CERTSWARRIOR

Cyber AB
CMMC-CCA
Cybersecurity Maturity Model Certification Accreditation Body: Certified CMMC Assessor (CCA) Exam

Questions&AnswersPDF

ForMoreInformation:

https://www.certswarrior.com/

Features:

- 90DaysFreeUpdates
- 30DaysMoneyBackGuarantee
- InstantDownloadOncePurchased
- 24/7OnlineChat Support
- ItsLatestVersion

Latest Version: 6.0

Question: 1

A Defense Contractor is a CMMC Level 2 organization that frequently needs to transport digital media containing CUI between their main office and an off-site data storage facility. In preparing for their upcoming CMMC assessment, the organization's OSC has closely reviewed the requirements of CMMC practice MP.L2-3.8.6-Portable Storage Encryption, which specifically addresses the protection of CUI stored on digital devices during transport. The OSC recognizes their current practices of simply placing the media in standard packaging and using commercial shipping services do not fully meet the control's mandatory requirements.
Under CMMC practice MP.L2-3.8.6-Portable Storage Encryption, what is the mandatory requirement to protect CUI stored on digital devices during transport?

A. To ensure it is safeguarded by trained guards and transported using a reputable shipping company
B. To protect its confidentiality by encrypting it using FIPS 140-2 compliant cryptographic modules
C. To never transport CUI outside the controlled environment
D. To store CUI only on self-destructing media that erases data if tampered with

Answer: B

Explanation:
CUI can be stored and transported on a variety of portable media, which increases the chance the CUI can be lost. When identifying the paths the CUI flows, the OSC must also identify devices to include in this practice. To mitigate the risk of losing or exposing CUI, CMMC practice MP.L2-3.8.6-Portable Storage Encryption mandates OSCs to implement an encryption scheme to protect the data. This way, even if the media is lost, proper encryption renders the data inaccessible. When encryption is not an option, apply alternative physical safeguards during transport.

Question: 2

The CMMC Assessment Process (CAP) requires the Lead Assessor to validate the CMMC Assessment Scope proposed by the OSC.
What is the main task the Lead Assessor must conduct in validating the CMMC Assessment Scope? Choose the option that best describes the validation.

A. Document any discrepancies between the OSC's proposed scope and the actual systems and data.
B. Ensure the OSC has reviewed and approved the assessment scope.
C. Determine if any additional systems or data should be included in the assessment scope.
D. Verify the boundaries within the organization's networked environment contain all the assets that will be assessed based on the assessment scope.

Answer: D

Explanation:
The CMMC Assessment Process (CAP) specifically requires the Lead Assessor to validate that the assessment scope proposed by the OSC accurately reflects the boundaries and assets within the organization's networked environment that will be assessed. This is a crucial step to ensure the completeness and accuracy of the assessment scope, which is a critical requirement in the CMMC Assessment Process.

Question: 3

During the planning and preparation discussions, a key member of the C3PAO Assessment team falls ill and is unavailable for the originally scheduled assessment dates. The OSC is eager to proceed as planned and has expressed willingness to accommodate a smaller assessment team.
Can the Lead Assessor proceed with the assessment using a reduced assessment team size?

A. Yes, but only with the express written consent of the Cyber AB.
B. The decision is solely up to the OSC.
C. No, the assessment must be postponed until the full team is available.
D. Yes, as long as the remaining team members possess the necessary qualifications to cover all CMMC practices.

Answer: D

Explanation:
The Lead Assessor is responsible for ensuring that Assessment Team members are sufficiently prepared to perform the planned assessment activities. This implies some flexibility in team size, provided the remaining members have the qualifications to cover all required CMMC practices. Thus, if the remaining assessment team members have the necessary qualifications, the assessment can proceed with approval from the C3PAO.

Question: 4

You are the Lead Assessor on a CMMC Assessment Team preparing for an upcoming assessment. You have received the final assessment scope and supporting documentation from the OSC.
What should you do next to ensure the assessment can proceed as planned?

A. Submit the assessment scope and documentation to the C3PAO for approval.
B. Verify that the assessment team members are familiar with the assessment scope, method, plan, and tools.
C. Perform a preliminary “triage” of all the available evidentiary materials mapped to their respective CMMC practices.
D. Immediately begin the assessment based on the provided scope and documentation.

Answer: C

Explanation:

After receiving the final assessment scope and supporting documentation, the Lead Assessor along with the Assessment Team collaborates with the OSC to correlate the results of the OSC's most recent self-assessment, the preliminary list of anticipated evidence, the System Security Plan and other relevant documentation; and a list of all OSC personnel who play a role in the procedures that are in scope, to each of the CMMC practices. The purpose of this process is to do a preliminary “triage” of all the available evidentiary materials and “map” or “crosswalk” each item to their respective CMMC practices in order to establish the mutual understanding that the OSC has, at a minimum, addressed each of the CMMC practices with some evidentiary basis.

Question: 5

During an assessment, it was uncovered that a CCA worked as a consultant for the OSC through their RPO. Unfortunately, the CCA didn’t disclose this when their C3PAO appointed them to participate in the assessment.
Did the CCA behave professionally? If not, what issues are likely to arise?

A. No, breach of confidentiality
B. Yes, the CCA behaved professionally.
C. No, lack of objectivity
D. No, assessor bias

Answer: D

Explanation:
The practice of professionalism demands that under no circumstances should credentialed or registered individuals conduct a certified assessment or participate on a certified Assessment Team if they have also served as a consultant to prepare the organization for that assessment. Consulting is defined as "providing direct assistance in creating processes, training, and technology required to meet the intent of CMMC controls and processes."

Question: 6

A mid-sized company specializing in machining is preparing to bid for an upcoming DoD contract to provide machined components crucial for defense systems. As CMMC compliance will be required, the company’s top executives have invited you to assess their implementation of CMMC Level 2 requirements. During your visit to their environment of operations, you discover its production floor has several Computer Numerical Control (CNC) machines for precision machining, all connected to a local network for data transfer and control.
The CNC machines receive design files from a central server in the company's data center and communicate with a SCADA quality control system that monitors production metrics and performance. The central server hosts the design files, which are only accessible to authorized engineers and operators and backed up in an Amazon EBS cloud instance to ensure availability across the company's multiple machining shops in different states. Furthermore, the company allows employees to upload designs to the server remotely using VPNs and virtual desktop instances.
What is the BEST physical control the company can use for preventive purposes?

A. Using proximity card readers
B. Installing CCTVs
C. Locking all entrances
D. Displaying a large banner that says "Authorized Personnel Only"

Answer: A

Explanation:
Some of the physical locations are the company's production floor and on-premises data centers hosting the central server. The company should limit access to these areas using various physical access control mechanisms, install surveillance cameras to monitor access, escort visitors into the facilities, manage and audit physical access, maintain and review physical access logs, and ensure CUI environments are adequately protected.

Question: 7

As a Certified CMMC Assessor, you are part of a team assessing a small defense contractor. During the assessment, an employee being interviewed appears unsure about some security practices and asks for your advice on how to answer certain questions to make their compliance appear better.
As a Certified CMMC assessor, what should you do in this situation?

A. Politely refuse to provide any assistance and continue the assessment as planned
B. Offer to create documentation to cover gaps in their compliance
C. Provide guidance on how to answer questions to maximize the appearance of compliance
D. Suggest they seek guidance from another Assessor

Answer: A

Explanation:
The employee is asking the assessor for guidance on how to answer questions to make their compliance appear better. This would be considered coaching them to provide misleading information, which directly violates the CMMC CoPC practice of adherence to materials and methods.
By providing such guidance, you would be actively participating in the employee's attempt to misrepresent the OSC's compliance status, thereby undermining the entire purpose of the CMMC assessment. This could also lead to the OSC receiving a CMMC certification that does not accurately reflect its true security posture, putting the overall CMMC program and its credibility at risk.

Question: 8

A software development company is applying for a CMMC Level 2 assessment. As the Lead Assessor, you request access to the company’s System Security Plan (SSP) as part of the initial objective evidence for validating the scope.
Which of the following is true about the software development company's obligations in honoring the request?

A. The software development company must furnish the Lead Assessor with the SSP.

B. The software development company is not obligated to provide the SSP until after the assessment has begun.
C. The software development company can choose to provide a redacted version of the SSP, omitting sensitive information.
D. The software development company can refuse to provide the SSP if they deem it contains proprietary information.

Answer: A

Explanation:
The OSC has the initial responsibility for establishing the scope, but the CCA (Lead Assessor) plays a crucial role in verifying its accuracy. The OSC must provide a set of initial objective evidence, including the SSP, to assist in defining the assessment scope.

Question: 9

While examining an OSC's system design documentation, you notice they have implemented a CUI enclave and have a documented procedure addressing boundary protection. They have segmented their network into different zones, each having its own rules to allow or deny traffic. The OSC has implemented strict firewall rules that deny all incoming and outgoing traffic by default, only allowing specific traffic as required. The OSC has provisioned a state-of-the-art Intrusion Detection and Prevention System (IDPS) to block unrecognized traffic patterns automatically. During an interview with the network administrator, you realize that OSC uses a whitelisting approach to explicitly allow only certain IP addresses, domains, or services to communicate with their system. Their IT security team monitors network traffic to detect any unauthorized attempts to connect or communicate with their system. The scenario states that network traffic is monitored to detect unauthorized connection attempts.
Which of the following best describes the purpose of monitoring network traffic in the context of CMMC practice SC.L2-3.13.6-Network Communication by Exception?

A. To generate reports on network bandwidth usage for capacity planning purposes
B. To identify and potentially respond to suspicious or anomalous traffic patterns that might indicate attempted breaches
C. To identify and automatically add to the allowlist new legitimate communication requests
D. To verify that firewall rules are correctly configured and functioning as intended

Answer: B

Explanation:
CMMC practice SC.L2-3.13.6-Network Communication by Exception requires organizations to deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). Monitoring network traffic in this context identifies and potentially responds to suspicious activity that might violate the deny-all principle of SC.L2-3.13.6. This proactive approach helps detect potential breaches and mitigate risks.

Question: 10

You are evaluating an OSC for compliance with CMMC Level 2 practices. During your assessment of SC controls, you use a series of assessment methods to understand how effectively the OSC has implemented them. The OSC has a documented security policy outlining user roles and responsibilities. The OSC's system and communications protection policy states that basic user and privileged functionalities are separated. They have deployed Azure AD to help enforce this requirement through identity management.
Interviews with system administrators reveal they have elevated privileges for system management tasks. A review of system configuration settings shows separate user accounts for standard users and administrators. However, you notice that some employees use personal cloud storage services for storing work documents.
Based on CMMC practice SC.L2-3.13.3-Role Separation, which of the following findings from the scenario is MOST concerning?

A. Azure AD is used for identity management and enforcing role separation.
B. Some employees use personal cloud storage services for work documents.
C. The security policy defines separate user roles.
D. System administrators have elevated privileges.

Answer: B

Explanation:
While the documented policy, Azure AD implementation, and separate user accounts demonstrate efforts toward role separation, as required by CMMC practice SC.L2-3.13.3-Role Separation, allowing personal cloud storage for work documents creates a gap. This practice bypasses organizational controls and increases the potential for unauthorized information transfer or data breaches. SC.L2-3.13.3 emphasizes separating user functionality from system management functionality to mitigate insider threats.

CERTSWARRIOR

FULL PRODUCT INCLUDES:

Money Back Guarantee

Instant Download after Purchase

90 Days Free Updates

PDF Format Digital Download

24/7 Live Chat Support

Latest Syllabus Updates

For More Information – Visit link below:

https://www.certswarrior.com

16 USD Discount Coupon Code: U89DY2AQ