



CAS-002^{Q&As}

CompTIA Advanced Security Practitioner Exam

Pass CompTIA CAS-002 Exam with 100% Guarantee

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

<https://www.passapply.com/cas-002.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 is tasked with securing a company's headquarters and branch offices move to unified communications. The Chief Information Officer (CIO) wants to integrate the corporate users' email, voice mail, telephony, presence and corporate messaging to internal computers, mobile users, and devices. Which of the following actions would BEST meet the CIO's goals while providing maximum unified communications security?

- A. Create presence groups, restrict IM protocols to the internal networks, encrypt remote devices, and restrict access to services to local network and VPN clients.
- B. Enable discretionary email forwarding restrictions, utilize QoS and Secure RTP, allow external IM protocols only over TLS, and allow port 2000 incoming to the internal firewall interface for secure SIP
- C. Set presence to invisible by default, restrict IM to invite only, implement QoS on SIP and RTP traffic, discretionary email forwarding, and full disk encryption.
- D. Establish presence privacy groups, restrict all IM protocols, allow secure RTP on session border gateways, enable full disk encryptions, and transport encryption for email security.

Correct Answer: A

QUESTION 2

A large corporation which is heavily reliant on IT platforms and systems is in financial difficulty and needs to drastically reduce costs in the short term to survive. The Chief Financial Officer (CFO) has mandated that all IT and architectural functions will be outsourced and a mixture of providers will be selected. One provider will manage the desktops for five years, another provider will manage the network for ten years, another provider will be responsible for security for four years, and an offshore provider will perform day to day business processing functions for two years. At the end of each contract the incumbent may be renewed or a new provider may be selected. Which of the following are the MOST likely risk implications of the CFO's business decision?

- A. Strategic architecture will be adversely impacted through the segregation of duties between the providers. Vendor management costs will remain unchanged. The risk position of the organization will decline as specialists now maintain the environment. The implementation of security controls and security updates will improve. Internal knowledge of IT systems will improve as providers maintain system documentation.
- B. Strategic architecture will improve as more time can be dedicated to strategy. System stability will improve as providers use specialists and tested processes to maintain systems. Vendor management costs will increase and the organization's flexibility to react to new market conditions will be reduced slightly. Internal knowledge of IT systems will improve as providers maintain system documentation. The risk position of the organization will remain unchanged.
- C. Strategic architecture will not be impacted in the short term, but will be adversely impacted in the long term through the segregation of duties between the providers. Vendor management costs will stay the same and the organization's flexibility to react to new market conditions will be improved through best of breed technology implementations. Internal knowledge of IT systems will decline over time. The implementation of security controls and security updates will not change.
- D. Strategic architecture will be adversely impacted through the segregation of duties between the providers. Vendor management costs will increase and the organization's flexibility to react to new market conditions will be reduced. Internal knowledge of IT systems will decline and decrease future platform development. The implementation of security controls and security updates will take longer as responsibility crosses multiple boundaries.

Correct Answer: D



QUESTION 3

The senior security administrator wants to redesign the company DMZ to minimize the risks associated with both external and internal threats. The DMZ design must support security in depth, change management and configuration processes, and support incident reconstruction. Which of the following designs BEST supports the given requirements?

- A. A dual firewall DMZ with remote logging where each firewall is managed by a separate administrator.
- B. A single firewall DMZ where each firewall interface is managed by a separate administrator and logging to the cloud.
- C. A SaaS based firewall which logs to the company's local storage via SSL, and is managed by the change control team.
- D. A virtualized firewall, where each virtual instance is managed by a separate administrator and logging to the same hardware.

Correct Answer: A

QUESTION 4

Ann, a software developer, wants to publish her newly developed software to an online store. Ann wants to ensure that the software will not be modified by a third party or end users before being installed on mobile devices. Which of the following should Ann implement to stop modified copies of her software from running on mobile devices?

- A. Single sign-on
- B. Identity propagation
- C. Remote attestation
- D. Secure code review

Correct Answer: C

QUESTION 5

A security administrator has finished building a Linux server which will host multiple virtual machines through hypervisor technology. Management of the Linux server, including monitoring server performance, is achieved through a third party web enabled application installed on the Linux server. The security administrator is concerned about vulnerabilities in the web application that may allow an attacker to retrieve data from the virtual machines.

Which of the following will BEST protect the data on the virtual machines from an attack?

- A. The security administrator must install the third party web enabled application in a chroot environment.
- B. The security administrator must install a software firewall on both the Linux server and the virtual machines.
- C. The security administrator must install anti-virus software on both the Linux server and the virtual machines.
- D. The security administrator must install the data exfiltration detection software on the perimeter firewall.



Correct Answer: A

[CAS-002 VCE Dumps](#)

[CAS-002 Practice Test](#)

[CAS-002 Braindumps](#)