

RC0-C02^{Q&As}

CompTIA Advanced Security Practitioner (CASP) Recertification Exam
for Continuing Education

Pass CompTIA RC0-C02 Exam with 100% Guarantee

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

<https://www.leads4pass.com/rc0-c02.html>

100% Passing Guarantee
100% Money Back Assurance

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

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



QUESTION 1

A corporation has Research and Development (RandD) and IT support teams, each requiring separate networks with independent control of their security boundaries to support department objectives. The corporation's Information Security Officer (ISO) is responsible for providing firewall services to both departments, but does not want to increase the hardware footprint within the datacenter. Which of the following should the ISO consider to provide the independent functionality required by each department's IT teams?

- A. Put both departments behind the firewall and assign administrative control for each department to the corporate firewall.
- B. Provide each department with a virtual firewall and assign administrative control to the physical firewall.
- C. Put both departments behind the firewall and incorporate restrictive controls on each department's network.
- D. Provide each department with a virtual firewall and assign appropriate levels of management for the virtual device.

Correct Answer: D

QUESTION 2

Which of the following technologies prevents an unauthorized HBA from viewing iSCSI target information?

- A. Deduplication
- B. Data snapshots
- C. LUN masking
- D. Storage multipaths

Correct Answer: C

A logical unit number (LUN) is a unique identifier that designates individual hard disk devices or grouped devices for address by a protocol associated with a SCSI, iSCSI, Fibre Channel (FC) or similar interface. LUNs are central to the management of block storage arrays shared over a storage area network (SAN).

LUN masking subdivides access to a given port. Then, even if several LUNs are accessed through the same port, the server masks can be set to limit each server's access to the appropriate LUNs. LUN masking is typically conducted at the host bus adapter (HBA) or switch level.

QUESTION 3

A company is in the process of outsourcing its customer relationship management system to a cloud provider. It will host the entire organization's customer database. The database will be accessed by both the company's users and its customers. The procurement department has asked what security activities must be performed for the deal to proceed. Which of the following are the MOST appropriate security activities to be performed as part of due diligence? (Select TWO).

- A. Physical penetration test of the datacenter to ensure there are appropriate controls.

- B. Penetration testing of the solution to ensure that the customer data is well protected.
- C. Security clauses are implemented into the contract such as the right to audit.
- D. Review of the organizations security policies, procedures and relevant hosting certifications.
- E. Code review of the solution to ensure that there are no back doors located in the software.

Correct Answer: CD

Due diligence refers to an investigation of a business or person prior to signing a contract. Due diligence verifies information supplied by vendors with regards to processes, financials, experience, and performance. Due diligence should verify the data supplied in the RFP and concentrate on the following: Company profile, strategy, mission, and reputation
Financial status, including reviews of audited financial statements
Customer references, preferably from companies that have outsourced similar processes
Management qualifications, including criminal background checks
Process expertise, methodology, and effectiveness
Quality initiatives and certifications
Technology, infrastructure stability, and applications
Security and audit controls
Legal and regulatory compliance, including any outstanding complaints or litigation
Use of subcontractors
Insurance
Disaster recovery and business continuity policies

C and D form part of Security and audit controls.

QUESTION 4

Company XYZ provides hosting services for hundreds of companies across multiple industries including healthcare, education, and manufacturing. The security architect for company XYZ is reviewing a vendor proposal to reduce company XYZ's hardware costs by combining multiple physical hosts through the use of virtualization technologies. The security architect notes concerns about data separation, confidentiality, regulatory requirements concerning PII, and administrative complexity on the proposal. Which of the following BEST describes the core concerns of the security architect?

- A. Most of company XYZ's customers are willing to accept the risks of unauthorized disclosure and access to information by outside users.
- B. The availability requirements in SLAs with each hosted customer would have to be re-written to account for the transfer of virtual machines between physical platforms for regular maintenance.
- C. Company XYZ could be liable for disclosure of sensitive data from one hosted customer when accessed by a malicious user who has gained access to the virtual machine of another hosted customer.
- D. Not all of company XYZ's customers require the same level of security and the administrative complexity of maintaining multiple security postures on a single hypervisor negates hardware cost savings.

Correct Answer: C

The hosting company (Company XYZ) is responsible for the data separation of customer data. If a malicious user gained access to a customer's sensitive data, the customer could sue the hosting company for damages. The result of such a lawsuit could be catastrophic for the hosting company in terms of compensation paid to the customer and loss of revenue due to the damaged reputation of the hosting company.

QUESTION 5

A security engineer is a new member to a configuration board at the request of management. The company has two new major IT projects starting this year and wants to plan security into the application deployment. The board is

primarily concerned with the applications' compliance with federal assessment and authorization standards. The security engineer asks for a timeline to determine when a security assessment of both applications should occur and does not attend subsequent configuration board meetings. If the security engineer is only going to perform a security assessment, which of the following steps in system authorization has the security engineer omitted?

- A. Establish the security control baseline
- B. Build the application according to software development security standards
- C. Review the results of user acceptance testing
- D. Consult with the stakeholders to determine which standards can be omitted

Correct Answer: A

A security baseline is the minimum level of security that a system, network, or device must adhere to. It is the initial point of reference for security and the document against which assessments would be done.

[Latest RC0-C02 Dumps](#)

[RC0-C02 VCE Dumps](#)

[RC0-C02 Braindumps](#)