CMMC-CCA Test Certification Cost, Latest CMMC-CCA Exam Online

As is known to all, CMMC-CCA practice test simulation plays an important part in the success of exams. By simulation, you can get the hang of the situation of the real exam with the help of our free demo. You can fight a hundred battles with no danger of defeat. Simulation of our CMMC-CCA Training Materials make it possible to have a clear understanding of what your strong points and weak points are and at the same time, you can learn comprehensively about the exam. By combining the two aspects, you are more likely to achieve high grades in the real exam.

Cyber AB CMMC-CCA Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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 3	• 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 4	• 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.

>> CMMC-CCA Test Certification Cost <<

Latest CMMC-CCA Exam Online & Latest CMMC-CCA Dumps Ebook

Cyber AB Certified CMMC Assessor (CCA) Exam Sample Questions (Q109-Q114):

NEW QUESTION # 109
You decide to interview the IT security team to understand if and how a contractor has implemented audit failure alerting. You learn they have deployed AlienVault OSSIM, a feature-rich security information and event management (SIEM) tool. The SIEM tool has been configured to send automatic alerts to system and network administrators if an event affects the audit logging process. Alerts are generated for the defined events that lead to failure in audit logging and can be found in the notification section of the SIEM portal.
However, the alerts are sent to the specified personnel 24 hours after the occurrence of an event. As an assessor evaluating the implementation of AU.L2-3.3.4 - Audit Failure Alerting, which of the following would be a key consideration regarding the evidence provided by the contractor?

- A. Checking if the alert notification process integrates with third-party monitoring services
- B. Verifying that the types of audit logging failures defined cover a comprehensive range of potential scenarios
- C. Determining if the documented personnel roles for alert notification align with the organization's hierarchy
- D. Ensuring the defined alert notification methods (e.g., email, SMS) are secure and encrypted

Answer: B

Explanation:
Comprehensive and Detailed In-Depth Explanation:
AU.L2-3.3.4 requires "alerting personnel when audit logging fails." A 24-hour delay is concerning, but the key consideration is whether defined failure types (B) are comprehensive (e.g., software, hardware, capacity issues), ensuring effective detection. Notification methods (A), roles (C), and third-party integration (D) are secondary to failure coverage, per CMMC guidance.
Extract from Official CMMC Documentation:
* CMMC Assessment Guide Level 2 (v2.0), AU.L2-3.3.4: "Verify defined failure types are comprehensive."
* NIST SP 800-171A, 3.3.4: "Examine failure scenarios covered."
Resources:
* https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level2_MasterV2.
0_FINAL_202112016_508.pdf

NEW QUESTION # 110
As the Lead Assessor for an OSC, John admires their advanced security solutions during the assessment.
However, his admiration distracts him from the assessment's focus. Instead, he engages in conversation about the OSC's robust security, becoming swayed by their capabilities. Consequently, John becomes hesitant to identify deficiencies or noncompliances, displaying a positive bias toward the OSC. What is the impact of this positive bias on the CMMC assessment of the OSC?

- A. It has no effect on the assessment process and outcomes
- B. It is not a concern in CMMC assessments
- C. It may lead to a more thorough and rigorous evaluation of the OSC
- D. It can result in a more lenient and inaccurate assessment of the OSC

Answer: D

Explanation:
Comprehensive and Detailed in Depth Explanation:
The CMMC Assessment Process (CAP) stresses that assessors must remain objective to ensure accurate and reliable outcomes. Positive bias, as exhibited by John, occurs when an assessor's admiration for an OSC's capabilities leads to overlooking deficiencies, compromising the assessment's integrity. This leniency can result in an inaccurate evaluation, failing to identify noncompliances that could leave CUI vulnerable, contrary to CMMC's goal of ensuring robust protection.
Option A (not a concern) ignores CAP's emphasis on objectivity. Option B (more rigorous evaluation) contradicts the leniency caused by positive bias. Option C (no effect) underestimates bias's impact on evidence interpretation. Option D correctly reflects the risk of a lenient, inaccurate assessment, aligning with CAP guidance, making it the correct answer.
Reference Extract:

* CMMC Assessment Process (CAP) v1.0, Section 2.3:"Positive or negative bias can lead to inconsistent or inaccurate outcomes...
Assessors must manage bias to ensure objective reviews."Resources:
https://cyberab.org/Portals/0/Documents/Process-Documents/CMMC-Assessment-Process-CAP-v1.0.
pdf

NEW QUESTION # 111
John, a CCA, has been assigned by his C3PAO to conduct a CMMC assessment for an OSC. During the assessment, John notices
that the OSC's security practices leave much to be desired. After speaking with the OSC's IT staff, John offers to connect them with
a vendor he knows who sells a vulnerability management tool that could address some of their weaknesses. According to the
CMMC CoPC, which of the following best describes John's actions?

- A. John did not show respect for intellectual property.
- B. John acted appropriately by trying to help the OSC improve its security posture.
- C. John violated the principles of professionalism and objectivity by soliciting business for a third-party vendor while serving on the Assessment Team.
- D. John's actions were deemed acceptable since he did not directly profit from connecting the OSC with the vendor.

Answer: C

Explanation:
Comprehensive and Detailed in Depth Explanation:
The CoPC prohibits CCAs from soliciting business or offering vendor recommendations during assessments, violating
Professionalism and Objectivity. Option A (appropriate) ignores this. Option B (IP) is unrelated.
Option C (no profit) doesn't excuse the violation. Option D is correct.
Extract from Official Document (CoPC):
* Paragraph 3.3(4) - Proper Use of Methods (pg. 7):"Do not solicit business for third-party vendors while serving on an Assessment
Team." References:
CMMC Code of Professional Conduct, Paragraph 3.3(4).

NEW QUESTION # 112
The OSC POC has prepared evidence from an internal pre-assessment for the C3PAO in preparation for a third-party assessment.
The OSC POC has identified that there are several ESPs (External Service Providers) involved in protecting the security of the
infrastructure. While reviewing the pre-assessment documentation regarding ESPs, the Lead Assessor will be looking for items that
are:

- A. Noted as inherited
- B. Marked as requiring a waiver
- C. Marked as NOT APPLICABLE
- D. Noted as partially implemented

Answer: A

Explanation:
When External Service Providers are used, the OSC can inherit practices from the ESP if sufficient evidence is provided (such as
FedRAMP authorization or equivalent). The Lead Assessor must verify which controls are noted as inherited, as these are assessed
differently from controls implemented directly by the OSC.
Exact Extracts:
* CMMC Assessment Guide: "An OSC may inherit practices from External Service Providers when those providers demonstrate
equivalent compliance (e.g., FedRAMP Moderate for CUI)."
* "Assessors must review documentation that identifies which practices are inherited, partially implemented, or implemented
internally."
* CMMC Scoping Guide: "Inherited controls must be clearly documented by the OSC in the SSP." Why the other options are not
correct:
* B: Waivers are not part of CMMC assessments.
* C: "Not Applicable" does not apply to ESP involvement; they either provide inherited practices or not.
* D: "Partially implemented" indicates deficiencies, not proper inheritance.
References:
CMMC Assessment Guide - Level 2, Version 2.13: External Service Providers and inheritance (pp. 10-13).
CMMC Scoping Guide - Level 2: Inherited practices documentation requirements.

NEW QUESTION # 113

A manufacturing company is seeking Level 2 certification. The loading docks are currently accessible directly from the company's main parking lot, which may lead to unauthorized access to facilities. Based on this information, how should this method be modified to BEST meet Level 2 requirements?

- A. Implement physical perimeter controls, such as turnstiles, to limit access.
- B. Implement physical perimeter controls, such as cameras, to limit access to only authorized personnel.
- C. Require visitors to check in at the reception desk and maintain a visitor log.
- D. Implement physical perimeter controls, such as a gate with a badge system, to limit access to only authorized personnel.

Answer: D

Explanation:
* Applicable Requirement: PE.L2-3.10.3 - "Control physical access to organizational systems, equipment, and the respective operating environments."
* Why D is Correct: A gate with a badge system represents preventive perimeter control that ensures only authorized personnel can access sensitive areas (e.g., loading docks). This directly aligns with Level 2 physical protection requirements.
Why Other Options Are Insufficient:
* A (Turnstiles): More relevant for internal building entry, not loading docks.
* B (Visitor log): Supports accountability, but does not prevent unauthorized entry.
* C (Cameras): Provides monitoring but not control - surveillance alone does not restrict access.
References (CCA Official Sources):
* NIST SP 800-171 Rev. 2 - PE.L2-3.10.3
* NIST SP 800-171A - PE.L2-3.10.3 Assessment Objectives
* CMMC Assessment Guide - Level 2, Physical Protection

NEW QUESTION # 114

......

In traditional views, the CMMC-CCA practice materials need you to spare a large amount of time on them to accumulate the useful knowledge may appearing in the real CMMC-CCA exam. However, our CMMC-CCA learning questions are not doing that way. According to data from former exam candidates, the passing rate of our CMMC-CCA learning material has up to 98 to 100 percent. There are adequate content to help you pass the exam with least time and money.

Latest CMMC-CCA Exam Online: https://www.examsreviews.com/CMMC-CCA-pass4sure-exam-review.html

- Unbeatable CMMC-CCA Practice Prep Offers You the Most Precise Exam Braindumps - www.prepawayete.com 🖐 Go to website ⇒ www.prepawayete.com ⇐ open and search for 🔲 CMMC-CCA 🔲 to download for free 🔲New CMMC-CCA Test Objectives
- www.stes.tyc.edu.tw, ycs.instructure.com, myportal.utt.edu.tt, bbs.t-firefly.com, www.stes.tyc.edu.tw, bbs.t-firefly.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

2026 Latest ExamsReviews CMMC-CCA PDF Dumps and CMMC-CCA Exam Engine Free Share:
https://drive.google.com/open?id=1_t7cnplPthHvk9oz0_3Ex9_TcAG5BOuI