

Free CMMC-CCA Practice Exams & Valid CMMC-CCA Exam Vce

Now Available...

The Certified CMMC Assessor (CCA) Practice Exam

Enhance your cybersecurity training portfolio with the CCA Practice Exam offering unlimited re-takes!


Tuuli Eaton
Head of Growth, Int'l
Logical Operations

Logical Operations

2025 Latest Pass4SureQuiz CMMC-CCA PDF Dumps and CMMC-CCA Exam Engine Free Share:
https://drive.google.com/open?id=17sw_jUqnCydHEbA_HF6nkvw_Llky8-_w

You only need 20-30 hours to learn our CMMC-CCA test torrents and prepare for the exam. After buying our CMMC-CCA exam questions you only need to spare several hours to learn our CMMC-CCA test torrents and commit yourselves mainly to the jobs, the family lives and the learning. Our answers and questions of CMMC-CCA Exam Questions are chosen elaborately and seize the focus of the exam so you can save much time to learn and prepare the exam. Because the passing rate is high as more than 98% you can reassure yourselves to buy our CMMC-CCA guide torrent.

Cyber AB CMMC-CCA Exam Syllabus Topics:

Topic	Details
Topic 1	<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 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">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	<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.

>> Free CMMC-CCA Practice Exams <<

2025 Free CMMC-CCA Practice Exams Pass Certify | Latest Valid CMMC-

CCA Exam Vce: Certified CMMC Assessor (CCA) Exam

Our CMMC-CCA study materials are closely linked with the test and the popular trend among the industries and provide all the information about the test. The answers and questions seize the vital points and are verified by the industry experts. Diversified functions can help you get an all-around preparation for the test. Our online customer service replies the clients' questions about our CMMC-CCA Study Materials at any time. So our CMMC-CCA study materials can be called perfect in all aspects.

Cyber AB Certified CMMC Assessor (CCA) Exam Sample Questions (Q41-Q46):

NEW QUESTION # 41

During a CMMC assessment, the Assessment Team identifies that the OSC has not implemented a practice due to a recent system upgrade that disrupted their previous controls. The OSC requests to include this practice in a POA&M. However, the practice is listed as one that could lead to significant network exploitation if not implemented. What should the Lead Assessor do?

- A. Recommend that the OSC implement the practice immediately and reassess it before concluding the assessment.
- **B. Mark the practice as "NOT MET" and inform the OSC that it is ineligible for a POA&M due to its critical nature.**
- C. Allow the practice to be included in the POA&M, as it was disrupted by a recent upgrade.
- D. Report the OSC to the Cyber AB for failing to maintain critical controls.

Answer: B

Explanation:

Comprehensive and Detailed in Depth Explanation:

The CAP excludes critical practices from POA&M if they risk exploitation, requiring a 'NOT MET' score (Option B). Options A, C, and D violate CAP rules.

Extract from Official Document (CAP v1.0):

* Section 2.3.2.1 - Ineligible Practices (pg. 28): "Practices that could lead to significant exploitation are ineligible for POA&M and must be scored 'NOT MET.'" References:

CMMC Assessment Process (CAP) v1.0, Section 2.3.2.1.

NEW QUESTION # 42

A company receives data that they suspect is CUI, but it is not marked as such. What is an acceptable way for the company to handle unmarked potential CUI?

- A. Have a procedure for deleting unlabeled data.
- B. If data are not marked, then they are not CUI.
- C. Treat all data as CUI even if not marked.
- **D. Have a procedure for proper handling of unlabeled data.**

Answer: D

Explanation:

The CMMC Assessment Guide (Level 2) requires organizations to have a documented procedure for the identification and handling of unmarked potential CUI. The DoD guidance specifies that contractors cannot assume unmarked data is not CUI; instead, they must have a process to ensure unmarked potential CUI is handled properly until its classification is clarified.

Extract from Assessment Guide:

"Organizations must establish procedures for the handling of unmarked data that is suspected of being CUI.

These procedures should define how unmarked information is protected until such time its status can be determined." Therefore, the correct answer is to have a procedure for proper handling of unlabeled data.

Reference: CMMC Assessment Guide, Level 2, CUI Handling Practices.

NEW QUESTION # 43

As part of a C3PAO Assessment Team, you are reviewing an OSC's security practices and documentation.

During your review, you notice that the OSC has presented the same evidence artifacts to support its implementation of several CMMC practices and objectives. Based on the scenario above and your understanding of the CMMC Assessment process, which of the following is true?

- A. The same evidence artifacts can be used for practices across multiple CMMC domains or assessment objectives.
- B. The same evidence artifacts can be used for practices across multiple CMMC domains, but not for assessment objectives.
- C. A POA&M can be used in place of evidence.
- D. Each CMMC domain or assessment objective requires a unique set of evidence artifacts.

Answer: A

Explanation:

Comprehensive and Detailed in Depth Explanation:

The CAP allows reuse of evidence across domains and objectives if relevant (Option C). Options A and B impose incorrect restrictions, and Option D misrepresents POA&M's role.

Extract from Official Document (CAP v1.0):

* Section 2.2 - Conduct Assessment (pg. 25): "The same evidence artifacts can be used for practices across multiple CMMC domains or assessment objectives if applicable." References:

CMMC Assessment Process (CAP) v1.0, Section 2.2.

NEW QUESTION # 44

As the Lead Assessor for a CMMC Level 2 assessment team, you have completed the examination of evidence and generated Preliminary Recommended Findings. Now, it is time to submit, package, and archive the assessment documentation, ensuring accuracy, completeness, and adherence to protocol. According to the CMMC Assessment Process, how long after the Final Findings Briefing must you submit the Assessment Results Package to the C3PAO CQAP?

- A. 15 business days
- B. 20 business days
- C. 10 business days
- D. 30 business days

Answer: C

Explanation:

Comprehensive and Detailed in Depth Explanation:

The CAP specifies a 10-business-day deadline for submitting the Assessment Results Package to the C3PAO CQAP after the Final Findings Briefing, ensuring timely quality review and submission to CMMC eMASS.

Options A, B, and D do not align with this explicit requirement.

Extract from Official Document (CAP v1.0):

* Section 3.2 - Report Recommended Assessment Results (pg. 32): "Reports must be submitted to the CQAP no later than 10 business days from the Final Findings Briefing." References:

CMMC Assessment Process (CAP) v1.0, Section 3.2.

NEW QUESTION # 45

You are a CCA conducting a CMMC assessment for an OSC. While evaluating Risk Assessment (RA) practices, you check how the OSC has addressed assessment objective [a] of RA.L2-3.11.1, "Determine if the frequency for assessing risk to organizational operations, organizational assets, and individuals is defined." Which Assessment Object would most likely provide the answer to this requirement?

- A. Plan of Actions
- B. Risk Assessment Report
- C. Vulnerability scanning results
- D. Risk Assessment Policy

Answer: D

Explanation:

Comprehensive and Detailed in Depth Explanation:

RA.L2-3.11.1[a] requires defining risk assessment frequency, per NIST SP 800-171A. The Risk Assessment Policy (Option A) explicitly states this frequency, making it the primary Assessment Object. Option B (Plan of Actions) addresses remediation, not frequency. Option C (reports) shows execution, not policy. Option D (scan results) is unrelated. Option A is the correct answer.

Reference Extract:

* NIST SP 800-171A, RA-3.11.1[a]: "Examine risk assessment policy for defined frequency." Resources:

