DUMPSBOSS.COM

Specialist Infrastructure Security

EMC DES-9131

Version Demo

Total Demo Questions: 10

Total Premium Questions: 64

Buy Premium PDF

https://dumpsboss.com

support@dumpsboss.com

QUESTION NO: 1

Which document provides an implementation plan to recover business functions and processes during and after an event?

A. Business Continuity Plan

B. Disaster Recovery Plan

C. Risk Assessment Strategy

D. Business Impact Analysis

ANSWER: B

Explanation:

Reference: https://www.bmc.com/blogs/disaster-recovery-planning/

QUESTION NO: 2

What are the five functions of the NIST Framework Core?

A. Identify, Protect, Detect, Respond, and Recover

B. Governance, Identify, Recover, Respond, and Recover

C. Protect, Detect, Respond, Governance, and Recover

D. Identify, Respond, Protect, Detect, and Governance

ANSWER: A

Explanation:

Reference https://www.nist.gov/cyberframework/online-learning/five-functions

QUESTION NO: 3

Which NIST Cybersecurity Framework function should be executed before any others?

A. Respond

B. Protect

C. Recover

D. Identify

ANSWER: D

Explanation:

Reference: https://www.nist.gov/cyberframework/online-learning/five-functions

QUESTION NO: 4

The CSIRT team is following the existing recovery plans on non-production systems in a PRE-BREACH scenario. This action is being executed in which function?

A. Protect

B. Recover

C. Identify

D. Respond

ANSWER: A

QUESTION NO: 5

What is the purpose of separation of duties?

A. Internal control to prevent fraud

B. Enhance exposure to functional areas

C. Encourage collaboration

D. Mitigate collusion and prevent theft

ANSWER: A

Explanation:

Reference: https://www.marsdd.com/mars-library/internal-controls-accounting-key-benefits/

QUESTION NO: 6

What must be done before returning a compromised laptop to normal operations in the environment?

A. Perform a virus scan

B. Eliminate the root cause of the compromise

C. Re-image the device

D. Device cannot be returned to the environment

ANSWER: C

QUESTION NO: 7

What type of system processes information, the loss of which would have a debilitating impact to an organization?

A. Mission critical

B. Security critical

C. Business critical

D. Safety critical

ANSWER: A

QUESTION NO: 8

What does a security benchmark help define?

A. Whether or not the organization should implement ISCM

B. The Baseline, or “as is” state

C. Which step of the DRP to execute first

D. What parts of the Baseline are appropriate

ANSWER: D

QUESTION NO: 9 - (DRAG DROP)

DRAG DROP

Rank order the relative severity of impact to an organization of each plan, where “1” signifies the most impact and “4” signifies the least impact.

Select and Place:

Backup Plan	1
Disaster Recovery Plan	2
Recovery Plan	3
Business Continuity Plan	4

ANSWER:

Backup Plan	Disaster Recovery Plan
Disaster Recovery Plan	Business Continuity Plan
Recovery Plan	Disaster Recovery Plan
Business Continuity Plan	Backup Plan

Explanation:

QUESTION NO: 10

When should event analysis be performed?

A. Only when requested by an auditor

B. Routinely for all events collected on a mission critical system

C. Only at the discretion of an authorized security analyst

D. After an event is triggered by the detection system

ANSWER: B