

Realistic Cyber AB CMMC-CCA Exam Questions with Accurate Answers



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

Questions & Answers PDF
(Demo Version – Limited Content)

For More Information – Visit link below:

<https://p2pexam.com/>

Visit us at: <https://p2pexam.com/cmmc-cca>

What's more, part of that GetValidTest CMMC-CCA dumps now are free: <https://drive.google.com/open?id=1iNLO8PhDZd8euSnk7FiB6YiILRmfQZA>

Exam CMMC-CCA tests your professional talent and expertise. This is the reason that passing this Cyber AB CMMC certification exam has been a tough challenge for professionals. But it is made easy now to ace it! The recently developed GetValidTest's CMMC-CCA Exam Questions dumps aim at to deliver you the shortest possible route to obtaining CMMC-CCA without any chance of losing the exam.

Cyber AB CMMC-CCA Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none">• 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 2	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none"> • 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.
Topic 4	<ul style="list-style-type: none"> • 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.

>> Latest CMMC-CCA Exam Test <<

Pass CMMC-CCA Exam with Realistic Latest CMMC-CCA Exam Test by GetValidTest

By keeping customer satisfaction in mind, GetValidTest offers you a free demo of the Certified CMMC Assessor (CCA) Exam (CMMC-CCA) exam questions. As a result, it helps you to evaluate the Certified CMMC Assessor (CCA) Exam (CMMC-CCA) exam dumps before making a purchase. GetValidTest is steadfast in its commitment to helping you pass the Cyber AB in CMMC-CCA Exam. A full refund guarantee (terms and conditions apply) offered by GetValidTest will save you from fear of money loss.

Cyber AB Certified CMMC Assessor (CCA) Exam Sample Questions (Q135-Q140):

NEW QUESTION # 135

After you ask to examine some audit records, the contractor's system administrator informs you that there is a process to follow before accessing them. The logs are hashed using SHA-512 algorithms, and the system administrator has to run an algorithm to recalculate the hashes for the audit records to verify their integrity before running a decryption algorithm to decrypt the data. Since this might take some time, you tour the facility while interviewing personnel with audit and accountability roles. You see an employee holding the door for another without using their physical access card. While interviewing the contractor's employees, you find that they can access all audit logging tools and tweak the settings according to their needs or requirements. Upon examining the contractor's access control policy, you realize they have not defined the measures to protect audit logging tools. Considering CMMC AU.L2-3.3.8 - Audit Protection and best practices, which of the following is the MOST concerning finding regarding the employees' access to audit logging tools?

- A. Employees have unrestricted access to all audit logging tools and can modify settings
- B. Employees hold doors for others without requiring physical access cards
- C. Audit logs are encrypted and hashed for integrity verification
- D. The system administrator needs to recalculate hashes for audit record verification before decryption

Answer: A

Explanation:

Comprehensive and Detailed In-Depth Explanation:

AU.L2-3.3.8 requires organizations to "protect audit information and audit logging tools from unauthorized access, modification, and deletion." Unrestricted employee access to audit logging tools, with the ability to modify settings, directly violates this by risking log integrity and authenticity-critical for security investigations. Door-holding (B) is a physical security issue unrelated to audit tools. Hash recalculation (C) is a procedural step, not a flaw. Encryption and hashing (D) are strengths, not concerns. The CMMC guide stresses limiting access to a defined subset of users.

Extract from Official CMMC Documentation:

* CMMC Assessment Guide Level 2 (v2.0), AU.L2-3.3.8: "Protect audit logging tools from unauthorized access and modification."

* NIST SP 800-171A, 3.3.8: "Examine access controls to ensure only authorized personnel can modify audit tools." Resources:

* https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level2_MasterV2.0_FINAL_202112016_508.pdf

0_FINAL_202112016_508.pdf

NEW QUESTION # 136

A CCA is asked to validate if an OSC has separated their systems containing CUI from other departments' systems on their local network. Which of the following MUST the CCA assess?

- A. Virtual Private Network (VPN)
- **B. Virtual Local Area Network (VLAN)**
- C. Network Address Translation (NAT)
- D. Area Network (WAN)

Answer: B

Explanation:

To validate separation of CUI systems from non-CUI systems on a local network, the assessor must evaluate the VLAN configuration. VLANs are a recognized logical segmentation method for separating enclaves, as defined in the CMMC Scoping Guide.

Exact Extracts:

* CMMC Scoping Guide: "Isolation can be achieved by implementing subnetworks with firewalls, routers, and VLANs to ensure separation of CUI assets from out-of-scope assets."

* "CUI Assets must be isolated from non-CUI assets unless those non-CUI assets are designated as Security Protection Assets or Contractor Risk Managed Assets." Why other options are not correct:

* A (WAN): Wide Area Networks describe external connectivity, not local separation.

* B (VPN): VPN provides encrypted remote access but does not enforce local network segmentation.

* D (NAT): NAT provides IP translation, not logical separation of traffic.

References:

CMMC Assessment Scope - Level 2, Version 2.13: Isolation requirements and VLAN as an example (pp. 9-11).

CMMC Assessment Guide - Level 2: Assessor validation of enclave boundary methods.

NEW QUESTION # 137

As a Certified CMMC Assessor (CCA), you evaluate an OSC's implementation of the AC.L2-3.1.11 - Session Termination requirement during a CMMC Level 2 assessment. This requirement mandates the organization to automatically terminate a user session after defined conditions are met. During your assessment, you want to determine whether the OSC has properly defined the conditions that would trigger the automatic termination of a user session, as required by assessment objective [a]. Which of the following assessment objects would you most likely examine to make this determination?

- A. Procedures addressing identification and authentication
- B. Interviews with system administrators and personnel with information security responsibilities
- C. The organization's system audit logs and records
- **D. The organization's Access Control Policy and system configuration settings**

Answer: D

Explanation:

Comprehensive and Detailed in Depth Explanation:

AC.L2-3.1.11[a] requires defining conditions for session termination, per NIST SP 800-171A. The Access Control Policy specifies these conditions (e.g., inactivity timeouts), and system configuration settings (e.g., timeout values) confirm their definition, making Option D primary. Option A (logs) shows execution, not definition. Option B (authentication procedures) is tangential. Option C (interviews) supplements but isn't definitive. Option D is the correct answer.

Reference Extract:

* NIST SP 800-171A, AC-3.1.11[a]: "Examine access control policy and system configurations for defined termination conditions." Resources: <https://csrc.nist.gov/pubs/sp/800/171/a/final>

NEW QUESTION # 138

While implementation validation of most CMMC requirements can be done virtually, the CMMC Assessment Process (CAP) identifies 15 CMMC practice objectives whose implementation must be observed by the Assessment Team in person and on the premises of the OSC. PE.L2-3.10.2 [c] and [d] are among these objectives. Both assessment objectives deal with monitoring the OSC's physical facilities and support infrastructure. Which assessment procedure or method can a CCA use to determine how well the OSC has implemented PE.L2-3.10.2 [c] and [d]?

- A. Test or examine mechanisms supporting or implementing physical access monitoring
- B. Interview personnel with information security responsibilities
- C. Test the OSC's Incident Response Plan
- D. Examine the System Security Plan

Answer: A

Explanation:

Comprehensive and Detailed in Depth Explanation:

PE.L2-3.10.2 [c] and [d] require monitoring physical facilities and infrastructure (e.g., cameras, sensors), per NIST SP 800-171 and CMMC Level 2. The CAP lists these among 15 objectives needing on-site validation.

Testing or examining mechanisms like access controls or monitoring systems (Option D) directly assesses implementation effectiveness, as required by NIST SP 800-171A's test/examine methods for physical controls. Option A (interviews) provides insight but not direct evidence. Option B (Incident Response Plan) is unrelated. Option C (SSP) documents intent, not execution. Option D is the correct answer per CAP and NIST guidance.

Reference Extract:

* CMMC Assessment Process (CAP) v1.0, Section 3.5.2: "PE.L2-3.10.2 [c] and [d] require on-site testing or examination of physical monitoring mechanisms."

* NIST SP 800-171A, PE-3.10.2[c,d]: "Test or examine physical access monitoring mechanisms."

Resources: <https://cyberab.org/Portals/0/Documents/Process-Documents/CMMC-Assessment-Process-CAP-v1.0.pdf>; <https://csrc.nist.gov/pubs/sp/800/171/a/final>

NEW QUESTION # 139

During a POA&M Close-Out Assessment, the Lead Assessor encounters a situation where the organization's corrective actions for a specific practice have inadvertently limited the effectiveness of another practice that was previously scored as 'MET' during the initial assessment. In this scenario, what should the Lead Assessor's recommendation to their C3PAO be?

- A. Update the POA&M and recommend the organization for CMMC Level 2 Final Certification, adding the affected practice to the POA&M.
- B. Defer the recommendation and request the organization to undergo a full reassessment.
- C. Recommend the organization not be granted CMMC Level 2 Final Certification.
- D. Recommend the organization for CMMC Level 2 Final Certification.

Answer: C

Explanation:

Comprehensive and Detailed in Depth Explanation:

The CAP prohibits Final Certification if corrective actions impair previously 'MET' practices (Option D).

Options A, B, and C do not address this requirement.

Extract from Official Document (CAP v1.0):

* Section 3.4 - POA&M Closeout (pg. 35): "If corrective actions limit the effectiveness of a practice previously scored as 'MET,' recommend the OSC not be granted Final Certification." References:

CMMC Assessment Process (CAP) v1.0, Section 3.4.

NEW QUESTION # 140

.....

GetValidTest has one of the most comprehensive and top-notch Cyber AB CMMC-CCA Exam Questions. We eliminated the filler and simplified the Certified CMMC Assessor (CCA) Exam preparation process so you can ace the Cyber AB certification exam on your first try. Our Cyber AB CMMC-CCA Questions include real-world examples to help you learn the fundamentals of the subject not only for the Cyber AB exam but also for your future job.

Latest Braindumps CMMC-CCA Book: <https://www.getvalidtest.com/CMMC-CCA-exam.html>

- Web-Based Cyber AB CMMC-CCA Practice Test Software Features The page for free download of CMMC-CCA on www.testkingpass.com will open immediately CMMC-CCA Valid Exam Topics
- Real CMMC-CCA Questions New CMMC-CCA Test Labs CMMC-CCA Valid Exam Topics Search for (CMMC-CCA) and download it for free immediately on www.pdfvce.com Test CMMC-CCA Vce Free
- High-quality Latest CMMC-CCA Exam Test | 100% Free Latest Braindumps CMMC-CCA Book Search for

