

Latest Version: 9.1

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: D

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: AE

Explanation:

A WAF protects your web apps by filtering, monitoring, and blocking any malicious HTTP/S traffic traveling to the web application, and prevents any unauthorized data from leaving the app. It does this by adhering to a set of policies that help determine what traffic is malicious and what traffic is safe.

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 nonrelational 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

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: B

Explanation:

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