Federal IT Security Professional (FITSP) Auditor Practice Exam (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. Which of the following is an example of Tier 1 risk?

A. Technological Innovation

B. Cost, Schedule, Performance

C. Public Relations

D. User Satisfaction

2. Applying the first three steps in the RMF to legacy systems can be viewed as a _____ to determine if the necessary and sufficient security controls have been appropriately selected and allocated.

A. Risk Assessment

B. Due Diligence

C. Gap Analysis

D. Capital Planning

3. What is the basis for the identification of information types?

A. Business Reference Model

B. Mission-Specific Function

C. Management Support Category

D. Performance Reference Model

4. Under FISMA 2014, which agencies are formally assigned information security responsibilities?

A. Commerce and Justice

B. DHS and OMB

C. FBI and NSA

D. State and Treasury

5. What are the two most important factors when selecting a security control assessor?

A. Independence/Expertise

B. Trustworthiness/Experience

C. Expertise/Trustworthiness

D. Experience/Independence

6. What is the FIPS publication that specifies the Rijndael algorithm?

A. FIPS 197

B. FIPS 198

C. FIPS 199

D. FIPS 200

7. Which contingency planning variable defines the maximum time a resource can be unavailable before it impacts operations?

A. RPO

B. MTTF

C. RTO

D. RFP

8. What are the two key components affecting the trustworthiness of information systems?

A. Confidentiality and Integrity

B. Security functionality and Security assurance

C. Availability and Accountability

D. Governance and Risk management

9. Which agency is responsible for publishing FISMA Reporting Metrics annually?

A. OMB

B. Commerce

C. Justice

D. DHS

10. What is the purpose of using Message Authentication Codes between parties?

A. To encrypt data

B. To authenticate data transmission

C. To sign messages

D. To compress data

Answers

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

Explanations

1. Which of the following is an example of Tier 1 risk?

A. Technological Innovation

B. Cost, Schedule, Performance

C. Public Relations

D. User Satisfaction

In the context of risk management, Tier 1 risks are typically the most significant risks that can impact an organization's ability to meet its objectives. These risks generally relate to the fundamental aspects of project management, including cost, schedule, and performance. Choosing cost, schedule, and performance as an example of Tier 1 risk highlights the critical nature of these elements in project and program success. If a project consistently goes over budget, misses deadlines, or fails to deliver the expected performance outcomes, it can jeopardize the overall goals of the initiative and the organization's strategic objectives. Tier 1 risks are often prioritized because they require immediate attention and management to prevent substantial negative impacts. In contrast, while technological innovation, public relations, and user satisfaction are also important considerations for organizations, they are typically classified as Tier 2 or Tier 3 risks. These risks are still relevant but may not have the same immediate and fundamental impact on the core operational aspects of a project as cost, schedule, and performance-related risks. Understanding this hierarchy helps organizations prioritize their risk management efforts effectively.

2. Applying the first three steps in the RMF to legacy systems can be viewed as a _____ to determine if the necessary and sufficient security controls have been appropriately selected and allocated.

A. Risk Assessment

B. Due Diligence

C. Gap Analysis

D. Capital Planning

Conducting a gap analysis is crucial when applying the first three steps of the Risk Management Framework (RMF) to legacy systems. A gap analysis allows organizations to evaluate existing security controls against the required standards and best practices, identifying any deficiencies or areas that do not meet current security requirements. In this context, the first three steps of the RMF—categorizing the information system, selecting security controls, and implementing those controls—provide a foundational structure. By performing a gap analysis, an organization can ascertain whether the selected and implemented controls are both necessary and sufficient for the unique risks and characteristics of the legacy system. This process not only highlights areas where controls may be lacking but also facilitates informed decision-making about enhancements or updates needed to mitigate identified risks. The goal is to ensure that the legacy system aligns with current security practices and adequately protects against potential threats. The other options do not capture the specific nature of evaluating the suitability of existing security measures in comparison to required standards. Risk assessment primarily focuses on identifying and examining risks rather than evaluating control adequacy. Due diligence typically refers to the necessary investigation or audit processes before making business decisions and does not specifically apply to evaluating existing security controls. Capital planning deals with financial resources allocated for projects and does not

3. What is the basis for the identification of information types?

A. Business Reference Model

B. Mission-Specific Function

C. Management Support Category

D. Performance Reference Model

The Business Reference Model (BRM) is a key framework utilized for identifying information types within an organization. It categorizes various aspects of business operations, allowing organizations to conceptualize and map out their functions. The model emphasizes the processes and activities that deliver value, and it helps in identifying and classifying information types according to the needs of the business and its operational processes. This framework not only supports the understanding of how different functions interact but also aids in the alignment of information management with organizational goals. By establishing a clear relationship between business processes and the types of information required, organizations can effectively manage and secure their data assets. Other options, while relevant to broader organizational frameworks or specific functions, do not provide the comprehensive foundation used for identifying and categorizing information types in the same way the Business Reference Model does.

4. Under FISMA 2014, which agencies are formally assigned information security responsibilities?

A. Commerce and Justice

B. DHS and OMB

C. FBI and NSA

D. State and Treasury

Under the Federal Information Security Management Act (FISMA) of 2014, the Department of Homeland Security (DHS) and the Office of Management and Budget (OMB) have been formally assigned significant information security responsibilities. This is due, in part, to their roles in overseeing the federal government's overall cybersecurity strategy and implementation. The DHS is responsible for coordinating the government's efforts to secure its IT infrastructure and ensuring that agencies adhere to cybersecurity practices and standards. This includes conducting assessments, providing guidance, and responding to incidents. The OMB, on the other hand, plays a crucial role in the budgetary aspects and compliance oversight of information security initiatives across federal agencies, enforcing policies that support federal information security programs and promoting best practices. This assignment of responsibilities ensures that there is a cohesive and coordinated approach to cybersecurity across various government sectors, particularly in safeguarding sensitive information and protecting critical infrastructure. The strategy laid out under FISMA emphasizes the collaborative nature required to effectively manage information security risks across diverse agencies.

5. What are the two most important factors when selecting a security control assessor?

A. Independence/Expertise

B. Trustworthiness/Experience

C. Expertise/Trustworthiness

D. Experience/Independence

Selecting a security control assessor is critical for ensuring the effectiveness and integrity of an organization's security posture. Independence and expertise stand out as the two most important factors in this selection process. Independence is crucial because it ensures that the assessment is unbiased. An independent assessor can provide an objective evaluation without any conflicts of interest that might arise if they were closely tied to the organization's operations or security team. This objectivity is vital for fostering trust in the assessment's findings and recommendations, allowing for a transparent evaluation of the security controls in place. Expertise is equally important, as a competent security control assessor must possess extensive knowledge and experience in evaluating security frameworks, compliance requirements, and best practices. Their expertise enables them to identify vulnerabilities and weaknesses effectively, ensuring that all relevant aspects of the security controls are scrutinized thoroughly. This proficiency also means they can offer valuable insights and recommendations based on industry standards and past experiences. Together, independence and expertise create a strong foundation for a security control assessment, leading to actionable insights and improvements in an organization's security posture.

6. What is the FIPS publication that specifies the Rijndael algorithm?

A. FIPS 197

B. FIPS 198

C. FIPS 199

D. FIPS 200

FIPS 197 is the publication that specifies the Rijndael algorithm, which is widely known as the Advanced Encryption Standard (AES). This standard was adopted by the National Institute of Standards and Technology (NIST) after a public competition to find a suitable replacement for the Data Encryption Standard (DES). The Rijndael algorithm, which was designed by Belgian cryptographers Joan Daemen and Vincent Rijmen, was selected because of its strong security capabilities and efficiency in processing. FIPS 197 details the technical specifications and requirements for implementing the Rijndael algorithm as a cryptographic standard for federal use. It outlines key aspects such as the algorithm's structure, its encryption and decryption processes, key sizes, and the block size, which ultimately provides a framework that ensures the protection of sensitive government data. The other FIPS publications mentioned do not pertain to the Rijndael algorithm. FIPS 198 deals with the HMAC (Hash-based Message Authentication Code) standard, FIPS 199 covers standards for security categorization of federal information and information systems, and FIPS 200 outlines minimum security requirements for federal information and information systems. Therefore, when looking for the publication that specifically describes the Rijndael algorithm, FIPS 197 is the

7. Which contingency planning variable defines the maximum time a resource can be unavailable before it impacts operations?

A. RPO

B. MTTF

C. RTO

D. RFP

The concept being addressed in this question revolves around contingency planning and the measures related to resource availability during a disruption. The correct answer relates to the Recovery Time Objective (RTO), which is a crucial metric in business continuity planning. RTO defines the maximum acceptable downtime for a resource or service before it begins to negatively affect operational capabilities. Essentially, it indicates the target time set for the recovery of IT and business activities after a disruption has occurred. Understanding the RTO helps organizations prioritize their recovery strategies and ensures that critical operations can be restored within a timeframe that minimizes adverse effects on the organization. In contrast, the other options pertain to different yet related concepts in disaster recovery and incident management. For instance, RPO, or Recovery Point Objective, deals with the maximum age of the data that can be lost in the event of a disruption, focusing specifically on data loss rather than operational downtime. MTTF, or Mean Time to Failure, refers to the average time until a system fails, and RFP is not a standard term typically used in this context. Each of these plays a role in overall recovery strategies, but only RTO specifically addresses the time limitations related to operational impact during resource unavailability.

8. What are the two key components affecting the trustworthiness of information systems?

A. Confidentiality and Integrity

B. Security functionality and Security assurance

C. Availability and Accountability

D. Governance and Risk management

The two key components affecting the trustworthiness of information systems are security functionality and security assurance. Security functionality refers to the measures and controls implemented within an information system to protect it from threats and vulnerabilities. This includes the various security features and capabilities that help ensure the system operates securely, such as access controls, encryption, and intrusion detection systems. Security assurance, on the other hand, pertains to the confidence that stakeholders have in the system's ability to protect its assets and perform its functions reliably. It involves the processes that assess, evaluate, and certify that the security mechanisms are effective and properly implemented. Assurance can be gained through audits, testing, and certifications that verify the system adheres to security standards and best practices. These two components work together to create a comprehensive trust model for information systems, ensuring they not only possess necessary security measures but also that these measures are effective and can be relied upon by users and stakeholders.

9. Which agency is responsible for publishing FISMA Reporting Metrics annually?

A. OMB

B. Commerce

C. Justice

D. DHS

The correct answer reflects that the Department of Homeland Security (DHS) is responsible for publishing FISMA (Federal Information Security Modernization Act) Reporting Metrics annually. This is important because FISMA requires federal agencies to develop, document, and implement an information security program, and consistency in reporting metrics is vital for assessing the overall security posture of these agencies. DHS's role in this process includes collecting data from other federal agencies about their cybersecurity practices and compliance with FISMA mandates. By publishing these metrics, DHS aids in creating a standardized approach to reporting and analyzing federal information security efforts, which ultimately helps to enhance the security framework across government entities. The role of other agencies in this context differs. While the Office of Management and Budget (OMB) and other departments like Commerce and Justice may have their responsibilities relating to information security policy and oversight, they do not specifically handle the annual publication of FISMA Reporting Metrics. Their functions are typically more broad-ranging and include oversight and guidance rather than the specific task of metric publication.

10. What is the purpose of using Message Authentication Codes between parties?

A. To encrypt data

B. To authenticate data transmission

C. To sign messages

D. To compress data

Using Message Authentication Codes (MACs) between parties serves the essential purpose of authenticating data transmission. A MAC provides a mechanism for ensuring both the integrity and authenticity of a message. It does this by allowing the sender to generate a code based on the message content and a secret key, which is then sent along with the message. The recipient, who also knows the secret key, can compute the MAC for the received message and compare it to the MAC that accompanied the message. If they match, the recipient can be assured that the message has not been altered during transmission and that it indeed came from the legitimate sender. This process is crucial in secure communications, as it helps to prevent data tampering and ensure that the message's origin is verified. It is important to note that while MACs contribute to the integrity and authenticity of data, they are not concerned with confidentiality; thus, they do not encrypt the data itself. Therefore, the purpose of using MACs centers on validating the authenticity of data exchanges, making it a critical component of secure communications between parties.