FedVTE Information Systems Security Management Professional (ISSMP) Practice Exam (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. Which of the following is an example of a physical security control?

A. Biometric access systems

B. Encryption software

C. Firewalls

D. Intrusion detection systems

2. Which of the following is NOT a necessary step to achieving data privacy?

A. Identify, classify, and chart access to sensitive data

B. Define security policy around identified data

C. Decide on new technologies to implement

D. Decide on mode of implementation

3. What is the primary purpose of conducting a security risk assessment?

A. To implement security training programs

B. To identify, evaluate, and prioritize risks to organizational assets

C. To develop disaster recovery plans

D. To automate security monitoring processes

4. What are the key components of a strategic IS plan?

A. Goals, resources, and stakeholders

B. Policies, procedures, and technology

C. Analysis, implementation, and evaluation

D. Budgeting, staffing, and auditing

5. Which of the following is NOT related to the management of privileged accounts?

A. A. Least privilege

B. B. Relationships

C. C. Job rotation

D. D. Entitlements

6. In the context of risk assessment, what is a primary focus?

A. Only physical security threats.

B. Balancing costs versus potential impact of risks.

C. Ensuring all employees follow security protocols.

D. Merging risk management with operational efficiency.

7. In risk management, what does a risk mitigation strategy involve?

A. Actions designed to eliminate all risks

B. Actions taken to reduce the likelihood or impact of a risk

C. Creating insurance policies for all risks

D. Developing recovery plans post-incident

8. What is an inappropriate method for evaluating personnel for security risks?

A. A. Driving record review

B. B. Passport number verification and validation

C. C. Drug and substance testing

D. D. Education, licensing, and certification verification

9. Which of the following is NOT considered a significant threat from employees to information systems?

A. IT sabotage

B. Fraud

C. Theft of intellectual property

D. Logic bombs

10. Consistent implementation of security configurations throughout an organization is known as:

A. Auditing.

B. Valid implementation.

C. Baselines.

D. Configuration management.

Answers

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

Explanations

1. Which of the following is an example of a physical security control?

A. Biometric access systems

B. Encryption software

C. Firewalls

D. Intrusion detection systems

A biometric access system is indeed an example of a physical security control because it is a technology that grants access to a physical location based on the verification of physical characteristics unique to an individual, such as fingerprints, retinal scans, or facial recognition. This type of control is specifically designed to protect physical spaces like buildings or secure areas by ensuring that only authorized personnel can enter. On the other hand, encryption software, firewalls, and intrusion detection systems serve as logical or technical security controls. They are primarily focused on protecting data, networks, and systems from unauthorized access and cyber threats, rather than physical access to specific locations. While all these controls are essential components of a comprehensive security strategy, the biometric access system distinctly classifies as a physical control focused on securing actual physical premises.

2. Which of the following is NOT a necessary step to achieving data privacy?

A. Identify, classify, and chart access to sensitive data

B. Define security policy around identified data

C. Decide on new technologies to implement

D. Decide on mode of implementation

Achieving data privacy involves a structured approach that includes several essential steps to ensure that sensitive information is properly protected. Identifying, classifying, and charting access to sensitive data provides a clear understanding of what data exists and who has access to it, forming the foundation for any privacy initiative. Defining security policies around the identified data is crucial as it sets the rules and guidelines for protecting that data, ensuring compliance with legal and regulatory requirements. The mode of implementation is also an important consideration, as it involves translating policies into actionable measures, such as procedures, technical controls, and training programs. Each of these steps directly contributes to the overall goal of safeguarding data privacy. In contrast, deciding on new technologies to implement, while a practical consideration, is not a necessary step to achieving data privacy itself. Technology decisions should be influenced by the established policies and the data protection needs highlighted in the earlier steps, but they are not foundational to the overall strategy for achieving data privacy. Therefore, this option does not align with the core steps required to secure data privacy, making it the choice that is not necessary in this context.

3. What is the primary purpose of conducting a security risk assessment?

A. To implement security training programs

B. To identify, evaluate, and prioritize risks to organizational assets

C. To develop disaster recovery plans

D. To automate security monitoring processes

The primary purpose of conducting a security risk assessment is to identify, evaluate, and prioritize risks to organizational assets. This process is essential because it allows organizations to understand the vulnerabilities they face and the potential impact of various threats. By systematically assessing risks, organizations can make informed decisions about where to allocate resources to mitigate those risks effectively. Through this assessment, leaders gain insight into which assets are most critical to their operations and what specific threats could jeopardize those assets. This prioritization helps in forming a strategic approach to risk management and ensures that the most pressing risks are addressed first. Ultimately, the goal of a security risk assessment is to enhance the organization's security posture and ensure that protective measures are aligned with the actual risks faced. While security training programs, disaster recovery plans, and automated security monitoring processes are important components of a comprehensive security strategy, they are not the primary focus of a risk assessment. A risk assessment lays the groundwork for these activities by providing the necessary context regarding the risks that need to be managed.

4. What are the key components of a strategic IS plan?

A. Goals, resources, and stakeholders

B. Policies, procedures, and technology

C. Analysis, implementation, and evaluation

D. Budgeting, staffing, and auditing

The key components of a strategic IS plan encompass a range of elements that aim to align information systems with organizational goals. The correct choice consists of policies, procedures, and technology, as these are fundamental to the development and execution of an effective strategic information systems plan. Policies outline the governance framework and dictate how information systems resources should be utilized in accordance with organizational objectives. They help ensure compliance with regulations, manage risk, and establish security protocols. Procedures provide the step-by-step methods for implementing the policies, ensuring that all stakeholders understand their roles in the management and operation of the information systems. Technology, which includes hardware, software, and network infrastructure, is the backbone that supports the strategic initiatives of the organization. It is vital for enabling the processes dictated by policies and procedures. By having a structured approach that integrates these three components, organizations can create a strategic IS plan that effectively supports their long-term goals and responds to changing business environments. The focus on policies ensures that the use of technology is not only effective but also responsible and secure, which is essential in today's digitally driven landscape.

5. Which of the following is NOT related to the management of privileged accounts?

A. A. Least privilege

B. B. Relationships

C. C. Job rotation

D. D. Entitlements

The concept of management of privileged accounts is primarily centered around principles and practices that ensure these accounts are secured and managed effectively to minimize risk. The correct choice identifies "job rotation" as the option that is not directly related to managing privileged accounts. "Job rotation" typically refers to the practice of moving employees between different roles or tasks over time. This technique is commonly applied in various organizational environments to reduce the risk of fraud or unethical behavior, as it prevents any one employee from gaining too much control over a process. While this is a valuable practice in overall security management, it does not specifically address the management of privileged accounts. In contrast, "least privilege," "relationships," and "entitlements" are directly applicable to the topic. "Least privilege" is a security principle that ensures users have only the minimum access rights necessary to perform their job functions, which is critical for the management of privileged accounts. "Entitlements" refer to the permissions and access levels granted to users, which are crucial in controlling and monitoring the actions of privileged users. "Relationships" can also pertain to the interactions between accounts and their required access, which is important for managing risks associated with privileged accounts. Thus, job rotation is not inherently linked to the specific management principles of

6. In the context of risk assessment, what is a primary focus?

A. Only physical security threats.

B. Balancing costs versus potential impact of risks.

C. Ensuring all employees follow security protocols.

D. Merging risk management with operational efficiency.

The primary focus in the context of risk assessment is balancing costs versus potential impact of risks. This approach is foundational in risk management as it requires organizations to evaluate the likelihood of various risks occurring and the potential consequences of those risks, which can include financial loss, reputational damage, or operational disruptions. By assessing both costs and impacts, organizations can make informed decisions about which risks to mitigate, which to accept, and how to allocate resources effectively. This risk-based decision-making process ensures that the organization's security measures are proportionate to the actual risks it faces, leading to more efficient and effective use of resources. In contrast, focusing solely on physical security threats limits the risk assessment process by ignoring other critical aspects such as cyber threats or operational vulnerabilities. Ensuring all employees follow security protocols, while essential for a robust security posture, addresses compliance rather than the risk assessment process itself. Merging risk management with operational efficiency is a valid consideration, but it does not capture the core objective of risk assessment, which is primarily concerned with evaluating risks and their impacts in relation to costs.

7. In risk management, what does a risk mitigation strategy involve?

A. Actions designed to eliminate all risks

B. Actions taken to reduce the likelihood or impact of a risk

C. Creating insurance policies for all risks

D. Developing recovery plans post-incident

A risk mitigation strategy is fundamentally concerned with reducing both the likelihood of a risk occurring and the potential impact it could have on an organization. This approach is proactive, aiming to lessen adverse effects through various measures such as implementing safeguards, strengthening security controls, or modifying processes. For example, if an organization identifies that its network is susceptible to cyber-attacks, possible risk mitigation strategies might include enhancing firewalls, applying software patches, and providing employee training on security protocols. Such actions do not aim to eliminate all risks entirely, which is why the first option is not suitable. Risk can never be fully eradicated; rather, the objective is to manage and minimize it effectively. Creating insurance policies, while a way to manage financial exposure from risks, does not directly address the risk itself but rather transfers the financial consequences of risks. This is why relying on insurance alone does not constitute a comprehensive risk mitigation strategy. Furthermore, developing recovery plans post-incident is focused on responding to risks after they have occurred rather than actively preventing or reducing them in advance. Hence, while recovery plans are essential components of overall risk management, they do not belong to the proactive measures associated with risk mitigation. In summary, a risk mitigation strategy is primarily about taking deliberate actions aimed at

8. What is an inappropriate method for evaluating personnel for security risks?

A. A. Driving record review

B. B. Passport number verification and validation

C. C. Drug and substance testing

D. D. Education, licensing, and certification verification

In evaluating personnel for security risks, it is essential to rely on methods that effectively identify potential vulnerabilities that may affect the security posture of an organization. Passport number verification and validation does not directly assess an individual's behavior, character, or reliability in a professional context related to security risks. Instead, it primarily confirms identity and travel eligibility, which is less relevant for evaluating someone's trustworthiness or suitability for roles that involve sensitive information or security responsibilities. In contrast, elements such as a driving record review, drug and substance testing, and verification of education, licensing, and certification are more pertinent to security assessments. Driving records can reveal risky behaviors that may correlate with reliability, while drug testing can identify substance abuse that could impair judgment or performance. Additionally, validating someone's education and professional credentials ensures that they possess the necessary qualifications and ethical grounding for their role. Overall, employing ineffective methods for assessing security risks, such as passport verification, fails to provide a meaningful evaluation of an individual's propensity for risk-related behavior in their job functions.

9. Which of the following is NOT considered a significant threat from employees to information systems?

A. IT sabotage

B. Fraud

C. Theft of intellectual property

D. Logic bombs

The correct answer identifies that logic bombs are not typically categorized as a significant threat from employees compared to the other options. Logic bombs are a form of malicious code that execute under specific conditions, and while they can indeed pose a threat, they are often more associated with external attackers or could be the result of malicious software from unauthorized sources rather than a direct action taken by an employee. In contrast, IT sabotage, fraud, and theft of intellectual property represent more common employee-related risks. Employees with access to sensitive systems and information may exploit their privileges to engage in sabotage, manipulating or destroying data intentionally, leading to significant operational disruptions. Fraud entails the misuse of corporate resources for personal gain, which employees are often in a position to commit. Similarly, employees may have the ability to access and misappropriate intellectual property, which can lead to substantial competitive and financial losses for an organization. These threats stem from insiders who are familiar with the organization's systems and processes, making them particularly dangerous as they may bypass conventional security measures. In conclusion, while logic bombs are certainly a concern in cyber security, they do not specifically align with the common and significant threats posed by employees.

10. Consistent implementation of security configurations throughout an organization is known as:

A. Auditing.

B. Valid implementation.

C. Baselines.

D. Configuration management.

The correct answer is that consistent implementation of security configurations throughout an organization is known as baselines. A baseline represents a set of minimum security controls or configurations that are established to ensure that all systems maintain a standard level of security. By establishing these baselines, organizations can ensure uniformity in how security measures are applied across different systems and devices, which is critical for reducing vulnerabilities and enhancing overall security posture. Baselines help organizations streamline their security processes and ensure compliance with regulations, as they provide a reference point for audits and assessments. When security configurations align with these predefined baselines, it indicates that the organization is effectively managing its security posture and enforcing policies consistently. In contrast, while auditing is the process of reviewing and verifying whether policies, procedures, and controls are being followed, it does not inherently guarantee that configurations are consistently implemented. Valid implementation refers to the successful deployment of configurations but does not capture the aspect of consistency across the organization. Configuration management involves maintaining and overseeing security configurations but focuses more broadly on managing changes and maintaining system integrity rather than just ensuring consistent application.