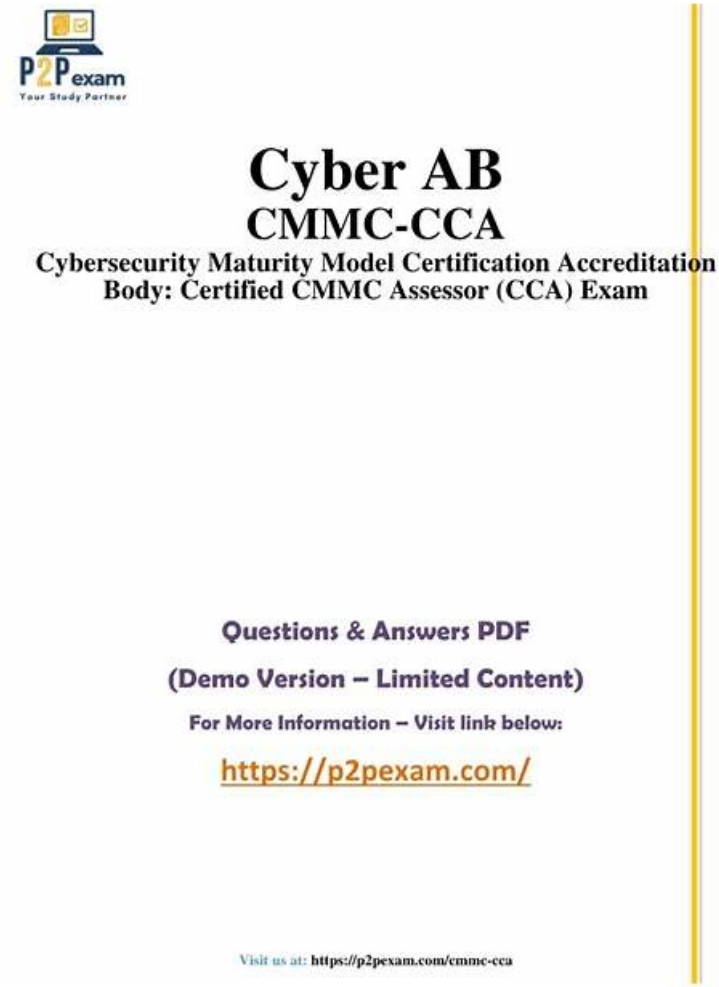
Cyber AB CMMC-CCA Latest Test Simulations - New Soft CMMC-CCA Simulations



BTW, DOWNLOAD part of Prep4sures CMMC-CCA dumps from Cloud Storage: https://drive.google.com/open?id=1biy4w11H8ZwLXrfevt9dgf-pjQ_ArnW6

As far as the price of Cyber AB CMMC-CCA exam practice test questions is concerned, these exam practice test questions are being offered at a discounted price. Get benefits from Cyber AB CMMC-CCA exam questions at discounted prices and download them quickly. Best of luck in CMMC-CCA Exam and career!!! Just choose the best CMMC-CCA exam questions format and start Cyber AB CMMC-CCA exam preparation without wasting further time.

Cyber AB CMMC-CCA Exam Syllabus Topics:

Topic	Details
Topic 1	• Assessing CMMC Level 2 Practices: This section of the exam measures skills of cybersecurity assessors in evaluating whether organizations meet the required practices of CMMC Level 2. It emphasizes applying CMMC model constructs, understanding model levels, domains, and implementation, and using evidence to determine compliance with established cybersecurity practices.
Topic 2	• CMMC Assessment Process (CAP): This section of the exam measures skills of compliance professionals and tests knowledge of the full assessment lifecycle. It covers the steps needed to plan, prepare, conduct, and report on a CMMC Level 2 assessment, including the phases of execution and how to document and follow up on findings in alignment with DoD and CMMC-AB expectations.

Topic 3	• CMMC Level 2 Assessment Scoping: This section of the exam measures skills of cybersecurity assessors and revolves around determining the proper scope of a CMMC assessment. It involves analyzing and categorizing Controlled Unclassified Information (CUI) assets, interpreting the Level 2 scoping guidelines, and making accurate judgments in scenario-based exercises to define what assets and systems fall within assessment boundaries.
Topic 4	• Evaluating Organizations Seeking Certification (OSC) against CMMC Level 2 Requirements: This section of the exam measures skills of cybersecurity assessors and focuses on evaluating the environments of organizations seeking certification at CMMC Level 2. It covers understanding differences between logical and physical settings, recognizing constraints in cloud, hybrid, on-premises, single, and multi-site environments, and knowing what environmental exclusions apply for Level 2 assessments.

Desktop and Web-Based Practice Exams to Evaluate CMMC-CCA Exam Preparation

It is a popular belief that only processional experts can be the leading one to do some adept job. And similarly, only high quality and high accuracy CMMC-CCA exam questions like ours can give you confidence and reliable backup to get the certificate smoothly because our experts have extracted the most frequent-tested points for your reference. Our CMMC-CCA exam questions generally raised the standard of practice materials in the market with the spreading of higher standard of knowledge in this area. So your personal effort is brilliant but insufficient to pass the Certified CMMC Assessor (CCA) Exam exam and our CMMC-CCA Test Guide can facilitate the process smoothly & successfully. Our Certified CMMC Assessor (CCA) Exam practice materials are successful by ensuring that what we delivered is valuable and in line with the syllabus of this exam.

Cyber AB Certified CMMC Assessor (CCA) Exam Sample Questions (Q70-Q75):

NEW QUESTION # 70
You are the Lead Assessor for a CMMC Assessment engagement with an OSC for CMMC Level 2. The OSC has provided you with their proposed CMMC Assessment Scope, which includes a network schematic diagram, their SSP, relevant policies, and organizational charts. During your review of the documentation, you notice they have excluded a subsidiary company's network and assets from the proposed CMMC Assessment Scope despite the subsidiary being involved in handling CUI related to federal contracts. If the OSC shares proprietary information with the Lead Assessor during the assessment engagement, what is the C3PAO's responsibility regarding this information after the completion of the assessment?

- A. The C3PAO can retain the OSC's proprietary information for future reference and use.
- B. The C3PAO is not responsible for the OSC's proprietary information once the Assessment is completed.
- C. The C3PAO must return and/or destroy any OSC proprietary information.
- D. The C3PAO can share the OSC's proprietary information with other clients for benchmarking purposes.

Answer: C

Explanation:
Comprehensive and Detailed in Depth Explanation:
The CAP and CoPC mandate that proprietary information be returned or destroyed post-assessment to protect OSC confidentiality, making Option D correct. Options A, B, and C violate these requirements.
Extract from Official Document (CAP v1.0):
* Section 3.5 - Archive Assessment Artifacts (pg. 36):"The C3PAO must return and/or destroy any OSC proprietary information after the engagement." References:
CMMC Assessment Process (CAP) v1.0, Section 3.5; CoPC Paragraph 3.2.

NEW QUESTION # 71
An OSC has documented HR and personnel security policies, which are well integrated. A key requirement is that credentials and

systems are revoked upon a transfer or termination. Their personnel security policy includes procedures for transfer and termination, a list of system accounts tied to each employee, and management of revoked or terminated credentials and authenticators. Examining the procedures addressing personnel transfer and termination, you learn that besides revoking or terminating system access, authenticators, and credentials, the OSC recovers all company IT equipment, access/identification cards, and keys from the transferred or terminated employee. They also interview the employee to remind them of their CUI handling obligations even after transfer and require them to sign an NDA. After every termination, they also change the password and other access control mechanisms and notify all the stakeholders that the employee has been terminated or transferred. Based on the scenario, the OSC can cite the following as evidence of collaborating on their implementation of CMMC practice PS.L2-3.9.2 - Personnel Actions, EXCEPT?

- A. List of usernames and passwords of all the employees
- B. Records of personnel transfer and termination actions
- C. Records of terminated or revoked authenticators and credentials
- D. Records of exit interviews accompanied by a list of terminated employees' identifiers

Answer: A

Explanation:
Comprehensive and Detailed In-Depth Explanation:
PS.L2-3.9.2 requires "reviewing and terminating system access upon personnel actions like termination." Evidence includes action records (B), exit interviews (C), and revoked credentials (D), demonstrating compliance. A list of usernames and passwords (A) isn't required, poses a security risk, and isn't tied to personnel actions, per the CMMC guide.
Extract from Official CMMC Documentation:
* CMMC Assessment Guide Level 2 (v2.0), PS.L2-3.9.2: "Examine termination records, exit interviews, and credential revocations; password lists not required."
* NIST SP 800-171A, 3.9.2: "Focus on action-specific evidence."
Resources:
* https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level2_MasterV2.
0_FINAL_202112016_508.pdf

NEW QUESTION # 72
When assessing an OSC's implementation of the System and Information Integrity (SI) practices, you examine their system and information integrity policy. You find that they have documented procedures addressing system monitoring tools and techniques, along with a monitoring strategy. The OSC has implemented a user behavior analytics tool to detect abnormal behavior anddeviations from normal patterns.
To ensure that only authorized users access the system, the OSC uses robust access controls and regularly audits security and system logs for unusual activities. Interviewing the network administration team, you learn they use a network monitoring tool to track inbound and outbound network traffic and identify any distinctive patterns that may suggest unauthorized use. You also learn that they use an IDS to identify suspicious activities, which are aggregated and analyzed using a state-of-the-art SIEM. The scenario mentions that the OSC uses a network monitoring tool to track inbound and outbound traffic and identify unusual patterns. However, it does not provide details on the tool's specific techniques or methods. Which of the following techniques would be most relevant for the assessor to inquire about during the assessment?

- A. Anomaly-based detection techniques
- B. Both signature-based and anomaly-based detection techniques
- C. Deep packet inspection techniques
- D. Signature-based detection techniques

Answer: B

Explanation:
Comprehensive and Detailed In-Depth Explanation:
CMMC practice SI.L2-3.14.6 - Monitor Communications for Attacks requires organizations to "monitor organizational communications at external boundaries and key internal boundaries for attacks or indicators of potential attacks." Effective monitoring typically employs bothsignature-based detection(identifying known threats via predefined patterns) andanomaly-based detection(flagging deviations from normal behavior), as these complementary techniques provide comprehensive coverage against known and emerging threats. The OSC's use of IDS, SIEM, and user behavior analytics suggests a mix of capabilities, but the specific techniques aren't detailed. Inquiring about both (C) ensures the assessor verifies a robust approach, as recommended by the CMMC guide. Anomaly-based (A) or signature-based (B) alone are insufficient, and while deep packet inspection (D) is useful, it's a narrower method not explicitly required.

Extract from Official CMMC Documentation:
* CMMC Assessment Guide Level 2 (v2.0), SI.L2-3.14.6: "Monitoring includes signature-based and anomaly-based detection to identify attacks."
* NIST SP 800-171A, 3.14.6: "Interview personnel to determine monitoring techniques, including signature and anomaly detection."
Resources:
* https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level2_MasterV2.
0_FINAL_202112016_508.pdf

NEW QUESTION # 73
The assessment team is discussing the pre-assessment scope with an OSC. The OSC would like to limit the scope of the security requirements in environments that contain FCI and/or CUI. In this case, the OSC should:

- A. Define an Assessment Scope for those assets that process, store, or transmit FCI
- B. Define a CMMC Self-Assessment Scope for only those assets that process, store, or transmit CUI
- C. Request a single CMMC certification for both activities
- D. Choose to conduct two separate CMMC certification activities

Answer: D

Explanation:
If an OSC wishes to separate environments that process FCI from those that process CUI, they may pursue two separate CMMC certifications (Level 1 for FCI and Level 2 for CUI). A single certification cannot cover both environments unless all requirements for the higher level are met across the entire enterprise.
Exact Extracts:
* CMMC Assessment Guide: "An OSC may choose to undergo multiple CMMC certification activities if they wish to limit scope between FCI and CUI environments."
* "Level 1 applies to safeguarding FCI, while Level 2 applies to CUI; separate certifications may be pursued if the OSC chooses to segregate these environments." Why the other options are not correct:
* A: A single certification would require all assets to meet Level 2 controls, which may not be the OSC's intent.
* C: Defining scope for FCI only aligns with Level 1, but this does not meet Level 2 certification requirements for CUI.
* D: A self-assessment scope only applies to Level 1 assessments, not Level 2 third-party certification.
References:
CMMC Assessment Guide - Level 2, Version 2.13: Scope determination for FCI vs CUI (pp. 3-5).
DoD CMMC Program documentation: Multiple certification options.

NEW QUESTION # 74
The client has a Supervisory Control and Data Acquisition (SCADA) system as OT to be evaluated as part of its assessment. In reviewing network architecture and conducting interviews, the assessor determines that a firewall separates the SCADA system from the client's enterprise network and that CUI is not processed by the SCADA system. Based on this information, what is an appropriate outcome?

- A. The assessor determines the SCADA system is out-of-scope for the assessment
- B. The assessor includes the OT within the assessment
- C. The assessor includes all systems identified by the client as part of the assessment
- D. The assessor determines that all Specialized Assets are within the scope of the assessment

Answer: A

Explanation:
In CMMC scoping, only assets that process, store, or transmit CUI (CUI Assets) or that can access them (Security Protection, Contractor Risk Managed, Specialized Assets) are in-scope. Since the SCADA system is firewalled off and does not handle CUI, it does not fall under CUI Asset classification and is considered Out- of-Scope.
Exact extracts:
* "CUI Assets are those that process, store, or transmit CUI."
* "Assets that do not process, store, or transmit CUI and have no connectivity to CUI Assets are considered Out-of-Scope."
* "Specialized Assets... are only in-scope if they process, store, or transmit CUI." Why the other options are incorrect:
* A: Inclusion requires processing/storing/transmitting CUI.
* C: OSC cannot arbitrarily bring unrelated systems into scope; CUI relevance governs scope.
* D: Not all Specialized Assets are in-scope; only those with CUI interaction are.

References:
CMMC Level 2 Scoping Guide - OT/ICS/SCADA asset treatment.

NEW QUESTION # 75
.....

The company is preparing for the test candidates to prepare the CMMC-CCA study materials professional brand, designed to be the most effective and easiest way to help users through their want to get the test CMMC-CCAcertification and obtain the relevant certification. In comparison with similar educational products, our training materials are of superior quality and reasonable price, so our company has become the top enterprise in the international market. Our CMMC-CCA Study Materials have been well received by the users, mainly reflected in the following advantages.

BTW, DOWNLOAD part of Prep4sures CMMC-CCA dumps from Cloud Storage: https://drive.google.com/open?id=1biy4w11H8ZwLXrfevt9dgf-pjQ_ArnW6