

ISC CC

ISC2 Certified in Cybersecurity (CC)

For More Information – Visit link below:

<https://www.examsempire.com/>

Product Version

- 1. Up to Date products, reliable and verified.**
- 2. Questions and Answers in PDF Format.**



<https://examsempire.com/>

Visit us at: <https://www.examsempire.com/cc>

Latest Version: 6.0

Question: 1

Which of the following scenarios BEST demonstrates an organization's need to update its standards?

- A. The organization has completed its annual review of procedures and found no gaps in compliance
- B. Employees are frequently late in completing security training modules
- C. A new law is passed requiring the use of cloud-based storage solutions
- D. The organization's data encryption policy is irrelevant due to encryption technology advancements

Answer: D

Explanation:

Standards need to be updated when technological advancements render existing guidelines obsolete, ensuring that the organization continues to meet its security goals effectively.

Finding no gaps in compliance suggests current procedures are sufficient.

A new law may impact policy, but standards address internal specifications.

Employee delays in completing training relate more to procedure enforcement than standards.

Question: 2

A company wants to assign private IP addresses to devices on its internal network. Which IP address range can be used for this purpose?

- A. 203.0.113.0–203.0.113.255
- B. 172.16.0.0–172.31.255.255
- C. 192.0.0.1–192.0.0.255
- D. 8.8.8.0–8.8.8.255

Answer: B

Explanation:

The 172.16.0.0–172.31.255.255 range is part of the private IP address space reserved for internal use within organizations alongside 192.168.0.0–192.168.255.255 and 10.0.0.0–10.255.255.255.

The other address ranges are not reserved for private use.

Question: 3

What is the purpose of implementing mantraps in physical access control systems?

- A. To monitor network traffic for unusual activity
- B. To ensure that only one person can enter or exit a secure area at a time

- C. To allow multiple individuals to enter a secure area quickly
- D. To increase the speed of employee access to secure areas

Answer: B

Explanation:

Mantraps are used to ensure that only one person can enter or exit a secure area at a time, preventing unauthorized individuals from tailgating or entering alongside authorized personnel.

Mantraps do not allow multiple individuals to enter quickly.

Mantraps do not monitor network traffic.

Mantraps are designed to enhance security, not to increase the speed of access.

Question: 4

What is a configuration baseline?

- A. A type of firewall rule that blocks unauthorized access
- B. The initial set of security settings in which a system must comply
- C. A collection of software patches applied to a system
- D. The process of monitoring system activity for unusual behavior

Answer: B

Explanation:

A configuration baseline refers to the documented set of configurations that serve as the standard for a system's security and performance. It ensures consistency and compliance within the system environment.

A collection of patches is related to system updates.

Monitoring system activity relates to intrusion detection or logging.

Firewall rules are unrelated to configuration baselines.

Question: 5

Why is it important for a security policy to include a section on compliance and enforcement?

- A. To state the date when the policy was written
- B. To define acceptable use of company resources
- C. To understand consequences of failing to follow the policy
- D. To provide a list of acceptable security tools

Answer: C

Explanation:

The compliance and enforcement section is essential because it outlines the consequences for non-compliance, ensuring individuals understand that failing to adhere to the policy can result in disciplinary action or other repercussions.

The effective date states when the policy was written or becomes active.

Acceptable use of resources is part of an Acceptable Use Policy (AUP), not general compliance.

A list of security tools would be part of a technical procedure, not the policy itself.

Question: 6

What is the PRIMARY goal of implementing segregation of duties in an organization?

- A. To ensure that no individual has control over all critical aspects of a process
- B. To allow employees to handle multiple tasks to improve efficiency
- C. To allow employees to access all parts of a system
- D. To limit access to sensitive data to only a few employees

Answer: A

Explanation:

Segregation of duties ensures that no single individual has control over all critical aspects of a process. This helps with reducing the risk of fraud or errors.

Allowing employees to handle multiple tasks is not the goal of segregation of duties and would actively go against this principle.

Limiting access to sensitive data relates more to access control, not specifically segregation of duties.

Allowing employees to access all parts of a system violates segregation of duties.

Question: 7

What is the PRIMARY purpose of a disaster recovery plan?

- A. To restore critical IT systems and data
- B. To improve employee satisfaction
- C. To increase the organization's profits
- D. To eliminate all potential risks to the organization

Answer: A

Explanation:

A Disaster Recovery (DR) plan is designed to restore critical IT systems and data following a disaster, ensuring the organization can resume normal operations.

Improving employee satisfaction is not the primary focus of a DR plan.

Eliminating all potential risks is impossible; DR plans aim to mitigate the impacts.

DR plans do not directly increase profits.

Question: 8

How does a Distributed Denial of Service (DDoS) attack typically work?

- A. By injecting malicious code into the target system
- B. By flooding the target with traffic
- C. By stealing sensitive data from the target
- D. By exploiting a vulnerability in the target system

Answer: B

Explanation:

A Distributed Denial of Service (DDoS) attack overwhelms a target system with traffic from multiple sources, rendering the service unusable.

Exploiting vulnerabilities, stealing data, and injecting code are tactics used in other types of attacks, such as exploits, data breaches, and viruses.

Question: 9

What does a SaaS product offer to users?

- A. Physical hardware that the user can manage directly
- B. On-premises network equipment
- C. A development platform to create custom applications
- D. Managed software applications hosted in the cloud

Answer: D

Explanation:

Software as a Service (SaaS) provides fully managed software applications that are hosted in the cloud. Users can access these applications over the internet without having to install or maintain them.

SaaS does not provide physical hardware.

SaaS does not offer a development platform; it is offered by Platform as a Service (PaaS).

SaaS is not related to on-premises network equipment.

Question: 10

Which of the following situations would MOST likely require a change in an organization's risk tolerance?

- A. A significant change in the organization's strategic objectives
- B. The company hires a new Chief Information Officer (CIO)
- C. The company experiences minor operational disruptions frequently
- D. A slight increase in customer complaints

Answer: A

Explanation:

A significant change in strategic objectives could require adjusting the risk tolerance to align with new goals or priorities.

Minor operational disruptions usually do not necessitate changes in risk tolerance.

A slight increase in customer complaints is typically a minor issue and may not affect risk tolerance.

Hiring a new Chief Information Officer (CIO) does not directly influence risk tolerance unless accompanied by changes in strategy.

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

**Check our Customer Testimonials and ratings
available on every product page.**

Visit our website.

<https://examsempire.com/>