

Demo Questions

CompTIA CAS-004 Exam

CompTIA Advanced Security Practitioner

Thank you for downloading **CAS-004 Exam** PDF

Question: 1

An organization is referencing NIST best practices for BCP creation while reviewing current internal organizational processes for mission-essential items.

Which of the following phases establishes the identification and prioritization of critical systems and functions?

- A. Review a recent gap analysis.
- B. Perform a cost-benefit analysis.
- C. Conduct a business impact analysis.
- D. Develop an exposure factor matrix.

Answer: C

Explanation:

Reference: <https://itsm.ucsf.edu/business-impact-analysis-bia-0>

Question: 2

An organization is preparing to migrate its production environment systems from an on-premises environment to a cloud service. The lead security architect is concerned that the organization's current methods for addressing risk may not be possible in the cloud environment.

Which of the following BEST describes the reason why traditional methods of addressing risk may not be possible in the cloud?

- A. Migrating operations assumes the acceptance of all risk.
 - B. Cloud providers are unable to avoid risk.
 - C. Specific risks cannot be transferred to the cloud provider.
 - D. Risks to data in the cloud cannot be mitigated.
-

Answer: C

Explanation:

Reference: <https://arxiv.org/ftp/arxiv/papers/1303/1303.4814.pdf>

Question: 3

A company created an external application for its customers. A security researcher now reports that the application has a serious LDAP injection vulnerability that could be leveraged to bypass authentication and authorization.

Which of the following actions would BEST resolve the issue? (Choose two.)

- A. Conduct input sanitization.
- B. Deploy a SIEM.
- C. Use containers.
- D. Patch the OS
- E. Deploy a WAF.
- F. Deploy a reverse proxy
- G. Deploy an IDS.

Answer: B, D

Explanation:

Question: 4

In preparation for the holiday season, a company redesigned the system that manages retail sales and moved it to a cloud service provider. The new infrastructure did not meet the company's availability requirements. During a postmortem analysis, the following issues were highlighted:

1. International users reported latency when images on the web page were initially loading.
2. During times of report processing, users reported issues with inventory when attempting to place orders.
3. Despite the fact that ten new API servers were added, the load across servers was heavy at peak times.

Which of the following infrastructure design changes would be BEST for the organization to implement to avoid these issues in the future?

- A. Serve static content via distributed CDNs, create a read replica of the central database and pull reports from there, and auto-scale API servers based on performance.
- B. Increase the bandwidth for the server that delivers images, use a CDN, change the database to a non-relational database, and split the ten API servers across two load balancers.
- C. Serve images from an object storage bucket with infrequent read times, replicate the database across different regions, and dynamically create API servers based on load.
- D. Serve static-content object storage across different regions, increase the instance size on the managed relational database, and distribute the ten API servers across multiple regions.

Answer: A

Explanation:

Question: 5

During a remodel, a company's computer equipment was moved to a secure storage room with cameras positioned on both sides of the door. The door is locked using a card reader issued by the security team, and only the security team and department managers have access to the room. The company wants to

be able to identify any unauthorized individuals who enter the storage room by following an authorized employee.

Which of the following processes would BEST satisfy this requirement?

- A. Monitor camera footage corresponding to a valid access request.
- B. Require both security and management to open the door.
- C. Require department managers to review denied-access requests.
- D. Issue new entry badges on a weekly basis.

Answer: A

Explanation:

Reference: <https://www.getkisi.com/access-control>

Question: 6

A company is preparing to deploy a global service.

Which of the following must the company do to ensure GDPR compliance? (Choose two.)

- A. Inform users regarding what data is stored.
- B. Provide opt-in/out for marketing messages.
- C. Provide data deletion capabilities.
- D. Provide optional data encryption.
- E. Grant data access to third parties.
- F. Provide alternative authentication techniques.

Answer: A, B

Explanation:

Reference: <https://gdpr.eu/compliance-checklist-us-companies/>

Question: 7

A SOC analyst is reviewing malicious activity on an external, exposed web server. During the investigation, the analyst determines specific traffic is not being logged, and there is no visibility from the WAF for the web application.

Which of the following is the MOST likely cause?

- A. The user agent client is not compatible with the WAF.
- B. A certificate on the WAF is expired.
- C. HTTP traffic is not forwarding to HTTPS to decrypt.
- D. Old, vulnerable cipher suites are still being used.

Answer: B

Explanation:

Reference: <https://aws.amazon.com/premiumsupport/knowledge-center/waf-block-http-requests-no-user-agent/>

Question: 8

A security analyst is reviewing the following output:

```
Request URL: http://www.largeworldwidebank.org/../../../../etc/password
Request Method: GET
Status Code: 200 OK
Remote Address: 107.240.1.127:443
Content-Length: 1245
Content-Type: text/html
Date: Tue, 03 Nov 2020 19:47:14 GMT
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cache-Control: max-age=0
Connection: keep-alive
Host: www.largeworldwidebank.org/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36
```

Which of the following would BEST mitigate this type of attack?

- A. Installing a network firewall
- B. Placing a WAF inline
- C. Implementing an IDS
- D. Deploying a honeypot

Answer: A

Explanation:

Question: 9

Which of the following terms refers to the delivery of encryption keys to a CASB or a third-party entity?

- A. Key sharing
- B. Key distribution
- C. Key recovery
- D. Key escrow

Answer: B

Explanation:

Reference: <https://www.open.edu/openlearn/ocw/mod/oucontent/view.php?id=48322§ion=1.3>

Question: 10

An organization is implementing a new identity and access management architecture with the following objectives:

- Supporting MFA against on-premises infrastructure
- Improving the user experience by integrating with SaaS applications
- Applying risk-based policies based on location

Performing just-in-time provisioning

Which of the following authentication protocols should the organization implement to support these requirements?

- A. Kerberos and TACACS
- B. SAML and RADIUS
- C. OAuth and OpenID
- D. OTP and 802.1X

Answer: A

Explanation:

Reference: <https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/migrate-application-authentication-to-azure-active-directory>