



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.pass4itsure.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 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? (Select TWO).

- A. Establish the security control baseline to be assessed
- B. Build the application according to software development security standards
- C. Write the systems functionality requirements into the security requirements traceability matrix
- D. Review the results of user acceptance testing
- E. Categorize the applications according to use
- F. Consult with the stakeholders to determine which standards can be omitted

Correct Answer: AE

QUESTION 2

A security consultant is conducting a network assessment and wishes to discover any legacy backup Internet connections the network may have. Where would the consultant find this information and why would it be valuable?

- A. This information can be found in global routing tables, and is valuable because backup connections typically do not have perimeter protection as strong as the primary connection.
- B. This information can be found by calling the regional Internet registry, and is valuable because backup connections typically do not require VPN access to the network.
- C. This information can be found by accessing telecom billing records, and is valuable because backup connections typically have much lower latency than primary connections.
- D. This information can be found by querying the network's DNS servers, and is valuable because backup DNS servers typically allow recursive queries from Internet hosts.

Correct Answer: A

QUESTION 3

Which of the following are components defined within an Enterprise Security Architecture Framework? (Select THREE).

- A. Implementation run-sheets
- B. Solution designs
- C. Business capabilities



- D. Solution architectures
- E. Business requirements documents
- F. Reference models
- G. Business cases
- H. Business vision and drivers

Correct Answer: CFH

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

QUESTION 5

An investigator wants to collect the most volatile data first in an incident to preserve the data that runs the highest risk of being lost. After memory, which of the following BEST represents the remaining order of volatility that the investigator should follow?

- A. File system information, swap files, network processes, system processes and raw disk blocks.
- B. Raw disk blocks, network processes, system processes, swap files and file system information.
- C. System processes, network processes, file system information, swap files and raw disk blocks.
- D. Raw disk blocks, swap files, network processes, system processes, and file system information.

Correct Answer: C

QUESTION 6

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

QUESTION 7

An internal committee comprised of the facilities manager, the physical security manager, the network administrator, and a member of the executive team has been formed to address a recent breach at a company's data center. It was discovered that during the breach, an HVAC specialist had gained entry to an area that contained server farms holding sensitive financial data. Although the HVAC specialist was there to fix a legitimate issue, the investigation concluded security be provided for the two entry and exit points for the server farm. Which of the following should be implemented to accomplish the recommendations of the investigation?

- A. Implement a policy that all non-employees should be escorted in the data center.
- B. Place a mantrap at the points with biometric security.
- C. Hire an HVAC person for the company, eliminating the need for external HVAC people.
- D. Implement CCTV cameras at both points.

Correct Answer: B

QUESTION 8

The company is about to upgrade a financial system through a third party, but wants to legally ensure that no sensitive information is compromised throughout the project. The project manager must also make sure that internal controls are set to mitigate the potential damage that one individual's actions may cause. Which of the following needs to be put in place to make certain both organizational requirements are met? (Select TWO).

- A. Separation of duties
- B. Forensic tasks
- C. MOU
- D. OLA
- E. NDA
- F. Job rotation

Correct Answer: AE



QUESTION 9

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

QUESTION 10

A security engineer wants to implement forward secrecy but still wants to ensure the number of requests handled by the web server is not drastically reduced due to the larger computational overheads. Browser compatibility is not a concern; however system performance is. Which of the following, when implemented, would BEST meet the engineer's requirements?

- A. DHE
- B. ECDHE
- C. AES128-SHA
- D. DH

Correct Answer: B

QUESTION 11

A company which manufactures ASICs for use in an IDS wants to ensure that the ASICs' code is not prone to buffer and integer overflows. The ASIC technology is copyrighted and the confidentiality of the ASIC code design is exceptionally important. The company is required to conduct internal vulnerability testing as well as testing by a third party.

Which of the following should be implemented in the SDLC to achieve these requirements?

- A. Regression testing by the manufacturer and integration testing by the third party
- B. User acceptance testing by the manufacturer and black box testing by the third party
- C. Defect testing by the manufacturer and user acceptance testing by the third party
- D. White box unit testing by the manufacturer and black box testing by the third party

Correct Answer: D

QUESTION 12



A Chief Information Security Officer (CISO) has requested that a SIEM solution be implemented. The CISO wants to know upfront what the projected TCO would be before looking further into this concern. Two vendor proposals have been received:

Vendor A: product-based solution which can be purchased by the pharmaceutical company.

Capital expenses to cover central log collectors, correlators, storage and management consoles expected to be \$150,000. Operational expenses are expected to be a 0.5 full time employee (FTE) to manage the solution, and 1 full time

employee to respond to incidents per year.

Vendor B: managed service-based solution which can be the outsourcer for the pharmaceutical company's needs.

Bundled offering expected to be \$100,000 per year.

Operational expenses for the pharmaceutical company to partner with the vendor are expected to be a 0.5 FTE per year.

Internal employee costs are averaged to be \$80,000 per year per FTE. Based on calculating TCO of the two vendor proposals over a 5 year period, which of the following options is MOST accurate?

- A. Based on cost alone, having an outsourced solution appears cheaper.
- B. Based on cost alone, having an outsourced solution appears to be more expensive.
- C. Based on cost alone, both outsourced and in-sourced solutions appear to be the same.
- D. Based on cost alone, having a purchased product solution appears cheaper.

Correct Answer: A

[CAS-002 PDF Dumps](#)

[CAS-002 Exam Questions](#)

[CAS-002 Braindumps](#)



To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

Try our product !

100% Guaranteed Success

100% Money Back Guarantee

365 Days Free Update

Instant Download After Purchase

24x7 Customer Support

Average 99.9% Success Rate

More than 800,000 Satisfied Customers Worldwide

Multi-Platform capabilities - [Windows](#), [Mac](#), [Android](#), [iPhone](#), [iPod](#), [iPad](#), [Kindle](#)

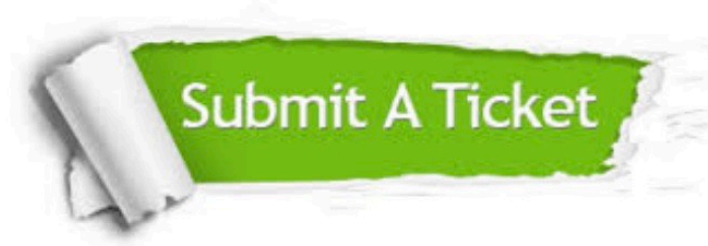
We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications. You can view Vendor list of All Certification Exams offered:

<https://www.pass4itsure.com/allproducts>

Need Help

Please provide as much detail as possible so we can best assist you.

To update a previously submitted ticket:



 <p>One Year Free Update Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 <p>Money Back Guarantee To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 <p>Security & Privacy We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.</p>
---	---	--

Any charges made through this site will appear as Global Simulators Limited.

All trademarks are the property of their respective owners.

Copyright © pass4itsure, All Rights Reserved.