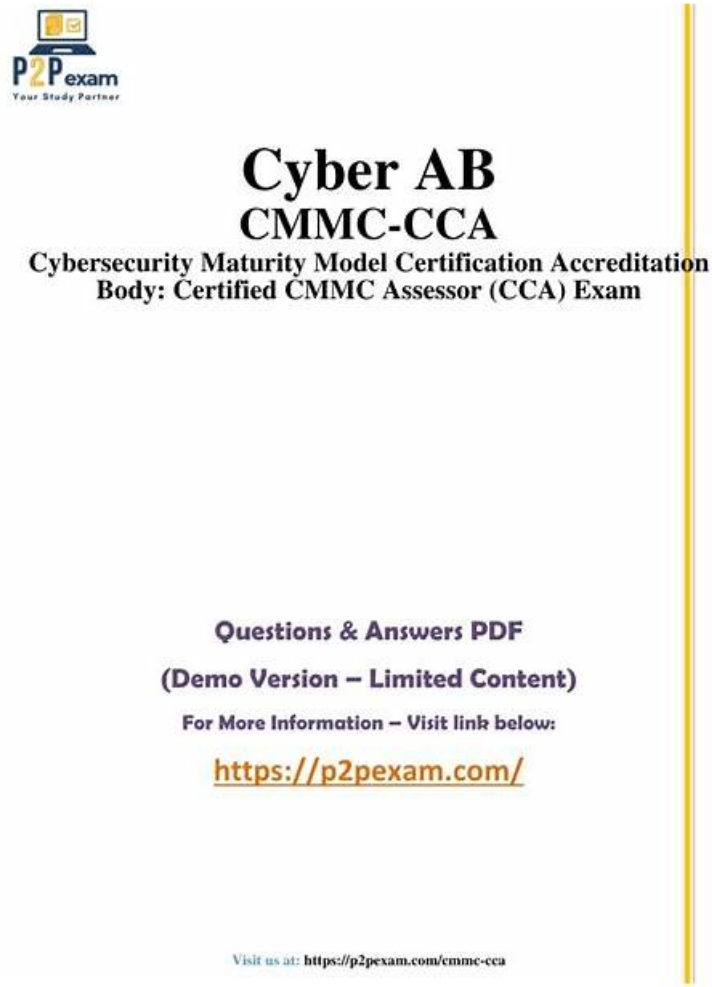
Cyber AB CMMC-CCA Quiz - CMMC-CCA Studienanleitung & CMMC-CCA Trainingsmaterialien



Auf der Webseite PrüfungFrage können Sie sich mühlos auf die Cyber AB CMMC-CCA Zertifizierungsprüfung vorbereiten und auch manche häufig vorkommenden Fehler vermeiden. Unsere Berufsgruppe aus gut ausgebildeten und erfahrenen IT-Eliten haben die Entwicklungen der ständig veränderten IT-Branche untersucht und erforscht, dann schließen Sie die Fragenkataloge zur Cyber AB CMMC-CCA Zertifizierungsprüfung für PrüfungFrage zusammen. Diese Cyber AB CMMC-CCA Fragenkataloge verfügen über hohe Genauigkeit und Autorität. PrüfungFrage wird Ihre beste Wahl sein!

Cyber AB CMMC-CCA Prüfungsplan:

Thema	Einzelheiten
Thema 1	• 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.
Thema 2	• 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.

Thema 3	• 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.
Thema 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 Prüfungsübungen, CMMC-CCA Examsfragen

Die Schulungsunterlagen zur Cyber AB CMMC-CCA Zertifizierungsprüfung von PrüfungFrage werden Ihnen nicht nur Energie und Ressourcen, sondern auch viel Zeit ersparen. Denn normalerweise müssen Sie einige Monate verwenden, um sich auf die Prüfung vorzubereiten. So, was Sie tun sollen, ist die Schulungsunterlagen zur Cyber AB CMMC-CCA Zertifizierungsprüfung von PrüfungFrage zu kaufen und somit das Zertifikat erhalten. Unser PrüfungFrage wird Ihnen helfen, die relevanten Kenntnisse und Erfahrungen zu bekommen. Wir bieten Ihnen auch ein ausführliches Prüfungsziel. Mit PrüfungFrage können Sie die Cyber AB CMMC-CCA Zertifizierungsprüfung einfach bestehen.

Cyber AB Certified CMMC Assessor (CCA) Exam CMMC-CCA Prüfungsfragen mit Lösungen (Q70-Q75):

70. Frage
The SSP for an OSC undergoing an assessment categorizes a device in the inventory that wirelessly connects to the network. In order to secure the connection of wireless devices that access a system that transmits, stores, or processes CUI, what are the requirements?

- A. Wireless access must be configured to use FIPS 140 validated cryptography.
- B. Wireless users must be vetted, and an Access Control List maintained for access to CUI.
- C. Wireless access must be configured to use FIPS 140 validated cryptography and limited to authenticated users.
- D. Wireless users must be specifically identified in network diagrams and configured to use FIPS 140 validated cryptography.

Antwort: C

Begründung:
Wireless access to systems transmitting, processing, or storing CUI must be protected with FIPS 140- validated cryptography and access must be limited to authenticated users. This ensures confidentiality and integrity of CUI while preventing unauthorized wireless access.
Exact Extracts (official CMMC Assessor/Study documents):
* SC.L2-3.13.13: "Employ FIPS-validated cryptography when used to protect the confidentiality of CUI."
* AC.L2-3.1.1 / 3.1.2: "Limit system access to authorized users... and authenticate the identities of those users."
* SC.L2-3.13.17: "Protect wireless access to the system using authentication and encryption."
* Assessment Guide clarifies: "Wireless access must use FIPS 140 validated cryptographic modules and must be restricted to authenticated users." Why other options are not correct:
* A: Only requires encryption; does not address authenticated access, which is mandatory.
* B: Vetting and access lists may be useful, but they are not sufficient substitutes for cryptographic and authentication requirements.
* D: Identifying users in diagrams is good documentation practice but not a CMMC requirement for wireless protection.
References (official CCA/CMMC documents):
* CMMC Assessment Guide - Level 2, Version 2.13: Practices SC.L2-3.13.13 and SC.L2-3.13.17 (pp. 134-136).
* NIST SP 800-171A, Assessment Objectives for wireless access and cryptographic requirements.

71. Frage

You have been sent to assess an OSC's implementation of CMMC practices, one of which is AC.L2-3.1.11 - Session Termination. In assessing the contractor's implementation of AC.L2-3.1.11, you'll likely need to examine the following specifications, EXCEPT?

- A. System security plan
- B. The session termination policy
- C. Mechanisms for implementing user session termination
- D. The access control policy

Antwort: C

Begründung:
Comprehensive and Detailed In-Depth Explanation:
AC.L2-3.1.11 involves "terminating user sessions after defined conditions." Specifications (documented artifacts like policies and plans-B, C, D) define these conditions and are examinable per NIST SP 800-171A.
Mechanisms (A) are technical implementations, not specifications, and are tested, not examined as documents. The CMMC guide distinguishes between examining policies and testing mechanisms.
Extract from Official CMMC Documentation:
* CMMC Assessment Guide Level 2 (v2.0), AC.L2-3.1.11: "Examine policies and plans; test termination mechanisms."
* NIST SP 800-171A, 3.1.11: "Specifications include policies, not mechanisms." Resources:
* https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level2_MasterV2.
0_FINAL_202112016_508.pdf

72. Frage
A CCA is conducting a CMMC assessment and notices that the OSC's evidence includes a policy document that is outdated by two years. The OSC insists that the policy is still in effect, but staff interviews indicate that newer, undocumented procedures are being followed. How should the CCA handle this situation?

- A. Document the discrepancy between the policy and actual procedures and assess based on all available evidence.
- B. Accept the outdated policy as evidence since the OSC claims it is still in effect.
- C. Request the OSC to update the policy document before proceeding with the assessment.
- D. Reject the policy document outright and score the practice as "NOT MET."

Antwort: A

Begründung:
Comprehensive and Detailed in Depth Explanation:
The CAP requires documenting discrepancies and assessing all evidence (Option B). Option A ignores reality, Option C is premature, and Option D involves consulting, which is prohibited.
Extract from Official Document (CAP v1.0):
* Section 2.2 - Conduct Assessment (pg. 25):"Document discrepancies between policy and practice as evidence gaps and assess based on all findings." References:
CMMC Assessment Process (CAP) v1.0, Section 2.2.

73. Frage
After thoroughly evaluating the evidence gathered, the Assessment Team has generated their preliminary findings and recommendations for the OSC's target CMMC level. However, before finalizing the results, they need to validate their findings through a review process. Once the Preliminary Recommended Findings have been generated and validated, the Assessment Team needs to properly record them in the appropriate document or system. Where should the Assessment Team enter or record the preliminary recommended findings after generating and validating them?

- A. CMMC Assessment In-Brief Template
- B. Daily Checkpoint Log
- C. In the CMMC Assessment Findings Brief.
- D. In the CMMC Assessment Results Template.

Antwort: C

Begründung:
Comprehensive and Detailed in Depth Explanation:

The CAP specifies that Preliminary Recommended Findings, after validation, are recorded in the CMMC Assessment Findings Brief, which summarizes practice scores and findings. Option A is for final results, Option B is for daily notes, and Option D is for initial planning.
Extract from Official Document (CAP v1.0):
* Section 2.4 - Generate Preliminary Findings (pg. 29):"The Assessment Team shall enter Preliminary Recommended Findings in the CMMC Assessment Findings Brief after generating and validating them." References:
CMMC Assessment Process (CAP) v1.0, Section 2.4.

74. Frage
An OSC outsources all of its security incident and event monitoring work to a third-party SOC. Additionally, the OSC utilizes a cloud-hosted antivirus (AV) system to fulfill the requirement of having virus protection without hosting additional servers on-site. During the scoping discussion, both the SOC and AV should be listed as what type of asset?

- A. They are Security Protection Assets due to their performance of security functions.
- B. They are Out-of-Scope Assets due to being fully hosted/operated by third parties.
- C. They are CUI Assets due to their operation within a CUI network.
- D. They are Contractor Risk Managed Assets because they are not physically or logically isolated from CUI assets.

Antwort: A

Begründung:
The Scoping Guidance defines Security Protection Assets as systems, tools, or services that provide security functions protecting CUI assets, even if outsourced to third parties.
Extract:
"Security Protection Assets are tools, systems, or services that provide security functionality (e.g., SOC, antivirus, logging) to protect CUI assets. These must be included in scope." Therefore, SOC and AV must be categorized as Security Protection Assets.
Reference: CMMC Scoping Guidance - Security Protection Assets.

75. Frage
.....

Ich glaube, egal in welcher Branche erwarten alle Beschäftigte eine gute Berufsaussichten. In der konkurrrenzfähigen IT-Branche gilt es auch. Die Fachleute in der IT-Branche erwarten eine gute Beförderungsmöglichkeit. Viele IT-Fachleute sind sich klar, dass die Cyber AB CMMC-CCA Zertifizierungsprüfung Ihren Traum verwirklichen kann. Und PrüfungFrage ist solch eine Website, die Ihnen zum Bestehen der Cyber AB CMMC-CCA Zertifizierungsprüfung verhilft.

Lernguide □ Öffnen Sie die Webseite □ www.itzert.com □ und suchen Sie nach kostenloser Download von ➽ CMMC-CCA □ □CMMC-CCA Praxisprüfung

- CMMC-CCA Aktuelle Prüfung - CMMC-CCA Prüfungsguide - CMMC-CCA Praxisprüfung □ Suchen Sie auf ☀ www.zertpruefung.de □☀□ nach kostenlosem Download von □ CMMC-CCA □ □CMMC-CCA Quizfragen Und Antworten
- CMMC-CCA Zertifizierungsprüfung □ CMMC-CCA Zertifikatsdemo □ CMMC-CCA Lernressourcen □ Suchen Sie jetzt auf ▷ www.itzert.com ◁ nach 《 CMMC-CCA 》 um den kostenlosen Download zu erhalten □CMMC-CCA Testing Engine
- CMMC-CCA Zertifikatsdemo □ CMMC-CCA Prüfungs □ CMMC-CCA PDF Demo □ Erhalten Sie den kostenlosen Download von □ CMMC-CCA □ mühelos über { www.pruefungfrage.de } □CMMC-CCA Prüfungsinformationen
- elearning.eauqardho.edu.so, learningmart.site, motionentrance.edu.np, study.stcs.edu.np, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, motionentrance.edu.np, www.stes.tyc.edu.tw, ncon.edu.sa, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes