ISC² Post Assessment Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. **What aspect of security can hinder productivity if not properly aligned with business needs?**
   - **A. Strict security measures**
   - **B. Increased monitoring**
   - **C. Deployment of firewalls**
   - **D. Conflicting security policies**

2. **What type of control would be most effective in ensuring cars do not collide with pedestrians?**
   - **A. Administrative**
   - **B. Technical**
   - **C. Physical**
   - **D. Nuanced**

3. **A human guard monitoring a hidden camera is an example of which type of control?**
   - **A. Detective**
   - **B. Preventive**
   - **C. Deterrent**
   - **D. Logical**

4. **Who typically dictates policy within an organization?**
   - **A. The security manager**
   - **B. The Human Resources office**
   - **C. Senior management**
   - **D. Auditors**

5. **To ensure availability for a data center, it is best to plan for both resilience and what aspect of the elements in the facility?**
   - **A. Uniqueness**
   - **B. Destruction**
   - **C. Redundancy**
   - **D. Hue**

6. What does a system that tracks user actions to provide accountability exemplify?

A. Non-repudiation

B. Multifactor authentication

C. Biometrics

D. Privacy

7. Who is responsible for approving an incident response policy?

A. The security manager

B. Investors

C. Senior management

D. (ISC)²

8. Which of the following incidents would fall under the responsibility of incident response teams?

A. Regular database maintenance

B. Data breaches

C. Employee onboarding procedures

D. Software updates

9. What is the primary goal of implementing security awareness training in an organization?

A. To comply with legal standards

B. To avoid financial losses

C. To prepare employees for cyber threats

D. To enhance company reputation

10. What is a risk associated with resuming normal operations too soon after a disaster recovery effort?

A. The organization could save money

B. Investors might be upset

C. The danger posed by the disaster might still be present

D. Regulators might disapprove

Answers

1. D
2. C
3. A
4. C
5. C
6. A
7. C
8. B
9. C
10. C

Explanations

1. What aspect of security can hinder productivity if not properly aligned with business needs?

A. Strict security measures

B. Increased monitoring

C. Deployment of firewalls

D. Conflicting security policies

Conflicting security policies can significantly hinder productivity when they do not align with the business's operational requirements. When a business has multiple security policies that contradict each other, employees may find it challenging to understand which protocols to follow. This confusion can lead to delays in processes, inefficiencies in workflows, and in some cases, employees may become discouraged, leading to a decline in morale and productivity. Additionally, if the policies conflict with business needs, employees might bypass them to accomplish their tasks, undermining the very purpose of the security measures. Proper alignment between security policies and business objectives is crucial to ensure that security supports the overall mission of the organization while safeguarding assets effectively. In contrast, while strict security measures, increased monitoring, and the deployment of firewalls are all vital components of a robust security framework, their presence alone does not inherently cause productivity issues unless they lead to restrictions or complications that are inconsistent with the organization's goals.

2. What type of control would be most effective in ensuring cars do not collide with pedestrians?

A. Administrative

B. Technical

C. Physical

D. Nuanced

Choosing physical controls as the most effective means to prevent cars from colliding with pedestrians is grounded in the nature of these controls. Physical controls are tangible structures or barriers that can be implemented in the environment to directly reduce or eliminate hazards. Examples include crosswalks, traffic signals, speed bumps, and pedestrian barriers. These measures physically separate vehicles from pedestrians or regulate the flow of both to ensure safer interactions. In this context, physical controls provide direct intervention in the driving and walking environment, thus lowering the risk of accidents effectively. They are easily observable and enforceable, allowing both drivers and pedestrians to understand the designated spaces for each. Other types of controls, such as administrative measures (like policies or training), technical solutions (like warning systems or sensors), and nuanced approaches (which might suggest a blend of controls or more advanced strategies), can support safety but do not have the same immediate and tangible impact on preventing collisions as physical controls do.

3. A human guard monitoring a hidden camera is an example of which type of control?

A. Detective

B. Preventive

C. Deterrent

D. Logical

A human guard monitoring a hidden camera is considered a detective control because it is designed to identify and monitor activities or security breaches after they occur. Detective controls are utilized to detect incidents, failures, or unauthorized actions that have already taken place. In this case, the guard's role involves observing the footage captured by the camera to recognize any suspicious behavior or security threats in real-time, enabling a prompt response to incidents. The nature of detective controls emphasizes their purpose in discovering and reporting issues rather than actively preventing them from happening or serving as a deterrent against potential threats. While preventive controls aim to stop incidents before they occur and deterrent controls seek to discourage undesirable actions through visible security measures or threats of consequence, the primary function of the guard monitoring the camera aligns directly with the goals of detection.

4. Who typically dictates policy within an organization?

A. The security manager

B. The Human Resources office

C. Senior management

D. Auditors

In most organizations, policy formulation is primarily the responsibility of senior management. This group includes executives and other leaders who set the strategic direction and organizational goals. They have the authority to create, modify, and endorse policies that govern the entire organization. These policies are often developed to align with the organization's mission, regulatory requirements, risk management strategies, and overall business objectives. Senior management is uniquely positioned to ensure that policies reflect the organization's values and comply with both internal and external expectations. Their broader perspective allows them to consider the implications of various policies across different departments and functions, which is crucial for effective governance. While roles like the security manager, Human Resources, and auditors contribute to the development and implementation of specific policies related to their areas of expertise, they typically operate within the frameworks established by senior management. Auditors focus on compliance and effectiveness of policies rather than creating them, and Human Resources manages policies related to personnel matters rather than overarching organizational directives. Therefore, the authority and responsibility for dictating policies lie predominantly with senior management.

5. To ensure availability for a data center, it is best to plan for both resilience and what aspect of the elements in the facility?

A. Uniqueness

B. Destruction

C. Redundancy

D. Hue

Planning for redundancy is crucial in ensuring availability for a data center because redundancy involves having multiple instances or backups of components and systems to take over if one fails. This approach reduces the chances of a single point of failure, thereby enhancing the overall reliability and availability of the data center operations. In the context of data centers, redundancy can apply to various components, such as power supplies, network connections, cooling systems, and storage. By incorporating redundant components, organizations can continue to operate smoothly even in the event of hardware failures or other disruptions. This capability is a fundamental principle of high-availability systems, which are designed to remain operational and minimize downtime. The other concepts, while potentially related to data center management, do not directly contribute to availability in the same way redundancy does. For instance, uniqueness could refer to having specialized systems or configurations, but it does not inherently address failure or availability. Destruction might pertain to planning for disaster recovery or data loss, yet it does not actively promote availability. Lastly, hue does not have any relevance in this context, as it relates more to color rather than operational reliability. Thus, redundancy stands out as the essential factor in maintaining high availability in a data center.

6. What does a system that tracks user actions to provide accountability exemplify?

A. Non-repudiation

B. Multifactor authentication

C. Biometrics

D. Privacy

A system that tracks user actions to provide accountability exemplifies non-repudiation, which is a fundamental security principle. Non-repudiation ensures that a user cannot deny having performed a particular action within a system. By maintaining a log of user actions, the system creates a verifiable record that can be used as evidence to confirm that the action took place and that the individual responsible for it is identifiable. This accountability is crucial in various contexts, such as financial transactions, legal compliance, and organizational policy enforcement, as it helps to prevent disputes regarding who did what and when. While the other options relate to aspects of security and user identity, they do not specifically address the concept of tracking actions for accountability. Multifactor authentication involves using multiple methods to verify a user's identity, which enhances security but does not provide a record of actions. Biometrics refers to using physical characteristics for identification, which, while useful in authentication, does not inherently provide accountability for actions taken within a system. Privacy concerns the protection of user information and data from unauthorized access, which, while important, does not directly relate to the accountability provided by tracking user actions.

7. Who is responsible for approving an incident response policy?

A. The security manager

B. Investors

C. Senior management

D. (ISC)²

The approval of an incident response policy is primarily the responsibility of senior management. This is because the incident response policy outlines how an organization plans to address and manage security incidents, which can have significant implications for the organization's operational capacity, reputation, and overall risk posture. Senior management is in a pivotal position to acknowledge the importance of cybersecurity and allocate resources to implement the policy effectively. Their approval signifies a commitment to prioritize incident response efforts and ensure that the policy aligns with the organization's broader business objectives and risk management strategies. In contrast, while a security manager may develop and propose the incident response policy, they generally do not have the authority to make final decisions regarding policy approval. Investors typically do not get involved in the day-to-day operational policies unless they directly impact financial outcomes. (ISC)² is a certification body that provides training and support for professionals in the field, but it does not have governance over an organization's internal policies.

8. Which of the following incidents would fall under the responsibility of incident response teams?

A. Regular database maintenance

B. Data breaches

C. Employee onboarding procedures

D. Software updates

The responsibility of incident response teams primarily revolves around identifying, managing, and mitigating security incidents that could jeopardize an organization's information systems and data integrity. Data breaches are a significant concern for organizations, as they involve unauthorized access to sensitive information, potentially leading to data loss, financial damage, or reputational harm. When a data breach occurs, incident response teams are tasked with quickly assessing the situation, containing the breach, conducting forensic analysis to understand its scope, and implementing measures to prevent future occurrences. This involves coordinated efforts across various domains, including IT security, legal, and public relations, to effectively address the breach and communicate with affected parties. In contrast, regular database maintenance, employee onboarding procedures, and software updates are aspects of IT operations and management rather than incidents demanding immediate incident response. These activities are essential for the continued robustness and security of systems but do not typically involve the reactive measures that incident response teams implement in response to a security threat like a data breach.

9. What is the primary goal of implementing security awareness training in an organization?

A. To comply with legal standards

B. To avoid financial losses

C. To prepare employees for cyber threats

D. To enhance company reputation

The primary goal of implementing security awareness training in an organization is to prepare employees for cyber threats. In today's digital landscape, employees are often the first line of defense against security breaches and potential cyber-attacks. Security awareness training equips them with the knowledge to recognize phishing attempts, understand social engineering tactics, and adopt best practices for safeguarding sensitive information. By fostering a security-conscious culture, organizations can significantly reduce the likelihood of successful attacks, as employees become more vigilant and proactive in their efforts to protect data. This level of awareness is crucial because human error is frequently a contributing factor in security incidents. Thus, the training aims to empower employees with the skills and understanding necessary to identify and report suspicious activities, enhancing the overall security posture of the organization.

10. What is a risk associated with resuming normal operations too soon after a disaster recovery effort?

A. The organization could save money

B. Investors might be upset

C. The danger posed by the disaster might still be present

D. Regulators might disapprove

Resuming normal operations too soon after a disaster recovery effort carries the significant risk that the underlying dangers associated with the disaster may still be present. When a disaster strikes, organizations typically implement recovery strategies and processes aimed at restoring functionality. However, these efforts may not address all residual risks or damage that could still affect the safety and security of operations. For example, if a natural disaster damaged infrastructure, it could take time to ensure that all systems are fully operational and secure. Rushing back into full operation without verifying that all risks have been mitigated can lead to further issues, such as potential safety hazards for employees, vulnerabilities to data breaches, or incomplete recovery of services, which ultimately can affect customer trust and the organization's reputation. Other options suggest potential financial or reputational consequences but do not directly address the critical safety and operational integrity concerns that arise from the residual risks that could threaten the organization if operations are resumed prematurely.