
- C. Provision
- D. Limit

Correct Answer: D

Limits are put in place to enforce a maximum on the amount of memory or processing a cloud customer can use. This can be done either on a virtual machine or as a comprehensive whole for a customer, and is meant to ensure that enormous cloud resources cannot be allocated or consumed by a single host or customer to the detriment of other hosts and customers.

QUESTION 11

Which of the following roles would be responsible for managing memberships in federations and the use and integration of federated services?

- A. Inter-cloud provider
- B. Cloud service business manager
- C. Cloud service administrator
- D. Cloud service integrator



Correct Answer: A

The inter-cloud provider is responsible for peering with other cloud services and providers, as well as overseeing and managing federations and federated services. A cloud service administrator is responsible for testing, monitoring, and securing cloud services, as well as providing usage reporting and dealing with service problems. The cloud service integrator is responsible for connecting existing systems and services with a cloud. The cloud service business manager is responsible for overseeing the billing, auditing, and purchasing of cloud services.

QUESTION 12

Which type of audit report is considered a "restricted use" report for its intended audience?

- A. SAS-70
- B. SSAE-16
- C. SOC Type 1
- D. SOC Type 2

Correct Answer: C

SOC Type 1 reports are considered "restricted use" reports. They are intended for management and stakeholders of an organization, clients of the service organization, and auditors of the organization. They are not intended for release beyond those audiences.

QUESTION 13

Many aspects and features of cloud computing can make eDiscovery compliance more difficult or costly.

Which aspect of cloud computing would be the MOST complicating factor?

- A. Measured service
- B. Broad network access
- C. Multitenancy
- D. Portability

Correct Answer: C

With multitenancy, multiple customers share the same physical hardware and systems. With the nature of a cloud environment and how it writes data across diverse systems that are shared by others, the process of eDiscovery becomes much more complicated. Administrators cannot pull physical drives or easily isolate which data to capture. They not only have to focus on which data they need to collect, while ensuring they find all of it, but they also have to make sure that other data is not accidentally collected and exposed along with it. Measured service is the aspect of a cloud where customers only pay for the services they are actually using, and for the duration of their use. Portability refers to the ease with which an application or service can be moved among different cloud providers. Broad network access refers to the nature of cloud services being accessed via the public Internet, either with or without secure tunneling technologies. None of these concepts would pertain to eDiscovery.

**QUESTION 14**

In order to prevent cloud customers from potentially consuming enormous amounts of resources within a cloud environment and thus having a negative impact on other customers, what concept is commonly used by a cloud provider?

- A. Limit
- B. Cap
- C. Throttle
- D. Reservation

Correct Answer: A

A limit puts a maximum value on the amount of resources that may be consumed by either a system, a service, or a cloud customer. It is commonly used to prevent one entity from consuming enormous amounts of resources and having an operational impact on other tenants within the same cloud system. Limits can either be hard or somewhat flexible, meaning a customer can borrow from other customers while still having their actual limit preserved. A reservation is a guarantee to a cloud customer that a certain level of resources will always be available to them, regardless of what operational demands are currently placed on the cloud environment. Both cap and throttle are terms that sound similar to limit, but they are not the correct terms in this case.

QUESTION 15

When a system needs to be exposed to the public Internet, what type of secure system would be used to perform only the desired operations?

- A. Firewall
- B. Proxy
- C. Honeypot
- D. Bastion

Correct Answer: D

A bastion is a system that is exposed to the public Internet to perform a specific function, but it is highly restricted and secured to just that function. Any nonessential services and access are removed from the bastion so that security countermeasures and monitoring can be focused just on the bastion's specific duties. A honeypot is a system designed to look like a production system to entice attackers, but it does not contain any real data. It is used for learning about types of attacks and enabling countermeasures for them. A firewall is used within a network to limit access between IP addresses and ports. A proxy server provides additional security to and rulesets for network traffic that is allowed to pass through it to a service destination.