



Download Cyber AB CMMC-CCP Exam Dumps Free

Shared by May on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page



Question 1

Question Type: MultipleChoice

What is objectivity as it applies to activities with the CMMC-AB?

Options:

- A- Ensuring full disclosure
- B- Reporting results of CMMC services completely
- C- Avoiding the appearance of or actual, conflicts of interest
- D- Demonstrating integrity in the use of materials as described in policy

Answer:

C

Explanation:

Understanding Objectivity in CMMC-AB Activities
Objectivity in CMMC-AB activities refers to the requirement that assessors and C3PAOs remain impartial, unbiased, and free from conflicts of interest while conducting assessments and providing CMMC-related services.

Key Aspects of Objectivity in CMMC Assessments:
No conflicts of interest---Assessors must not assess organizations they have financial, professional, or personal ties to.

Unbiased reporting---Findings must be based solely on evidence, with no external influence.

Avoiding even the appearance of a conflict---If there is any perception of bias, it must be addressed.

A . Ensuring full disclosure Incorrect

Full disclosure is important but does not define objectivity. Objectivity means remaining neutral and free from conflicts.

B . Reporting results of CMMC services completely Incorrect

While accurate reporting is required, objectivity focuses on impartiality, not just completeness.

C . Avoiding the appearance of or actual, conflicts of interest Correct

Objectivity in CMMC-AB activities is primarily about preventing bias and ensuring fair assessments.

Avoiding conflicts of interest ensures that assessments are credible and trustworthy.

D . Demonstrating integrity in the use of materials as described in policy Incorrect

Integrity is important, but objectivity is specifically about avoiding bias and conflicts of interest.

Why is the Correct Answer 'C. Avoiding the appearance of or actual, conflicts of interest'?

CMMC-AB Code of Professional Conduct

Requires assessors and C3PAOs to avoid conflicts of interest and maintain impartiality.

CMMC Assessment Process (CAP) Document

Emphasizes that assessments must be free from external influence and conflicts of interest.

ISO/IEC 17020 Requirements for Inspection Bodies

Defines objectivity as avoiding conflicts of interest in the assessment process.

CMMC 2.0 Reference Supporting This Answer:

Question 2

Question Type: MultipleChoice

Which entity specifies the required CMMC Level in Requests for Information and Requests for Proposals?

Options:

A- DoD

B- NARA

C- NIST

D- Department of Homeland Security

Answer:

A

Explanation:

The U.S. Department of Defense (DoD) determines the required CMMC Level based on the sensitivity of the information involved in a contract.

The required CMMC Level is specified in Requests for Information (RFIs) and Requests for

Proposals (RFPs).

DFARS 252.204-7021 (CMMC Requirements)

CMMC 2.0 Program Documentation

Step 2: Why Other Answer Choices Are Incorrect

B. NARA (Incorrect):
The National Archives and Records Administration (NARA) oversees CUI program policies but does not assign CMMC levels.

C. NIST (Incorrect):

The National Institute of Standards and Technology (NIST) develops cybersecurity frameworks (e.g., NIST SP 800-171), but it does not specify CMMC Levels in contracts.

D. Department of Homeland Security (Incorrect):

The Department of Homeland Security (DHS) is responsible for cybersecurity at the national level, but CMMC applies specifically to DoD contractors.

Final Confirmation of Correct Answer: The DoD determines and specifies the required CMMC Level in RFIs and RFPs.

Question 3

Question Type: MultipleChoice

Exercising due care to ensure the information gathered during the assessment is protected even after the engagement has ended meets which code of conduct requirement?

Options:

- A- Availability
- B- Confidentiality
- C- Information Integrity
- D- Respect for Intellectual Property

Answer:

B

Explanation:

The requirement to exercise due care in protecting information gathered during an assessment aligns with the principle of Confidentiality under the CMMC Code of Professional Conduct (CoPC). This ensures that sensitive assessment data, findings, and any Controlled Unclassified Information (CUI) remain protected even after the engagement concludes.

Definition of Confidentiality in CMMC Context:

Confidentiality refers to protecting sensitive information from unauthorized disclosure.

In the context of a CMMC assessment, it includes safeguarding assessment artifacts, findings, and other sensitive data collected during the evaluation process.

CMMC Code of Professional Conduct (CoPC) Reference:

The CMMC Code of Professional Conduct states that assessors and organizations must handle all collected information with discretion and ensure its protection post-engagement.

Clause on 'Maintaining Confidentiality' specifies that assessors must:

Not disclose sensitive information to unauthorized parties.

Secure data in storage and transmission.

Retain and dispose of data securely in accordance with federal regulations.

Alignment with NIST 800-171 & CMMC Practices:

CMMC Level 2 incorporates NIST SP 800-171 controls, which include:

Requirement 3.1.3: "Control CUI at rest and in transit" to ensure unauthorized individuals do not gain access.

Requirement 3.1.4: "Separate the duties of individuals to reduce risk" ensures that assessment findings are only shared with authorized personnel.

These requirements align with the duty to exercise due care in protecting assessment-related information.

Why the Other Options Are Incorrect:

(A) Availability: This refers to ensuring data is accessible when needed but does not directly relate to protecting gathered information post-assessment.

(C) Information Integrity: This focuses on preventing unauthorized modifications rather than restricting disclosure.

(D) Respect for Intellectual Property: While related to ethical handling of proprietary data, it does not directly cover post-engagement confidentiality requirements.

The CMMC Code of Professional Conduct and NIST SP 800-171 control requirements confirm that Confidentiality is the correct answer, as it directly pertains to protecting information post-

assessment.

Step-by-Step Breakdown:Final Validation from CMMC Documentation:Thus, the correct answer is B. Confidentiality.

Question 4

Question Type: MultipleChoice

An OSC receives an email with "CUI//SP-PRVCY//FED Only" in the body of the message Which organization's website should the OSC go to identify what this marking means?

Options:

- A- NARA
- B- CMMC-AB
- C- DoD Contractors FAQ page
- D- DoD 239.7601 Definitions page

Answer:

A

Explanation:

What Does 'CUI//SP-PRVCY//FED Only' Mean?

The email contains Controlled Unclassified Information (CUI) with specific categories and dissemination controls.

CUI//SP-PRVCY//FED Only breaks down as follows:

CUI Controlled Unclassified Information designation.

SP-PRVCY Specified category for Privacy Information (SP stands for 'Specified').

FED Only Restriction for Federal Government use only (not for contractors or the public).

Who Maintains the Official CUI Registry?

The National Archives and Records Administration (NARA) oversees the CUI Program and maintains the official CUI Registry (<https://www.archives.gov/cui>).

The CUI Registry provides definitions, marking guidance, and categories for all CUI labels,

including 'SP-PRVCY' and dissemination controls like 'FED Only.'

Why NARA is the Correct Answer:

NARA is the governing body responsible for defining and managing CUI markings.

Any organization handling CUI should refer to the NARA CUI Registry for official marking interpretations.

DoD contractors and other organizations must comply with NARA guidelines when handling, marking, and disseminating CUI.

B . CMMC-AB-- The CMMC Accreditation Body manages certification assessments but does not define or interpret CUI markings.

C . DoD Contractors FAQ Page-- The DoD may provide general contractor guidance, but CUI markings are governed by NARA, not an FAQ page.

D . DoD 239.7601 Definitions Page-- This refers to general DoD acquisition definitions, but CUI categories and markings fall under NARA's authority.

DoD CUI Program Guidance (DoD CIO Site)

CMMC 2.0 Level 2 Compliance Requirements (Cyber AB)

Final Answer: A. NARA

Question 5

Question Type: MultipleChoice

In many organizations, the protection of FCI includes devices that are used to scan physical documentation into digital form and print physical copies of digital FCI. What technical control can be used to limit multi-function device (MFD) access to only the systems authorized to access the MFD?

Options:

- A- Virtual LAN restrictions
- B- Single administrative account
- C- Documentation showing MFD configuration
- D- Access lists only known to the IT administrator

Answer:

A

Explanation:

Understanding Multi-Function Device (MFD) Security in CMMC Multi-function devices (MFDs), such as scanners, printers, and copiers, process, store, and transmit FCI, making them a potential attack surface for unauthorized access.

The best technical control to limit MFD access to only authorized systems is Virtual LAN (VLAN) restrictions, which segment and isolate network traffic.

VLAN Restrictions Provide Network Segmentation

VLANs isolate the MFD from unauthorized systems, ensuring only approved devices can communicate with it.

Prevents unauthorized network access by limiting connections to specific IPs or subnets.

Meets CMMC 2.0 Network Security Controls

Aligns with CMMC System and Communications Protection (SC) Practices for network segmentation and access control.

Reduces the risk of unauthorized access to scanned and printed FCI.

B . Single administrative account Incorrect

A single admin account does not restrict access between devices, only controls who can configure the MFD.

C . Documentation showing MFD configuration Incorrect

Documentation helps with compliance but does not actively restrict access.

D . Access lists only known to the IT administrator Incorrect

Access lists should be system-enforced, not just 'known' to the administrator.

CMMC Practice SC.3.192 (Network Segmentation)-- Requires restricting access using network segmentation techniques such as VLANs.

NIST SP 800-171 (SC Family)-- Supports isolation of sensitive devices using VLANs and other segmentation controls.

Why the Correct Answer is 'A. Virtual LAN (VLAN) Restrictions'? Why Not the Other Options? Relevant CMMC 2.0 Reference: Final Justification: Since Virtual LAN (VLAN) restrictions enforce access control at the network level, the correct answer is A. Virtual LAN (VLAN) restrictions.

Question 6

Question Type: MultipleChoice

A contractor stores security policies, system configuration files, and audit logs in a centralized file repository for later review. According to CMMC terminology, the file repository is being used to:

Options:

- A- protect CUI.
- B- transmit CUI.
- C- store CUI.
- D- generate CUI



Answer:

C

Question 7

Question Type: MultipleChoice

During assessment planning, the OSC recommends a person to interview for a certain practice. The person being interviewed MUST be the person who:

Options:

- A- funds that practice.
- B- audits that practice.
- C- supports, audits, and performs that practice.
- D- implements, performs, or supports that practice.



Answer:

D

Explanation:

Who Should Be Interviewed During a CMMC Assessment? During assessment planning,

the Organization Seeking Certification (OSC) may suggest personnel for interviews. However, the person interviewed must be someone who:

Implements the practice (directly responsible for executing it).

Performs the practice (carries out day-to-day security operations).

Supports the practice (provides necessary resources or oversight).

The assessor needs direct insights from individuals actively involved in the practice.

Funding (Option A) does not provide technical or operational insight into practice execution.

Auditing (Option B) focuses on compliance checks, but auditors do not implement the practice.

Supporting, auditing, and performing (Option C) includes auditors, who are not necessarily the right interviewees.

Why 'Implements, Performs, or Supports That Practice' is Correct? Breakdown of Answer Choices

Description

Correct?

A . Funds that practice.

Incorrect--Funding is important but does not mean direct involvement.

B . Audits that practice.

Incorrect--Auditors check compliance but do not implement practices.

C . Supports, audits, and performs that practice.

Incorrect--Auditing is not a requirement for interviewees.

D . Implements, performs, or supports that practice.

Correct -- The interviewee must have direct involvement in execution.

CMMC Assessment Process Guide (CAP)-- Requires that interviewees be directly responsible for implementing, performing, or supporting the practice.

Official Reference from CMMC 2.0 Documentation Final Verification and Conclusion The correct answer is D. Implements, performs, or supports that practice, as the interviewee must actively contribute to the execution of the practice.

Question 8

Question Type: MultipleChoice

As defined in the CMMC-AB Code of Professional Conduct, what term describes any contract between two legal entities?

Options:

- A- Union
- B- Accord
- C- Alliance
- D- Agreement



Answer:

D

Explanation:

Understanding the Definition of an Agreement in the CMMC-AB Code of Professional Conduct
The CMMC-AB Code of Professional Conduct defines an agreement as any contract between two legal entities. This includes:

Contracts between an OSC and a C3PAO for CMMC assessments.

Service agreements between cybersecurity providers and defense contractors.

Any formal, legally binding arrangement related to CMMC compliance.

A . Union Incorrect

A union typically refers to an organization representing workers and is not used to describe a contractual relationship.

B . Accord Incorrect

While an accord can mean an agreement, it is not the standard legal term for a binding contract in CMMC documentation.

C . Alliance Incorrect

An alliance refers to a strategic partnership, but does not necessarily imply a legally binding contract.

D . Agreement Correct

The CMMC-AB Code of Professional Conduct defines an agreement as any legally binding contract between two entities.

Why is the Correct Answer 'D. Agreement'?

CMMC-AB Code of Professional Conduct

Defines 'Agreement' as a legally binding contract between two parties.

CMMC-AB Licensed Training and Assessment Provider Guidelines

Requires that all engagements be governed by a formal agreement (contract) between the parties.

DFARS and CMMC Certification Contracts

States that OSC-C3PAO relationships must be formalized through a legal agreement.

CMMC 2.0 Reference Supporting This Answer:

Question 9

Question Type: MultipleChoice

A C3PAO is near completion of a Level 2 Assessment for an OSC. The CMMC Findings Brief and CMMC Assessment Results documents have been developed. The Final Recommended Assessment Results are being generated. When generating these results, what MUST be included?

Options:

- A- An updated Assessment Plan
- B- Recorded and final updated Daily Checkpoint
- C- Fully executed CMMC Assessment contract between the C3PAO and the OSC
- D- Review documentation for the CMMC Quality Assurance Professional (CQAP)

Answer:

D

Explanation:

AC3PAO (Certified Third-Party Assessment Organization) is responsible for conducting CMMC Level

2 assessments.

After completing the assessment, the C3PAO generates the Final Recommended Assessment Results, which include key documentation reviewed by the CMMC Quality Assurance Professional (CQAP) for quality control.

CMMC Assessment Process (CAP) Guide

Step 2: Role of the CMMC Quality Assurance Professional (CQAP) The CQAP is responsible for reviewing assessment documentation to ensure it aligns with CMMC requirements and DoD expectations.

Before finalizing the assessment results, the C3PAO must include documentation for CQAP review to maintain compliance.

Step 3: Why Other Answer Choices Are Incorrect A. An updated Assessment Plan (Incorrect):

The Assessment Plan is developed before the assessment begins, not during the final recommended results phase.

B . Recorded and final updated Daily Checkpoint (Incorrect):

Daily Checkpoints are internal tracking tools used during assessments, but they are not mandatory for final results.

C . Fully executed CMMC Assessment contract between the C3PAO and the OSC (Incorrect):

While a contract is required for the assessment, it is not part of the Final Recommended Assessment Results.

Final Confirmation of Correct Answer: Review documentation for the CMMC Quality Assurance Professional (CQAP) must be included in the Final Recommended Assessment Results.

Thus, the correct answer is: D. Review documentation for the CMMC Quality Assurance Professional (CQAP)

Question 10

Question Type: MultipleChoice

During a CMMC readiness review, the OSC proposes that an associated enclave should not be applicable in the scope. Who is responsible for verifying this request?

Options:

- A- CCP
- B- C3PAO
- C- Lead Assessor
- D- Advisory Board

Answer:

C

Explanation:

During a CMMC readiness review, an Organization Seeking Certification (OSC) may argue that a specific enclave (network segment or system) is out of scope for assessment. The Lead Assessor is responsible for verifying and approving this request.

Certified CMMC Professional (CCP)

A CCP supports OSCs in preparing for assessments but does not make final scope determinations.

Certified Third-Party Assessment Organization (C3PAO)

The C3PAO oversees the assessment but does not personally verify scope exclusions---that falls under the Lead Assessor's role.

Lead Assessor (Correct Answer)

The Lead Assessor has the authority to determine if an enclave is out of scope based on OSC-provided evidence.

The Lead Assessor follows CMMC Assessment Process (CAP) guidelines to ensure proper scoping.

Advisory Board

The CMMC-AB (Advisory Board) does not make scope determinations. It focuses on program oversight and certification processes.

CMMC Assessment Process (CAP) v1.0

The Lead Assessor is responsible for confirming the assessment scope and determining enclave applicability.

CMMC Scoping Guidance for Level 2 Assessments

Requires the Lead Assessor to review and approve any enclave exclusions before finalizing the assessment scope.

Roles and Responsibilities in CMMC Assessments: Official Reference Supporting the Correct Answer: Conclusion: The Lead Assessor is the correct answer because they have the authority to verify scope determinations during the assessment.

Correct Answer: C. Lead Assessor

Question 11

Question Type: MultipleChoice

There are 15 practices that are NOT MET for an OSC's Level 2 Assessment. All practices are applicable to the OSC. Which determination should be reached?

Options:

- A- The OSC may have 90 days for remediating NOT MET practices.
- B- The OSC is not eligible for an option to remediate NOT MET practices.
- C- The OSC may be eligible for an option to remediate NOT MET practices.
- D- The OSC is not eligible for an option to remediate after the assessment is canceled.

Answer:

B

Explanation:

In the context of the Cybersecurity Maturity Model Certification (CMMC) 2.0, achieving Level 2 compliance requires an Organization Seeking Certification (OSC) to implement all 110 security practices outlined in NIST SP 800-171 Revision 2. The CMMC framework allows for a limited use of Plans of Action and Milestones (POA&Ms) to address certain deficiencies; however, this is contingent upon meeting specific criteria.

According to the final CMMC rule, to obtain a Conditional Level 2 status, an OSC must achieve a minimum score of 88 out of 110 points during the assessment. This scoring system assigns weighted values to each of the 110 security requirements, with some controls deemed critical and others non-critical. The POA&M mechanism permits OSCs to temporarily address non-critical deficiencies, provided the minimum score threshold is met. Critical controls, however, must be fully implemented at the time of assessment; they cannot be deferred and included in a POA&M.

MWE

In the scenario where 15 practices are NOT MET, the OSC's score would fall below the required 88-point threshold, rendering the organization ineligible for Conditional Level 2 status. Consequently, the OSC would not have the option to remediate these deficiencies through a POA&M. Instead, the organization must fully implement and rectify all NOT MET practices before undergoing a subsequent assessment to achieve the necessary compliance level.

This policy ensures that organizations handling Controlled Unclassified Information (CUI) have adequately addressed all critical and non-critical security requirements, thereby maintaining the integrity and security of sensitive information within the Defense Industrial Base.

For detailed guidance on assessment criteria and the use of POA&Ms, refer to the CMMC Assessment Guide -- Level 2 and the official CMMC documentation provided by the Department of Defense.



To Get Premium Files for CMMC-CCP Visit

<https://www.p2pexams.com/products/cmmc-ccp>

For More Free Questions Visit

<https://www.p2pexams.com/cyber-ab/pdf/cmmc-ccp>

20%
DISCOUNT

P2P
exams