Shared Assessments
CTPRP
Certified Third-Party Risk Professional (CTPRP)

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/

Latest Version: 6.0

Question: 1

What is the main purpose of the remote wipe feature in company-owned devices?

A. To increase the resale value of company devices
B. To track the location of company devices continuously
C. To prevent unauthorized access to sensitive information
D. To enforce software updates on multiple devices simultaneously

Answer: C

Explanation:
The main purpose of the remote wipe feature is to secure sensitive information by ensuring it does not fall into unauthorized hands if a company-owned device is lost or stolen.

Question: 2

Which scenario best describes the appropriate use of a remote wipe?

A. A device is scheduled for regular maintenance
B. A company device is lost during business travel
C. An employee requests a newer model of their device
D. A device displays a software error repeatedly

Answer: B

Explanation:
The appropriate use of a remote wipe feature is exemplified when a company device containing sensitive information is lost during business travel, necessitating immediate action to secure the data.

Question: 3

Given the security measures listed, which one would not directly impact the evaluation of remote access risks?

A. Implementing end-to-end encryption for data in transit to safeguard against interception.
B. Employing multifactor authentication to verify the identity of users accessing systems remotely.
C. Application whitelisting, as it focuses on limiting software execution based on pre-established security policies.
D. Remote desktop protocol (RDP) security, as it directly relates to the safety of remote desktop connections.

Explanation:
Application whitelisting's focus is specifically on controlling application execution based on a list of approved software, which does not directly deal with the integrity of remote access connections or the authentication and authorization processes involved in remote access scenarios.

Question: 4

In a company where the third line of defense is reviewing compliance practices, what is their main objective?

A. Monitoring the adherence to international standards
B. Evaluating the effectiveness of risk management and control systems
C. Ensuring that all employees are trained on risk protocols
D. Implementing new technologies to enhance security measures

Explanation:
The main goal of this function is to verify and ensure that all risk management processes are working effectively and that the organization's control culture is robust, assisting in safeguarding the organization's operations and reputation.

Question: 5

What aspect of a service provider's program is least affected by whistleblower compliance mechanisms?

A. The monitoring and reporting of network security incidents.
B. The routine maintenance and updating of cybersecurity software.
C. The effectiveness of data encryption and secure data storage techniques.
D. The awareness and prevention of data breaches and unauthorized access.

Explanation:
Whistleblower compliance mechanisms primarily relate to ethical conduct and accountability within an organization but have minimal direct impact on the practical measures for preventing data breaches and unauthorized access. These mechanisms are less involved in the day-to-day operations concerning security breaches or privacy issues directly.

Question: 6

What does an unrecoverable data loss after a system restore indicate about the Recovery Point Objective (RPO)?

A. It shows that the incident response was not initiated in a timely manner.
B. It reflects an adequate level of preparedness and compliance with industry standards.
C. It suggests the Recovery Time Objective (RTO) metrics were not calculated correctly.
D. It indicates that the Recovery Point Objective was not met as the data loss exceeded the allowable period.

Answer: D

Explanation:
The Recovery Point Objective (RPO) defines the maximum period during which data can be lost due to an incident. If data restoration after a system failure results in unrecoverable data loss exceeding this period, it signifies that the RPO was not achieved, hence the disaster recovery strategies need reassessment to align with the established RPO.

Question: 7

In a scenario where a subcontractor fails to meet data protection standards, what likely was not effectively implemented?

A. Adequate due diligence and monitoring of subcontractor compliance.
B. Strict limitations on the amount of data accessible to subcontractors.
C. General guidelines provided to subcontractors without specific requirements.
D. Reliance solely on third-party assurances without independent verification.

Answer: A

Explanation:
If a subcontractor fails to meet data protection standards, it likely indicates that there was insufficient due diligence and ongoing monitoring of the subcontractor's compliance with the organization's required standards. Adequate due diligence would typically include verifying the subcontractor's practices and ensuring they meet the organization's data protection criteria.

Question: 8

In a scenario where a patch caused additional software incompatibilities post-deployment, what could have been neglected?

A. Reviewing user feedback on performance issues after deploying the patch.
B. Comprehensive testing of the patch in a controlled environment.
C. Quick rollout of the patch to a limited number of users to gather feedback.
D. Direct modification of the production code to apply critical security fixes.

Explanation:
If a patch deployment results in additional software incompatibilities, it suggests that the patch was not sufficiently tested in environments that mimic real-world operating conditions. Comprehensive testing should uncover potential conflicts with existing configurations or dependencies before the patch is widely deployed.

Question: 9

Which of the following would most likely require a reassessment of a vendor?

A. A significant change in the vendor's scope of work
B. A minor amendment to the service agreement with the vendor
C. The vendor's decision to relocate its primary data centers
D. Updating the vendor's technological infrastructure

Answer: A

Explanation:
A significant alteration in the scope of the vendor's work could fundamentally change their access to sensitive data or systems, necessitating a thorough reassessment to ensure ongoing compliance and security measures are adequate.

Question: 10

What is a likely consequence of a weak risk culture in an organization?

A. It leads to the creation of silos and conflicts that undermine risk management.
B. It enhances the organization's capability to respond to market changes rapidly.
C. It increases the efficiency of processes and reduces operational costs.
D. It fosters rapid innovation by encouraging risk-taking without sufficient oversight.

Answer: A

Explanation:
A weak risk culture often leads to the creation of silos and internal conflicts, which significantly undermine effective risk management. These silos prevent cohesive and coordinated efforts to address risks, thereby exposing the organization to greater vulnerabilities and inefficiencies.

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/