CompTIA Security+ Practice Exam (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. Which type of device provision allows both work-related and personal use?

A. Corporate-Owned, Business Only

B. Corporate-Owned, Personally-Enabled

C. Choose Your Own Device

D. Wearable Technology

2. What describes an incremental approach where steps are followed in sequential order?

A. Spiral

B. Waterfall

C. Agile

D. Iterative Development

3. What type of solution runs applications on servers located in a centralized location?

A. Terminal Services

B. Cloud Applications

C. Application Layering

D. Remote Application Services

4. What is the primary purpose of advisory policies in an organization?

A. To enforce compliance with regulations

B. To provide guidance for acceptable activities

C. To detail technical specifications

D. To manage financial expenditures

5. What implementation prevents printing to networked or USB-connected printers?

A. Print blocking

B. Clipboard restrictions

C. Network isolation

D. Access control lists

6. Which term refers to a more extreme process of making sure data is not recoverable after removal?

A. Data Removal

B. Data Destruction

C. Data Retention

D. Data Preservation

7. What term describes data that remains intact after a power loss?

A. Persistent

B. Non-Persistent

C. Volatile

D. Temporary

8. What technology retrieves an item from a database without revealing which item is retrieved?

A. Data Masking

B. Private Information Retrieval (PIR)

C. Access Control

D. Data Minimization

9. What does the Requirements Definition document outline?

A. Testing results and strategies

B. Application architecture and its components

C. Functional requirements and security needs

D. Product marketing strategies

10. What term is associated with the British Invasion of German-occupied territories?

A. Declassification

B. Data format

C. Bigot

D. Confidential

Answers

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

Explanations

1. Which type of device provision allows both work-related and personal use?

A. Corporate-Owned, Business Only

B. Corporate-Owned, Personally-Enabled

C. Choose Your Own Device

D. Wearable Technology

The choice that allows both work-related and personal use is Corporate-Owned, Personally-Enabled. This provisioning model typically refers to a scenario where the organization owns the devices but allows employees to use them for personal activities as well. It strikes a balance between securing corporate data and providing flexibility and convenience for employees, enabling them to integrate their work and personal lives more seamlessly. In this approach, organizations can implement security policies and management controls without completely isolating users from personal usage, which can enhance employee satisfaction and productivity. Additionally, it facilitates easier maintenance and updates since the organization retains ownership of the devices. Other choices may not offer the same level of flexibility. For example, Corporate-Owned, Business Only is geared towards business use only, meaning personal activities could be restricted. The Choose Your Own Device model typically allows employees to use their personal devices for work, but it does not imply that the devices are corporate-owned. Meanwhile, Wearable Technology refers to specific types of devices and does not inherently imply any provisioning model regarding work and personal use.

2. What describes an incremental approach where steps are followed in sequential order?

A. Spiral

B. Waterfall

C. Agile

D. Iterative Development

The Waterfall model is characterized by its linear and sequential approach to software development and project management. In this methodology, the project is divided into distinct phases, where each phase must be completed before the next one begins. These phases typically include requirements gathering, design, implementation, testing, deployment, and maintenance. The key characteristic of the Waterfall approach is that each step must be finished before moving on to the subsequent step, which creates a structured progression through the project. This is in contrast to more flexible methodologies like Agile, which allow for overlapping phases and continuous improvement based on feedback. This sequential flow aids in clearly defining project milestones and deliverables at each stage. It is particularly effective in environments where project requirements are well understood upfront and unlikely to change throughout the development process.

3. What type of solution runs applications on servers located in a centralized location?

A. Terminal Services

B. Cloud Applications

C. Application Layering

D. Remote Application Services

The correct choice is Terminal Services because it specifically refers to a technology that enables users to run applications on centralized servers and access them remotely from their own devices. This model allows multiple users to work with applications hosted on a server, rather than requiring each user to install and run the software on their individual machines. Terminal Services works by creating a session for each user on the server, and any input is sent to the server while the server processes the tasks and sends back the display outputs to the user's device. This central management improves resource utilization, simplifies software updates, and enhances security since sensitive data can be kept on the server rather than distributed across various endpoints. While Cloud Applications do involve centralized application access, they usually embody software as a service (SaaS) that is hosted in the cloud, which may not distinctly use the concept of sessions as Terminal Services does. Application Layering focuses on creating modular applications that can be dynamically assigned and provisioned but does not imply a centralized execution on servers like Terminal Services. Remote Application Services is somewhat vague but generally refers to technologies allowing remote access to applications, which encompasses a broader range of solutions, making Terminal Services the more accurate answer for the specific scenario described.

4. What is the primary purpose of advisory policies in an organization?

A. To enforce compliance with regulations

B. To provide guidance for acceptable activities

C. To detail technical specifications

D. To manage financial expenditures

The primary purpose of advisory policies in an organization is to provide guidance for acceptable activities. These policies serve as a framework for employees and stakeholders, outlining the expected behaviors and practices within the organization without being mandatory like compliance policies. They help create a shared understanding of what is considered appropriate or best practice in various situations. Advisory policies are particularly valuable because they promote consistency and enhance decision-making processes among staff. They help in shaping the culture of the organization by encouraging employees to adhere to certain standards and values, which facilitates a more cohesive and efficient work environment. While other types of policies, such as those focused on compliance, technical specifications, or financial management, have their specific roles, advisory policies are centered around guiding conduct and decision-making rather than enforcing rules.

5. What implementation prevents printing to networked or USB-connected printers?

A. Print blocking

B. Clipboard restrictions

C. Network isolation

D. Access control lists

Print blocking is a security implementation specifically designed to prevent printing to both networked and USB-connected printers. This measure is often used in organizations to protect sensitive information from being inadvertently printed and left unsecured. By disabling printing capabilities on certain devices or networks, organizations can minimize the risk of data leakage. In environments where sensitive data is handled, restricting print capabilities can help ensure that confidential information does not get exposed through hard copies, which can be easily accessed or misplaced. Print blocking can be implemented through various software solutions that manage print jobs and enforce printing policies based on user roles or classification of the material. The other options, while they have their own security functions, do not directly relate to preventing printing capabilities. Clipboard restrictions are focused on controlling data copied to the clipboard, network isolation pertains to separating networks for security purposes, and access control lists are used to manage permissions and access rights to resources, but none specifically block printing outputs.

6. Which term refers to a more extreme process of making sure data is not recoverable after removal?

A. Data Removal

B. Data Destruction

C. Data Retention

D. Data Preservation

The term that refers to a more extreme process of ensuring that data is not recoverable after removal is data destruction. This process goes beyond merely deleting files; it involves methods that render the data completely irretrievable. Data destruction can involve physical methods, such as shredding hard drives, or logical methods, such as overwriting data with random information multiple times to prevent recovery. This practice is crucial for sensitive information, especially in contexts where data breaches could have significant repercussions, such as in healthcare, finance, or when complying with legal regulations like GDPR or HIPAA. The key aspect that distinguishes data destruction from other options is its focus on the finality of data removal and assurance that no residual data can be recovered. On the other hand, data removal, while it may imply deleting files or data from a storage medium, does not necessarily imply that the data is completely irrecoverable. Data retention and data preservation refer to keeping data available for a certain period for future use or legal compliance, which is contrary to the goal of destruction.

7. What term describes data that remains intact after a power loss?

A. Persistent

B. Non-Persistent

C. Volatile

D. Temporary

The term that describes data that remains intact after a power loss is "persistent." Persistent data is stored in non-volatile memory or storage, such as hard drives, SSDs, or databases, where it is retained even when the device is powered down. This characteristic is crucial for data integrity, as it ensures that important information is not lost during power outages or system reboots. Having persistent data allows systems to recover from failures and continue to operate without losing prior information. In contrast, including options like non-persistent, volatile, and temporary data refer to data types that do not retain their state after losing power. Non-persistent data typically refers to information that is not saved and is usually transient. Volatile data is specifically stored in RAM, which loses all stored information once power is off. Temporary data is often used for immediate tasks but is not meant to be stored long-term or retained after shutdown.

8. What technology retrieves an item from a database without revealing which item is retrieved?

A. Data Masking

B. Private Information Retrieval (PIR)

C. Access Control

D. Data Minimization

Private Information Retrieval (PIR) is a technology designed specifically to enable a user to retrieve data from a database without exposing which particular data item is being accessed. This is accomplished through cryptographic techniques that ensure the privacy of the query, thereby allowing the user to obtain information without revealing their search intentions to the database owner or any observing parties. PIR is particularly important in scenarios where confidentiality is critical, such as in personal medical records or sensitive financial information. By using PIR, users can maintain their privacy while still accessing the necessary data, which is essential in today's data-driven world where information security is paramount. This technology is vital for protecting against potential misuse of query information and ensures that the user's actions remain anonymous. In contrast, the other options relate to different aspects of data security but do not specifically address the retrieval of data while maintaining the privacy of the query itself. Data Masking is focused on obscuring data to protect sensitive information, Access Control pertains to user permissions and rights to access data, and Data Minimization emphasizes limiting data collection to only what is necessary. While all these concepts are important in the realm of data security, they do not fulfill the specific function that Private Information Retrieval is designed for.

9. What does the Requirements Definition document outline?

A. Testing results and strategies

B. Application architecture and its components

C. Functional requirements and security needs

D. Product marketing strategies

The Requirements Definition document serves as a foundational element in the development process, and its primary focus is on detailing the functional requirements and security needs of a system or application. This document is crucial as it lays out what the end-users expect the system to accomplish and how it should protect sensitive data from potential threats. By articulating functional requirements, the document ensures that developers understand what features and capabilities the system must include to meet user needs. It also addresses security requirements, identifying necessary safeguards and compliance standards that the application must adhere to. This comprehensive framework helps align the project's goals with user expectations and security protocols, ensuring a cohesive development process. While testing results and strategies, application architecture, and product marketing strategies are important aspects of a project, they do not directly reside within the focus of a Requirements Definition document. Such elements are typically developed in separate documentation that addresses those specific areas of the project lifecycle.

10. What term is associated with the British Invasion of German-occupied territories?

A. Declassification

B. Data format

C. Bigot

D. Confidential

The term "bigot" in the context of military operations such as the British Invasion of German-occupied territories refers to a specific security classification used during World War II. In this military vernacular, "bigot" indicated that certain information was restricted and should only be accessed by personnel who were "bigoted"—in other words, those who had been cleared and were authorized to participate in sensitive operations. This classification was crucial for maintaining operational security, as it protected crucial and potentially vulnerable information from being disclosed to unauthorized personnel, thus preventing compromise of military strategies and deployments. The use of "bigot" helps to highlight the importance of information control in military contexts, where trust and security are paramount to ensure successful operations. The other terms presented do not relate specifically to military classification or operations in the same direct manner. "Declassification" pertains to the process of removing confidentiality from information, "data format" refers to the structure in which data is stored or transmitted, and "confidential" is a general term used for information that is not meant to be shared publicly. Thus, "bigot" stands out as the most relevant term associated with the scenario described in the question.