

# Review CMMC-CCP Guide, Trustworthy CMMC-CCP Source

## Table of Contents

1.0	CMMC Ecosystem	18
2.0	CMMC-AB Code of Professional Conduct (Ethics)	36
3.0	CMMC Governance and Source Document	46
4.0	Scoping	96
5.0	CMMC Assessment Process	120
6.0	CMMC Model Construct and Implementation Evaluation	144
	Access Control (AC) Domain	162
	Audit and Accountability (AU) Domain	210
	Awareness and Training (AT) Domain	231
	Configuration Management (CM) Domain	239
	Identification and Authentication (IA) Domain	261
	Incident Response (IR) Domain	285
	Maintenance (MA) Domain	293
	Media Protection (MP) Domain	307
	Personnel Security (PS) Domain	327
	Physical Protection (PE) Domain	334
	Risk Assessment (RA) Domain	348
	Security Assessment (CA) Domain	357
	Systems and Communications Protection (SC) Domain	368
	System and Information Integrity (SI) Domain	403
7.0	Appendix A: Scoring Practices	420
8.0	Acronym List	428
9.0	Glossary	430
10.0	Index	449

P.S. Free 2026 Cyber AB CMMC-CCP dumps are available on Google Drive shared by Actual4Labs:  
<https://drive.google.com/open?id=1Qz49Kee9rVN8MUEw9z1ghQy1dzV3bIf6>

The cost of registering a CMMC-CCP Certification is quite expensive, ranging between \$100 and \$1000. After paying such an amount, the candidate is sure to be on a tight budget. Actual4Labs provides Cyber AB CMMC-CCP preparation material at very low prices compared to other platforms. We also assure you that the amount will not be wasted and you will not have to pay for the certification a second time. For added reassurance, we also provide up to 1 year of free updates. Free demo version of the actual product is also available so that you can verify its validity before purchasing.

## Cyber AB CMMC-CCP Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none"><li>CMMC Governance and Source Documents: This section of the exam measures the capabilities of legal or compliance advisors, covering key regulatory frameworks that govern cybersecurity compliance. Topics include Federal Contract Information, Controlled Unclassified Information, the role of NIST SP 800-171, DFARS, FAR, and the structure and requirements of CMMC v2.0, including self-assessments and certification levels.</li></ul>

Topic 2	<ul style="list-style-type: none"> <li>• <b>CMMC Model Construct and Implementation Evaluation:</b> This section of the exam measures the evaluative skills of cybersecurity assessors, focusing on the application and assessment of the CMMC model. It includes understanding its levels, domains, practices, and implementation criteria, and how to assess whether organizations meet the required cybersecurity practices using evidence-based evaluation.</li> </ul>
Topic 3	<ul style="list-style-type: none"> <li>• <b>CMMC-AB Code of Professional Conduct (Ethics):</b> This section of the exam measures the integrity of cybersecurity professionals by evaluating their understanding of the CMMC-AB Code of Professional Conduct. It emphasizes ethical responsibilities, including confidentiality, objectivity, professionalism, conflict-of-interest avoidance, and respect for intellectual property, ensuring candidates can uphold ethical standards throughout their CMMC-related duties.</li> </ul>
Topic 4	<ul style="list-style-type: none"> <li>• <b>CMMC Assessment Process (CAP):</b> This section of the exam measures the planning and execution skills of audit and assessment professionals, covering the end-to-end CMMC Assessment Process. This includes planning, executing, documenting, reporting assessments, and managing Plans of Action and Milestones (POA&amp;M) in alignment with DoD and CMMC-AB methodology.</li> </ul>

>> Review CMMC-CCP Guide <<

## Excellent Offers By Actual4Labs - Free Cyber AB CMMC-CCP Dumps Updates and Free Demo

In order to better meet users' need, our CMMC-CCP study questions have set up a complete set of service system, so that users can enjoy our professional one-stop service. We not only in the pre-sale for users provide free demo, when buy the user can choose in we provide in the three versions, at the same time, our CMMC-CCP Training Materials also provides 24-hour after-sales service. Such a perfect one-stop service of our CMMC-CCP test guide, believe you will not regret your choice, and can better use your time, full study, efficient pass the CMMC-CCP exam.

## Cyber AB Certified CMMC Professional (CCP) Exam Sample Questions (Q182-Q187):

### NEW QUESTION # 182

In the CMMC Model, how many practices are included in Level 1?

- A. 72 practices
- B. 110 practices
- C. 17 practices
- **D. 15 practices**

**Answer: D**

Explanation:

CMMC (Cybersecurity Maturity Model Certification) 2.0 Level 1 is designed to protect Federal Contract Information (FCI) and consists of 17 foundational cybersecurity practices. These practices are directly derived from FAR 52.204-21 (Basic Safeguarding of Covered Contractor Information Systems), which outlines minimum security requirements for contractors handling FCI.

Breakdown of CMMC Level 1 Practices: The 17 practices in Level 1 focus on basic cybersecurity hygiene and fall under the following 6 domains:

Access Control (AC)- 4 practices

AC.L1-3.1.1: Limit system access to authorized users

AC.L1-3.1.2: Limit user access to authorized transactions and functions AC.L1-3.1.20: Verify and control connections to external systems AC.L1-3.1.22: Control information posted or processed on publicly accessible systems

Identification and Authentication (IA)- 2 practices IA.L1-3.5.1: Identify and authenticate system users IA.L1-3.5.2: Use multifactor authentication for local and

network access Media Protection (MP)- 1 practice MP.L1-3.8.3: Sanitize media before disposal or reuse Physical Protection (PE)-

4 practices PE.L1-3.10.1: Limit physical access to systems containing FCI PE.L1-3.10.3: Escort visitors and monitor visitor activity

PE.L1-3.10.4: Maintain audit logs of physical access PE.L1-3.10.5: Control and manage physical access devices System and

Communications Protection (SC)- 2 practices SC.L1-3.13.1: Monitor and control communications at system boundaries SC.L1-

3.13.5: Implement subnetworks for publicly accessible system components System and Information Integrity (SI)- 4 practices

SI.L1-3.14.1: Identify, report, and correct system flaws in a timely manner SI.L1-3.14.2: Provide protection from malicious code at designated locations SI.L1-3.14.4: Update malicious code protection mechanisms periodically SI.L1-3.14.5: Perform scans of system components and real-time file scans Official Reference from CMMC 2.0 Documentation The 17 practices for CMMC Level 1 are explicitly listed in the CMMC 2.0 Appendices and Assessment Guide for Level 1, as well as in the FAR 52.204-21 requirements.

These practices represent basic safeguarding measures that all DoD contractors handling FCI must implement.

#CMMC 2.0 Level 1 Summary:

Focus: Basic safeguarding of FCI

Total Practices: 17

Derived From: FAR 52.204-21

Assessment Type: Self-assessment (annual)

Final Verification and Conclusion The correct answer is B. 17 practices as verified from the CMMC 2.0 official documents and FAR 52.204-21 requirements.

### NEW QUESTION # 183

The Lead Assessor is presenting the Final Findings Presentation to the OSC. During the presentation, the Assessment Sponsor and OSC staff inform the assessor that they do not agree with the assessment results.

Who has the final authority for the assessment results?

- A. Assessment Team
- B. Assessment Sponsor
- C. CMMC-AB
- D. C3PAO

**Answer: D**

### NEW QUESTION # 184

When a conflict of interest is unavoidable, a CCP should NOT:

- A. Inform their organization
- B. Take action to minimize its impact
- C. Disclose it to affected stakeholders
- D. Conceal it from the Assessment Team lead

**Answer: D**

Explanation:

CMMC Assessment Process (CAP) and CMMC Code of Professional Conduct emphasize that conflicts of interest (COI) must be disclosed and managed transparently. A Certified CMMC Professional (CCP) is required to:

- \* Inform their organization,
- \* Disclose the COI to the affected stakeholders, and
- \* Take reasonable steps to minimize the impact.

What they must NOT do is conceal it from the Assessment Team Lead or others. Concealing a COI violates the CMMC Code of Professional Conduct and compromises the integrity of the assessment.

Reference Documents:

- \* CMMC Assessment Process (CAP), v1.0
- \* CMMC Code of Professional Conduct, CMMC-AB

### NEW QUESTION # 185

Per DoDI 5200.48: Controlled Unclassified Information (CUI), CUI is marked by whom?

- A. Authorized holder
- B. Information Disclosure Official
- C. DoD OUSD
- D. Presidential authorized Original Classification Authority

**Answer: A**

Explanation:

Who is Responsible for Marking CUI? According to DoDI 5200.48 (Controlled Unclassified Information (CUI)), the responsibility for marking CUI falls on the authorized holder of the information.

- \* Definition of an Authorized Holder

- \* Per DoDI 5200.48, Section 3.4, an authorized holder is anyone who has been granted access to CUI and is responsible for handling, safeguarding, and marking it according to DoD CUI policy.

- \* The authorized holder may be:

- \* A DoD employee

- \* A contractor handling CUI

- \* Any organization or individual authorized to access and manage CUI

- \* DoD Guidance on CUI Marking Responsibilities

- \* DoDI 5200.48, Section 4.2:

- \* The individual creating or handling CUI must apply the appropriate markings as per the DoD CUI Registry guidelines.

- \* DoDI 5200.48, Section 5.2:

- \* The marking responsibility is NOT limited to a specific position like an Information Disclosure Official or a high-level DoD office.

- \* Instead, it is the responsibility of the person or entity generating, handling, or disseminating the CUI.

- \* Why the Other Answer Choices Are Incorrect:

- \* (A) DoD OUSD (Office of the Under Secretary of Defense):

- \* The OUSD plays a policy-setting role but does not directly mark CUI.

- \* (C) Information Disclosure Official:

- \* This role is responsible for public release of information, but marking CUI is the duty of the authorized holder managing the data.

- \* (D) Presidential authorized Original Classification Authority (OCA):

- \* OCAs classify national security information (Confidential, Secret, Top Secret), not CUI, which is not classified information.

Step-by-Step Breakdown: Final Validation from DoDI 5200.48: Per DoDI 5200.48, authorized holders are explicitly responsible for marking CUI, making this the correct answer.

## NEW QUESTION # 186

What is the LAST step when developing an assessment plan for an OSC?

- **A. Obtain and record commitment to the assessment plan.**
- B. Perform certification assessment readiness review.
- C. Verify the readiness to conduct the assessment.
- D. Update the assessment plan and schedule as needed

**Answer: A**

Explanation:

Last Step in Developing an Assessment Plan for an OSC: Developing an assessment plan involves:

- \* Defining the assessment scope (e.g., systems, networks, locations).

- \* Planning test activities (e.g., interviews, evidence review, technical testing).

- \* Verifying the OSC's readiness (e.g., ensuring required documents are available).

- \* Updating the assessment plan and schedule as needed.

- \* Final Step: Obtaining and recording the OSC's commitment to the assessment plan.

Why is obtaining commitment the last step? # The assessment cannot proceed unless the OSC agrees to the finalized plan.

# This ensures OSC leadership understands the scope, timeline, and responsibilities.

# The C3PAO must document this commitment to formalize the agreement.

- \* A. Verify the readiness to conduct the assessment # Incorrect

- \* Readiness verification happens earlier in the planning process, not as the last step.

- \* B. Perform certification assessment readiness review # Incorrect

- \* A readiness review is conducted before finalizing the plan, not at the very end.

- \* C. Update the assessment plan and schedule as needed # Incorrect

- \* Updating the plan happens before commitment is obtained; it is not the final step.

- \* D. Obtain and record commitment to the assessment plan # Correct

- \* This is the final step before conducting the assessment. The OSC must formally agree to the plan.

Why is the Correct Answer "D. Obtain and record commitment to the assessment plan"?

- \* CMMC Assessment Process (CAP) Document

- \* States that the OSC must confirm agreement to the assessment plan before execution.

- \* CMMC-AB Guidelines for C3PAOs

- \* Specifies that finalizing the assessment plan requires documented commitment from the OSC.

- \* CMMC Assessment Guide

Final Answer:#D. Obtain and record commitment to the assessment plan.

• • • • •

**Trustworthy CMMC-CCP Source:** <https://www.actual4labs.com/Cyber-AB/CMMC-CCP-actual-exam-dumps.html>

- BONUS!!! Download part of Actual4Labs CMMC-CCP dumps for free: <https://drive.google.com/open?id=1Oz49Kee9rVN8MUEw9z1ghOv1dzV3b1fe>