

# CMMC-CCA퍼펙트덤프공부자료, CMMC-CCA시험유효자료



참고: KoreaDumps에서 Google Drive로 공유하는 무료 2026 Cyber AB CMMC-CCA 시험 문제집이 있습니다:  
<https://drive.google.com/open?id=1u5uzulwA-7qgrfllhwZc2qLRc7s4hH-u>

Cyber AB인증 CMMC-CCA시험을 통과하여 자격증을 취득하여 IT 업계에서의 자신의 자리를 지키려면 많은 노력이 필요합니다. 회사일도 바쁜데 시험공부까지 스트레스가 장난아니게 싸이고 몸도 많이 상하겠죠. KoreaDumps는 여러분을 위해 최신Cyber AB인증 CMMC-CCA시험에 대비한Cyber AB인증 CMMC-CCA덤프를 발췌하였습니다. Cyber AB인증 CMMC-CCA덤프는Cyber AB인증 CMMC-CCA시험의 기출문제와 예상문제가 묶여져 있어 시험적중율이 굉장히 높습니다. 쉽게 시험을 통과하려면KoreaDumps의 Cyber AB인증 CMMC-CCA덤프를 추천합니다.

## Cyber AB CMMC-CCA 시험요강:

주제	소개
주제 1	<ul style="list-style-type: none"><li>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.</li></ul>
주제 2	<ul style="list-style-type: none"><li>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.</li></ul>
주제 3	<ul style="list-style-type: none"><li>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.</li></ul>
주제 4	<ul style="list-style-type: none"><li>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.</li></ul>

## CMMC-CCA시험유료자료, CMMC-CCA최신 시험기출문제

KoreaDumps는 여러분의 시간을 절약해드릴 뿐만 아니라 여러분들이 안심하고 응시하여 순조로이 패스할수 있도록 도와주는 사이트입니다. KoreaDumps는 믿을 수 있는 사이트입니다. IT업계에서는 이미 많이 알려 저있습니다. 그리고 여러분에 신뢰를 드리키 위하여Cyber AB CMMC-CCA관련자료의 일부분 문제와 답 등 샘플을 무료로 다운 받아 체험해볼 수 있게 제공합니다. 아주 만족할 것이라고 믿습니다. 우리는KoreaDumps제품에 대하여 아주 자신이 있습니다. 우리Cyber AB CMMC-CCA도 여러분의 무용지물이 아닌 아주 중요한 자료가 되리라 믿습니다. 여러분께서는 아주 순조로이 시험을 패스하실 수 있을 것입니다. KoreaDumps선택은 틀림없을 것이며 여러분의 만족할만한 제품만을 제공할것입니다.

### 최신 Cyber AB CMMC CMMC-CCA 무료샘플문제 (Q138-Q143):

#### 질문 # 138

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

정답: B

설명:

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.

#### 질문 # 139

During the examination of evidence for access control procedures, you review an OSC's Access Control List (ACL). The ACL appears to include most user accounts, but you notice that it lacks entries for several newly hired employees. You also realize that some parts of the OSC's access control policy haven't been signed and endorsed by senior management. Additionally, you notice multiple attestations from employees who are not the proper system owners. How should you proceed when encountering an incomplete artifact, such as the missing personnel in the access control list?

- A. Mark the associated CMMC practice as 'NOT MET' due to the incomplete artifact.
- B. Request the OSC to provide a revised, complete version of the artifact within a specified timeframe.
- C. Disregard the incomplete artifact and rely on other evidence for the practice assessment.
- **D. Document the incomplete artifact as an evidence gap and proceed with assessing the practice based on the available evidence.**

정답: D

설명:

Comprehensive and Detailed in Depth Explanation:

The CAP instructs assessors to document incomplete artifacts as evidence gaps and proceed with the assessment using available evidence, rather than immediately failing a practice or demanding revisions during the assessment. Option A (requesting revision) is not an option during evidence examination per CAP; remediation occurs post-assessment if needed. Option B (disregarding) risks missing critical gaps. Option D (marking 'NOT MET') is premature without assessing all evidence. Option C ensures a systematic approach, recording gaps for later scoring consideration.

Extract from Official Document (CAP v1.0):

\* Section 2.2 - Conduct Assessment (pg. 25): "Incomplete documents should be recorded as evidence gaps. The Assessment Team shall methodically document all gaps and proceed with assessing the practice based on the remaining available evidence."

References:

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

#### 질문 # 140

After completing a CMMC assessment, the OSC should hash all the evidence artifacts in accordance with the CMMC Artifact Hashing Tool User Guide. However, you have just realized that this requirement was not fulfilled, and the OSC Assessment Official cannot be reached to confirm it was done. To avoid any issues, you quickly complete this step and later inform the OSC Assessment Official. Which CoPC principle have you just violated by hashing the evidence artifacts in place of the OSC?

- A. Objectivity
- **B. Information Integrity**
- C. Professionalism
- D. Confidentiality

정답: B

설명:

Comprehensive and Detailed in Depth Explanation:

Hashing evidence artifacts is the OSC's responsibility to ensure their integrity, not the Lead Assessor's. By performing this task, the Lead Assessor compromises the evidence package's integrity, violating the CoPC's Information Integrity principle. Option A (Professionalism) is not directly breached here. Option B (Confidentiality) is unrelated, as no disclosure occurred. Option C (Objectivity) is unaffected by this action.

Option D is the correct violation.

Extract from Official Document (CoPC):

\* Paragraph 3.4(2) - Information Integrity (pg. 7): "Ensure that actions taken do not compromise the integrity of evidence packages, which is the responsibility of the OSC." References:

CMMC Code of Professional Conduct, Paragraph 3.4(2).

#### 질문 # 141

During your on-site assessment, you examine an OSC's network architecture and the components that make up its defined security boundary. You notice various network devices, servers, and endpoints that are considered part of the OSC's information system. Additionally, the design team also uses a 3D printer to produce model prototypes. Which of the following is not a boundary component?

- A. The virtualization systems
- B. The router
- C. The gateway
- **D. The 3D printer**

정답: D

설명:

Comprehensive and Detailed Explanation:

Boundary components in the CMMC Assessment Scope - Level 2 are network infrastructure elements (e.g., routers, gateways, virtualization systems) that define and protect the security boundary. The 3D printer, while a Specialized Asset if tied to CUI-related prototyping, is a peripheral device, not a core boundary component like Options A, C, and D. It doesn't inherently define or secure the network boundary, making B the correct answer.

Reference:

CMMC Assessment Scope - Level 2, Section 2.2 (Boundary Definition), p. 4: "Boundary components include network devices and systems, not ancillary equipment."

#### 질문 # 142

A CCA who works for a C3PAO doubles as a penetration tester. When conducting a CMMC assessment for an OSC, he realizes their cybersecurity practices are lacking. Recognizing potential vulnerabilities in their systems, the CCA approaches the OSC's cyber team and offers his penetration testing services. Which CoPC guiding principle or practice has the CCA failed to live up to?

그 외, KoreaDumps CMMC-CCA 시험 문제집 일부가 지금은 무료입니다: <https://drive.google.com/open?id=1u5uzulwA-7qgrfilhwZc2qLRc7s4hH-u>