CCSP$^{Q\&As}$

Cloud Security

Pass ISC CCSP Exam with 100% Guarantee

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

https://www.passapply.com/ccsp.html

100% Passing Guarantee
100% Money Back Assurance

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

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

If a key feature of cloud computing that your organization desires is the ability to scale and expand without limit or concern about available resources, which cloud deployment model would you MOST likely be considering?

A. Public

B. Hybrid

C. Private

D. Community

Correct Answer: A

Public clouds, such as AWS and Azure, are massive systems run by major corporations, and they account for a significant share of Internet traffic and services. They are always expanding, offer enormous resources to customers, and are the least likely to run into resource constraints compared to the other deployment models. Private clouds would likely have the resources available for specific uses and could not be assumed to have a large pool of resources available for expansion. A community cloud would have the same issues as a private cloud, being targeted to similar organizations. A hybrid cloud, because it spans multiple clouds, would not fit the bill either, without the use of individual cloud models.

QUESTION 3

Your company is in the planning stages of moving applications that have large data sets to a cloud environment.

What strategy for data removal would be the MOST appropriate for you to recommend if costs and speed are primary considerations?

A. Shredding

B. Media destruction

C. Crypthographic erasure

D. Overwriting

Correct Answer: C

Cryptographic erasure involves having the data encrypted, typically as a matter of standard operations, and then rendering the data useless and unreadable by destroying the encryption keys for it. It represents a very cheap and immediate way to destroy data, and it works in all environments. With a cloud environment and multitenancy, media destruction or the physical destruction of storage devices, including shredding, would not be possible. Depending on the environment, overwriting may or may not be possible, but cryptographic erasure is the best answer because it is always an available option and is very quick to implement.

QUESTION 4

In a federated identity arrangement using a trusted third-party model, who is the identity provider and who is the relying party?

A. The users of the various organizations within the federations within the federation/a CASB

B. Each member organization/a trusted third party

C. Each member organization/each member organization

D. A contracted third party/the various member organizations of the federation

Correct Answer: D

In a trusted third-party model of federation, each member organization outsources the review and approval task to a third party they all trust. This makes the third party the identifier (it issues and manages identities for all users in all organizations in the federation), and the various member organizations are the relying parties (the resource providers that share resources based on approval from the third party).

QUESTION 5

Which of the following is NOT a major regulatory framework?

A. PCI DSS

B. HIPAA

C. SOX

D. FIPS 140-2

Correct Answer: D

FIPS 140-2 is a United States certification standard for cryptographic modules, and it provides guidance and requirements for their use based on the requirements of the data classification. However, these are not actual regulatory requirements. The Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), and the Payment Card Industry Data Security Standard (PCI DSS) are all major regulatory frameworks either by law or specific to an industry.

CCSP Practice Test   CCSP Study Guide   CCSP Exam Questions