Certified CMMC Assessor (CCA) Practice Exam (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. **What should interviews conducted during an assessment demonstrate?**
   - **A. Financial investment in security tools**
   - **B. All levels of management approval**
   - **C. Implementation and performance of relevant processes**
   - **D. Knowledge of the assessment protocol**

2. **What is the function of a RADIUS server in accessing wireless networks?**
   - **A. To monitor internet traffic**
   - **B. To provide centralized authentication for users**
   - **C. To manage shared passwords across devices**
   - **D. To restrict access based on device type**

3. **Which organization produces the CMMC doctrine that guides assessment procedures?**
   - **A. National Security Agency**
   - **B. Department of Defense**
   - **C. The Cyber AB**
   - **D. Federal Trade Commission**

4. **In the context of CMMC, what primarily defines 'logical access'?**
   - **A. Physical security measures**
   - **B. Software mechanisms that control data flow**
   - **C. Human oversight of systems**
   - **D. Monitoring equipment for vulnerabilities**

5. **Which term refers to the scope of the system and environment being assessed?**
   - **A. Data sensitivity**
   - **B. System Boundary**
   - **C. Operational Technology**
   - **D. Asset Coverage**

6. What does the CMMC requirement for system baselining aim to ensure?

- **A. Consistent and secure configuration management**
- **B. Immediate access for all users**
- **C. Prevention of all communications**
- **D. Elimination of change control**

7. What does the practice AC.L2-3.1.8 require organizations to define in relation to logon attempts?

- **A. The number of successful logon attempts**
- **B. The number of device connections allowed**
- **C. The number of unsuccessful logon attempts and subsequent actions**
- **D. The number of user accounts created**

8. What does SI.L2-3.14.5 emphasize about scanning systems and files?

- **A. All files must be manually reviewed**
- **B. Periodic and real-time scans for malicious code**
- **C. Scans should be avoided during business hours**
- **D. Only external files need to be scanned**

9. Which of the following best describes the Internet of Things (IoT)?

- **A. A collection of software applications**
- **B. A network of interconnected devices exchanging data**
- **C. An isolated computing environment**
- **D. A system for managing traditional IT operations**

10. What is required for an artifact to be considered acceptable evidence in a CMMC assessment?

- **A. It must be documented by an external auditor**
- **B. It must demonstrate combat readiness**
- **C. It must show implementation of relevant processes**
- **D. It must be signed by organizational leadership**

Answers

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

Explanations

1. What should interviews conducted during an assessment demonstrate?

A. Financial investment in security tools

B. All levels of management approval

C. Implementation and performance of relevant processes

D. Knowledge of the assessment protocol

Interviews conducted during an assessment are designed to evaluate the implementation and performance of relevant processes. This is crucial because the primary goal of these interviews is to gather insights into how well an organization adheres to established security practices and policies. By focusing on the implementation aspect, the assessment can gauge whether the processes are not only in place but are also functioning effectively. Understanding performance is vital as it reveals if the organization's security controls are actively mitigating risks and contributing to their cybersecurity posture. Interviewing various personnel allows assessors to see firsthand the alignment between documented procedures and actual practices. This, in turn, informs the overall assessment of compliance with CMMC standards and helps identify areas for improvement. While knowledge of the assessment protocol, levels of management approval, and financial investment in security tools are relevant topics, they do not directly address the effectiveness and operational status of the security processes being evaluated. Thus, focusing on the implementation and performance of relevant processes provides the most pertinent information during an assessment.

2. What is the function of a RADIUS server in accessing wireless networks?

A. To monitor internet traffic

B. To provide centralized authentication for users

C. To manage shared passwords across devices

D. To restrict access based on device type

The function of a RADIUS server in accessing wireless networks primarily involves providing centralized authentication for users. RADIUS, which stands for Remote Authentication Dial-In User Service, is a networking protocol that facilitates user authentication, authorization, and accounting (AAA) for access to networks. When a user attempts to connect to a wireless network, the RADIUS server verifies the user's credentials—usually through a username and password or other authentication methods. This centralized approach allows network administrators to manage user access efficiently, ensuring that only authenticated users can connect to the network. It is particularly beneficial in environments with multiple access points, as it allows for consistent security policies and user management across the entire network. This functionality is critical for maintaining security in wireless networks, as it prevents unauthorized access and helps to manage user identities effectively. Centralized authentication also simplifies scaling, as adding new users or updating credentials can be done in one place rather than on each individual access point. Other options, while relevant to aspects of network management, do not accurately capture the primary role of a RADIUS server in the context of wireless network access.

3. Which organization produces the CMMC doctrine that guides assessment procedures?

A. National Security Agency

B. Department of Defense

C. The Cyber AB

D. Federal Trade Commission

The correct answer is that The Cyber AB produces the CMMC doctrine that guides assessment procedures. The Cyber AB, formally known as the Cybersecurity Maturity Model Certification Accreditation Body, is responsible for maintaining the CMMC program and ensuring that it effectively enhances security practices within the defense industrial base. This organization develops not only the framework of the CMMC but also the necessary documentation, guidance, and training for assessors and organizations seeking certification. Understanding the role of The Cyber AB is crucial for comprehending how the CMMC operates. It serves as the central authority responsible for evolving the CMMC standards and ensuring that they meet the needs of the Department of Defense and the broader cybersecurity landscape. This includes refining the assessment processes that organizations must undergo to achieve compliance. On the other hand, while the Department of Defense is the overarching entity that established the need for CMMC to secure the defense supply chain, it does not create the assessment protocols itself. The National Security Agency and the Federal Trade Commission also do not play a direct role in CMMC doctrine formulation; their functions pertain to broader national security and consumer protection, respectively.

4. In the context of CMMC, what primarily defines 'logical access'?

A. Physical security measures

B. Software mechanisms that control data flow

C. Human oversight of systems

D. Monitoring equipment for vulnerabilities

The primary definition of 'logical access' in the context of CMMC pertains to the use of software mechanisms that control access to data and systems. Logical access involves the regulations and tools that determine who can access information, what information can be accessed, and how that access is managed through user identification, authentication, and authorization processes. These software controls play a critical role in protecting sensitive information within an organization, as they establish permissions and restrictions based on user roles and security policies. This ensures that only those who are properly authorized can access or manipulate the data, thereby maintaining the confidentiality, integrity, and availability of critical information assets. In contrast, other aspects such as physical security measures are more concerned with protecting the physical assets and environments where data is stored and processed, not necessarily the logical structures governing access to data. Similar distinctions apply to human oversight, which focuses on monitoring and administrative functions, and to monitoring equipment for vulnerabilities, which addresses the technology used to detect weaknesses but does not directly relate to the mechanisms that specifically control access.

5. Which term refers to the scope of the system and environment being assessed?

A. Data sensitivity

B. System Boundary

C. Operational Technology

D. Asset Coverage

The term that refers to the scope of the system and environment being assessed is "System Boundary." This concept is critical in information security and compliance frameworks like the Cybersecurity Maturity Model Certification (CMMC), as it defines the limits of the system under review. A clear understanding of the system boundary helps assessors determine which components of the information system are included in the assessment, ensuring that all relevant assets, processes, and data are considered. By establishing the system boundary, organizations can identify what falls under their security protocols and compliance efforts, helping to mitigate risks effectively. This clarity is vital not only for compliance but also for resource allocation, as it allows organizations to focus their security measures where they are most needed. In contrast, while data sensitivity refers to the classification of data based on its importance and the level of protection required, it's not the same as defining the system's scope. Operational technology pertains to hardware and software systems that detect or control physical devices, which is not directly related to the assessment boundary. Asset coverage may refer to how comprehensively an organization's assets are managed or protected, but it does not specifically denote the scope of the system undergoing assessment. Thus, the specificity of "System Boundary" makes it the correct term in this context.

6. What does the CMMC requirement for system baselining aim to ensure?

A. Consistent and secure configuration management

B. Immediate access for all users

C. Prevention of all communications

D. Elimination of change control

The requirement for system baselining within the Cybersecurity Maturity Model Certification (CMMC) framework is focused on achieving consistent and secure configuration management throughout an organization’s systems. Baselining refers to the process of establishing a standard for the desired state of a system’s configuration. This standard includes the configuration settings, hardware, software, and other components of the system that are deemed secure. By establishing a baseline, organizations can effectively monitor deviations from this standard, which helps in identifying potential security vulnerabilities and misconfigurations. It ensures that all components of a system are configured correctly, thereby reducing the risk of exploitation by malicious actors. Moreover, consistent configuration management aligns with best practices for maintaining system integrity, availability, and confidentiality, which are critical aspects of cybersecurity. This approach does not favor immediate access for all users, as user access controls are critical for maintaining security. It also does not support the idea of preventing all communications, which would hinder operational functionality. Lastly, eliminating change control would be detrimental to maintaining a secure and stable environment, as managing changes effectively is vital for safeguarding systems against security threats. Thus, the correct choice emphasizes the importance of consistent and secure configuration management achieved through systematic baselining.

7. What does the practice AC.L2-3.1.8 require organizations to define in relation to logon attempts?

A. The number of successful logon attempts

B. The number of device connections allowed

C. The number of unsuccessful logon attempts and subsequent actions

D. The number of user accounts created

The practice AC.L2-3.1.8 focuses on the importance of monitoring and responding to logon attempts to enhance security within an organization. Specifically, it requires organizations to define the number of unsuccessful logon attempts allowed and the subsequent actions that should be taken if that threshold is reached. This practice aims to mitigate risks associated with unauthorized access attempts and potential brute-force attacks. By establishing a clear protocol for managing unsuccessful logon attempts, organizations can ensure they have an effective response strategy in place, such as locking accounts after a certain number of failed attempts, notifying users of suspicious activity, or triggering security alerts. This proactive approach helps protect sensitive assets and information by discouraging repeated unauthorized access attempts. In contrast, simply monitoring successful logon attempts does not provide insights into potential security threats. The options related to device connections and the number of user accounts created do not focus on the process of managing access attempts, which is central to maintaining robust access controls and a secure environment. Thus, defining actions related to unsuccessful logon attempts directly aligns with best practices in access control management as required by the CMMC framework.

8. What does SI.L2-3.14.5 emphasize about scanning systems and files?

A. All files must be manually reviewed

B. Periodic and real-time scans for malicious code

C. Scans should be avoided during business hours

D. Only external files need to be scanned

The correct answer emphasizes the importance of conducting periodic and real-time scans for malicious code. This practice is crucial for maintaining the integrity and security of information systems within an organization. Regular scanning helps in early detection of potential threats and vulnerabilities, ensuring that malicious software is identified and addressed promptly to prevent any damage or data breaches. Implementing both periodic and real-time scans creates multiple layers of defense, allowing organizations to not only react to current threats but also to anticipate and mitigate future risks. This proactive approach to cybersecurity is a key component of effective risk management and supports the overall goal of safeguarding sensitive information. The other options do not align with the practices outlined in the CMMC framework. For instance, requiring manual reviews for all files would be inefficient and impractical in most scenarios, especially given the volume of files that organizations handle. Avoiding scans during business hours could leave systems vulnerable during peak operational times. Lastly, limiting scans to only external files ignores the necessity of scanning internal files, which can also harbor threats.

9. Which of the following best describes the Internet of Things (IoT)?

A. A collection of software applications

B. A network of interconnected devices exchanging data

C. An isolated computing environment

D. A system for managing traditional IT operations

The Internet of Things (IoT) is best described as a network of interconnected devices exchanging data. This reflects the fundamental nature of IoT, which involves various devices—ranging from everyday appliances to complex industrial tools—being linked together through the internet. These devices can communicate and share data with one another, often without human intervention, enabling enhanced automation, remote monitoring, and intelligent decision-making based on the data exchanged. The essence of IoT lies in its ability to connect devices and sensors, allowing them to gather data and interoperate to improve performance, efficiency, and user experience. As such, options describing it as a collection of software applications, an isolated computing environment, or a system for managing traditional IT operations do not accurately capture the essence of what makes IoT distinct. Rather, IoT encompasses far more than just software or isolated systems—its core is the connectivity and collaboration between devices across diverse applications and environments.

10. What is required for an artifact to be considered acceptable evidence in a CMMC assessment?

A. It must be documented by an external auditor

B. It must demonstrate combat readiness

C. It must show implementation of relevant processes

D. It must be signed by organizational leadership

For an artifact to be considered acceptable evidence in a CMMC assessment, it is essential that it demonstrates the implementation of relevant processes. This ensures that the evidence is grounded in real practices and activities that the organization has carried out in relation to the Cybersecurity Maturity Model Certification requirements. Artifacts that illustrate how security controls are put into practice provide verifiable proof that the organization not only has policies in place but is actively following them. This verification is crucial for assessors as they evaluate an organization's compliance with the specific CMMC model level. In addition, showing implementation helps in establishing a link between documented procedures and actual behavior, which is important for the integrity of the assessment process. This kind of direct evidence allows assessors to evaluate the effectiveness of a company's cybersecurity posture and its ability to protect Controlled Unclassified Information (CUI). The other options do not align with this fundamental requirement. While documentation from an external auditor, combat readiness, or signatures from leadership may hold significance in other contexts, they do not directly provide evidence of active implementation of security processes necessary for CMMC compliance.