



# RC0-C02<sup>Q&As</sup>

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.passapply.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 security administrator wants to calculate the ROI of a security design which includes the purchase of new equipment. The equipment costs \$50,000 and it will take 50 hours to install and configure the equipment. The administrator plans to hire a contractor at a rate of \$100/hour to do the installation. Given that the new design and equipment will allow the company to increase revenue and make an additional \$100,000 on the first year, which of the following is the ROI expressed as a percentage for the first year?

- A. -45 percent
- B. 5.5 percent
- C. 45 percent
- D. 82 percent

Correct Answer: D

Return on investment = Net profit / Investment

where: Net profit = gross profit - expenses

investment = stock + market outstanding[when defined as?] + claims

or

Return on investment = (gain from investment - cost of investment) / cost of investment  
Thus  $(100\,000 - 55\,000) / 50\,000 = 0,82 = 82\%$

References:

Gregg, Michael, and Billy Haines, *CASP CompTIA Advanced Security Practitioner Study Guide*, John Wiley and Sons, Indianapolis, 2012, p. 337 [http://www.financeformulas.net/Return\\_on\\_Investment.html](http://www.financeformulas.net/Return_on_Investment.html)

---

### QUESTION 2

An architect has been engaged to write the security viewpoint of a new initiative. Which of the following BEST describes a repeatable process that can be used for establishing the security architecture?

- A. Inspect a previous architectural document. Based on the historical decisions made, consult the architectural control and pattern library within the organization and select the controls that appear to best fit this new architectural need.
- B. Implement controls based on the system needs. Perform a risk analysis of the system. For any remaining risks, perform continuous monitoring.
- C. Classify information types used within the system into levels of confidentiality, integrity, and availability. Determine minimum required security controls. Conduct a risk analysis. Decide on which security controls to implement.
- D. Perform a risk analysis of the system. Avoid extreme risks. Mitigate high risks. Transfer medium risks and accept low risks. Perform continuous monitoring to ensure that the system remains at an adequate security posture.

Correct Answer: C



### QUESTION 3

A company has implemented data retention policies and storage quotas in response to their legal department's requests and the SAN administrator's recommendation. The retention policy states all email data older than 90 days should be eliminated. As there are no technical controls in place, users have been instructed to stick to a storage quota of 500Mb of network storage and 200Mb of email storage. After being presented with an e-discovery request from an opposing legal council, the security administrator discovers that the user in the suit has 1Tb of files and 300Mb of email spanning over two years. Which of the following should the security administrator provide to opposing council?

- A. Delete files and email exceeding policy thresholds and turn over the remaining files and email.
- B. Delete email over the policy threshold and hand over the remaining emails and all of the files.
- C. Provide the 1Tb of files on the network and the 300Mb of email files regardless of age.
- D. Provide the first 200Mb of e-mail and the first 500Mb of files as per policy.

Correct Answer: C

---

### QUESTION 4

An administrator is implementing a new network-based storage device. In selecting a storage protocol, the administrator would like the data in transit's integrity to be the most important concern. Which of the following protocols meets these needs by implementing either AES-CMAC or HMAC-SHA256 to sign data?

- A. SMB
- B. NFS
- C. FCoE
- D. iSCSI

Correct Answer: A

Server Message Block (SMB) is a protocol that has long been used by Windows computers for sharing files, printers and other resources among computers on the network. The server message blocks are the requests that an SMB client sends to a server and the responses that the server sends back to the client.

Microsoft has improved the SMB protocol over the years. In 2006, they came out with a new version, SMB 2.0, in conjunction with Vista, and SMB 2.1 with Windows 7. Version 2 was a major revision with significant changes, including a

completely different packet format. Windows 8 introduces another new version, SMB 3.0. Microsoft has made a number of security improvements in SMB 3.0, which will be introduced in the Windows 8 client and Windows Server 2012. A new

algorithm is used for SMB signing. SMB 2.x uses HMAC-SHA256. SMB 3.0 uses AES-CMAC. CMAC is based on a symmetric key block cipher (AES), whereas HMAC is based on a hash function (SHA). AES (Advanced Encryption Standard)

is the specification adopted by the U.S. government in 2002 and was approved by the National Security Agency (NSA)



for encryption of top secret information.

---

#### QUESTION 5

Company XYZ provides cable television services to several regional areas. They are currently installing fiber-to-the-home in many areas with hopes of also providing telephone and Internet services. The telephone and Internet services portions of the company will each be separate subsidiaries of the parent company. The board of directors wishes to keep the subsidiaries separate from the parent company. However all three companies must share customer data for the purposes of accounting, billing, and customer authentication. The solution must use open standards, and be simple and seamless for customers, while only sharing minimal data between the companies. Which of the following solutions is BEST suited for this scenario?

- A. The companies should federate, with the parent becoming the SP, and the subsidiaries becoming an IdP.
- B. The companies should federate, with the parent becoming the IdP, and the subsidiaries becoming an SSP.
- C. The companies should federate, with the parent becoming the IdP, and the subsidiaries becoming an SP.
- D. The companies should federate, with the parent becoming the ASP, and the subsidiaries becoming an IdP.

Correct Answer: C

The question states that "all three companies must share customer data for the purposes of accounting, billing, and customer authentication". The simplest solution is a federated solution. In a federated solution, you have a single authentication provider.

In this question, the parent company should be the authentication provider. The authentication provider is known as the IdP (Identity Provider). The IdP is the partner in a federation that creates security tokens for users. The other two

subsidiaries, the telephone and Internet services providers will be the SP (Service Provider). The SP is the partner in a federation that consumes security tokens for providing access to applications.

[RC0-C02 PDF Dumps](#)

[RC0-C02 VCE Dumps](#)

[RC0-C02 Study Guide](#)