



Cyber AB CMMC-CCP Practice Questions

Shared by Dixon on 12-10-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page



Question 1

Question Type: MultipleChoice

On a Level 2 Assessment Team, what are the roles of the CCP and the CCA?

Options:

- A- The CCP leads the Level 2 Assessment Team, which consists of one or more CCAs.
- B- The CCA leads the Level 2 Assessment Team, which can include 3 CCP with US Citizenship.
- C- The CCA leads the Level 2 Assessment Team, which can include a CCP regardless of citizenship.
- D- The CCP leads the Level 2 Assessment Team, which can include a CCA. regardless of citizenship.

Answer:

C

Explanation:

Step 1: Define Roles -- CCP and CCA

CCP (Certified CMMC Professional):

Entry-level certification in the CMMC ecosystem.

Supports assessment activities under the supervision of a CCA.

May assist in consulting roles outside of formal assessments.

CCA (Certified CMMC Assessor):

Certified to lead assessments under the CMMC model.

Required for conducting Level 2 formal assessments.

Can be part of a C3PAO assessment team or lead it.

Source: CMMC Assessment Process (CAP) v1.0, Section 2.3 -- Assessment Team Composition

"Level 2 assessments must be led by a Certified CMMC Assessor (CCA), who may be supported by one or more CCPs."

Step 2: Citizenship Requirements

CAP v1.0 -- Appendix B: Team Composition and Clearance Requirements

"All team members performing Level 2 assessments must be U.S. citizens when handling CUI, regardless of role."

But for supporting team members who do not handle CUI or in FCI-only scoping, there is no automatic exclusion based on citizenship.

So:

The CCA leads the team.

CCPs can be team members regardless of citizenship, unless restricted by contract or CUI handling needs.

Why the Other Options Are Incorrect

A . The CCP leads the Level 2 Assessment Team...

Incorrect. CCPs cannot lead Level 2 assessments.

B . The CCA leads... includes 3 CCP with US Citizenship.

Incorrect. Citizenship is required only when handling CUI, not a universal requirement.

D . The CCP leads...

Again, CCPs do not have the authority to lead formal CMMC assessments.

Only a Certified CMMC Assessor (CCA) may lead a Level 2 Assessment Team, and they may include CCPs, even non-U.S. citizens, if citizenship is not a requirement based on contractual or data sensitivity scope.

Question 2

Question Type: Multiple Choice

The practices in CMMC Level 2 consists of the security requirements specified in:

Options:

A- NIST SP 800-53.

B- NIST SP 800-171.

C- 48 CFR 52.204-21.

D- DFARS 252.204-7012.

Answer:

B

Explanation:

The Cybersecurity Maturity Model Certification (CMMC) Level 2 is designed to ensure that organizations can adequately protect Controlled Unclassified Information (CUI). To achieve this, CMMC Level 2 incorporates specific security requirements.

Step-by-Step

Alignment with NIST SP 800-171:

CMMC Level 2 aligns directly with the security requirements outlined in the National Institute of Standards and Technology Special Publication 800-171 (NIST SP 800-171). This publication, titled 'Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations,' provides a comprehensive framework for safeguarding CUI.

Incorporation of Security Requirements:

The practices required for CMMC Level 2 certification encompass all 110 security requirements specified in NIST SP 800-171. These requirements are organized into 14 families, each addressing different aspects of cybersecurity, such as access control, incident response, and risk assessment.

Purpose of Alignment:

By integrating the NIST SP 800-171 requirements, CMMC Level 2 aims to standardize the implementation of cybersecurity practices across organizations handling CUI, ensuring a consistent and robust approach to protecting sensitive information.

CMMC Model Overview Version 2.13, which details the incorporation of NIST SP 800-171 requirements into CMMC Level 2 practices.

Dodcio

This alignment underscores the importance of adhering to established federal guidelines to maintain the security and integrity of CUI within nonfederal systems.

Question 3

Question Type: MultipleChoice

During Phase 4 of the Assessment process, what MUST the Lead Assessor determine and recommend to the C3PAO concerning the OSC?

Options:

- A- Ability
- B- Eligibility
- C- Capability
- D- Suitability

Answer:

B

Explanation:

What Happens in Phase 4 of the CMMC Assessment Process? Phase 4 of the CMMC Assessment Process (CAP) is the Final Reporting and Decision Phase. During this phase, the Lead Assessor must:

Review all assessment findings

Determine the Organization Seeking Certification's (OSC) eligibility for certification

Make a recommendation to the C3PAO (Certified Third-Party Assessment Organization)

Ensure that the OSC has met the required practices and processes.

Confirm that any deficiencies have been corrected or appropriately documented.

Recommend whether the OSC is eligible for certification based on assessment results.

Key Responsibilities of the Lead Assessor in Phase 4: Since the Lead Assessor must determine and recommend the OSC's eligibility to the C3PAO, the correct answer is B. Eligibility.

A . Ability Incorrect. While assessing an OSC's ability to meet CMMC requirements is part of the process, the final determination in Phase 4 is about eligibility for certification.

C . Capability Incorrect. Capability refers to an organization's technical and operational readiness. The Lead Assessor is making a recommendation on eligibility, not just capability.

D . Suitability Incorrect. Suitability is not a defined term in the CMMC CAP process for final assessment recommendations. The correct term is eligibility.

Why the Other Answers Are Incorrect

CMMC Assessment Process (CAP) Document-- Specifies that the Lead Assessor must determine and recommend the eligibility of the OSC in Phase 4.

CMMC 2.0 Model-- Defines the assessment process, including certification decision-making.

CMMC Official Reference Thus, option B (Eligibility) is the correct answer, as per official CMMC guidance.

Question 4

Question Type: MultipleChoice

A CCP is working as an Assessment Team Member on a CMMC Level 2 Assessment. The Lead Assessor has assigned the CCP to assess the OSC's Configuration Management (CM) domain. The CCP's first interview is with a subject-matter expert for user-installed software. With respect to user-installed software, what facet should the CCP's interview focus on?

Options:

- A- Controlled and monitored
- B- Removed from the system
- C- Scanned for malicious code
- D- Limited to mission-essential use only

Answer:

A

Explanation:

Understanding Configuration Management (CM) in CMMC Level 2
In CMMC Level 2, the Configuration Management (CM) domain is critical for ensuring that systems are securely configured, maintained, and monitored to prevent unauthorized changes. One key aspect of CM is managing user-installed software, which can introduce security risks if not properly controlled.

The correct approach to managing user-installed software aligns with CM.3.068 from NIST SP 800-171, which requires organizations to:

Establish and enforce configuration settings to ensure security.

Monitor and control user-installed software to prevent unauthorized or insecure applications from running on organizational systems.

Why 'Controlled and Monitored' is Correct? The CCP (Certified CMMC Professional) conducting the interview should focus on whether the user-installed software is controlled and monitored to align with CMMC Level 2 requirements. This means verifying:

Approval processes for user-installed software.

Monitoring mechanisms (e.g., system logs, audits) to track software changes.

Policies that restrict unauthorized installation to prevent security risks.

Breakdown of Answer ChoicesOption

Description

Correct?

A . Controlled and monitored

Ensures compliance with CM.3.068, verifying that user-installed software is managed securely.

Correct

B . Removed from the system

Software is not always removed--only unauthorized or risky software should be.

Incorrect

C . Scanned for malicious code

While scanning is important (covered in SI.3.218), it is not the primary focus of Configuration Management.

Incorrect

D . Limited to mission-essential use only

While limiting software is useful, monitoring and controlling is the key security measure.

Incorrect

NIST SP 800-171, CM.3.068-- 'Control and monitor user-installed software.'

CMMC 2.0 Level 2 Requirements-- Directly aligned with NIST SP 800-171 security controls.

Official Reference from CMMC 2.0 Documentation Final Verification and Conclusion The correct answer is A. Controlled and monitored, as per CM.3.068 in NIST SP 800-171 and CMMC 2.0 documentation.

Question 5

Question Type: MultipleChoice

Plan of Action defines the clear goal or objective for the plan. What information is generally NOT a part of a plan of action?

Options:

- A- Completion dates
- B- Milestones to measure progress
- C- Ownership of who is accountable for ensuring plan performance
- D- Budget requirements to implement the plan's remediation actions

Answer:

D

Explanation:

Under the Cybersecurity Maturity Model Certification (CMMC) 2.0, a Plan of Action (POA) is a critical document that outlines the specific actions a contractor needs to take to remediate cybersecurity deficiencies. While POAs serve as a roadmap for achieving compliance with required controls, the inclusion of certain elements is standardized.

Key Elements of a Plan of Action (POA)

According to the CMMC guidelines and NIST SP 800-171, which underpins many CMMC requirements, a POA typically includes:

Completion Dates: Identifies target deadlines for resolving deficiencies.

Milestones to Measure Progress: Includes interim steps or markers to ensure progress is monitored over time.

Ownership or Accountability: Clearly assigns responsibility for each action item to specific personnel or teams.

What is Generally NOT Part of a POA?

Budget requirements to implement the plan's remediation actions (Option D) are generally not included in a POA. While budgeting is critical for ensuring the plan's success, it is considered a part of the broader project management or resource planning process, not the POA itself. This distinction is intentional to keep the POA focused on actionable items rather than resource allocation.

Supporting Reference

NIST SP 800-171A, Appendix D: Provides an overview of POA components, emphasizing the prioritization of corrective actions, responsibility, and measurable outcomes.

CMMC Level 2 Practices (Aligned with NIST SP 800-171): Specifically, the focus is on actions, timelines, and accountability rather than financial planning.

By excluding budget details, the POA remains a tactical document that supports immediate action and compliance tracking, separate from financial considerations.

Question 6

Question Type: MultipleChoice

An Assessment Team is conducting a Level 2 Assessment at the request of an OSC. The team has begun to score practices based on the evidence provided. At a MINIMUM what is required of the Assessment Team to determine if a practice is scored as MET?

Options:

- A- All three types of evidence are documented for every control.
- B- Examine and accept evidence from one of the three evidence types.
- C- Complete one of the following; examine two artifacts, either observe a satisfactory demonstration of one control or receive one affirmation from the OSC personnel.
- D- Complete two of the following: examine one artifact, either observe a satisfactory demonstration of one control or receive one affirmation from the OSC personnel.

Answer:

D

Explanation:

This question pertains to the minimum evidence requirements needed by a CMMC Assessment Team to score a practice as MET during a Level 2 Assessment.

The CMMC Level 2 assessment must align with NIST SP 800-171 and follow the procedures outlined in the CMMC Assessment Process (CAP) Guide v1.0, particularly around evidence collection and scoring methodology.

Step 1: Refer to the CMMC Assessment Process (CAP) Guide v1.0 CAP v1.0 -- Section 3.5.4: Evaluate Evidence and Score Practices "To assign a MET determination, the Assessment Team must collect and corroborate at least two types of objective evidence: either through examination of artifacts, interviews (affirmation), or testing (demonstration)."

This means at least two types of the following evidence are required:

Examine (documentation/artifacts),

Interview (affirmation from personnel),

Test (demonstration of implementation).

Step 2: Clarify the Official Minimum Standard for a Practice to be Scored MET The CAP explicitly states:

"A practice can only be scored MET when a minimum of two types of evidence from the E-I-T

(Examine, Interview, Test) triad are successfully collected and evaluated."

The evidence types must come from two different categories, for example:

An artifact(Examine)+ an interview affirmation(Interview),

A demonstration(Test)+ an interview(Interview),

Etc.

This cross-validation ensures that the control is implemented, documented, and understood by personnel --- a core principle in assessing effective cybersecurity implementation.

Why the Other Options Are Incorrect
A. All three types of evidence are documented for every control. **Incorrect:** While collecting all three types (E-I-T) strengthens the assessment, the minimum requirement is only two. Collecting all three is not required for a practice to be scored MET.

B. Examine and accept evidence from one of the three evidence types. **Incorrect:** This fails to meet the minimum two-evidence-type requirement set by the CAP. Single-source evidence is not sufficient to score a practice as MET.

C. Complete one of the following; examine two artifacts, observe one demonstration, or receive one affirmation. **Incorrect:** Even if two artifacts are examined, this is still only one type of evidence (Examine). The CAP requires two types --- not two instances of the same type.

Why D is Correct
D. Complete two of the following: examine one artifact, either observe a satisfactory demonstration of one control or receive one affirmation from the OSC personnel.

This directly reflects the CAP's requirement for collecting two different types of objective evidence to determine a practice is MET.

BLUF (Bottom Line Up Front): To score a CMMC Level 2 practice as MET, the Assessment Team must collect a minimum of two distinct types of evidence --- from the Examine, Interview, Test (E-I-T) categories. This requirement is clearly stated in the CMMC Assessment Process (CAP) v1.0.

Question 7

Question Type: Multiple Choice

What are CUI protection responsibilities?

Options:

A- Shielding

B- Governing

- C- Correcting
- D- Safeguarding

Answer:

D

Explanation:

Understanding CUI Protection Responsibilities Controlled Unclassified Information (CUI) is sensitive but not classified information that requires protection under DoD Instruction 5200.48 and DFARS 252.204-7012.

The primary responsibility for handling CUI is safeguarding it against unauthorized access, disclosure, or modification.

The CUI Program (as per NARA and DoD) mandates safeguarding measures to protect CUI in both digital and physical forms.

CMMC 2.0 Level 2 (Advanced) practices align with NIST SP 800-171, which focuses on safeguarding CUI through access controls, encryption, and monitoring.

DFARS 252.204-7012 requires DoD contractors to implement cybersecurity safeguards to protect CUI.

A . Shielding (Incorrect)--Shielding is not a cybersecurity term associated with CUI protection.

B . Governing (Incorrect)--Governing refers to policy-making, not direct protection.

C . Correcting (Incorrect)--Correcting implies remediation, but the primary responsibility is to safeguard CUI proactively.

The correct answer is D. Safeguarding, as CUI protection focuses on implementing cybersecurity safeguards.

DoD Instruction 5200.48 (CUI Program)

DFARS 252.204-7012

CMMC 2.0 Level 2 Practices (NIST SP 800-171)

Question 8

Question Type: Multiple Choice

What is the main intent of the verify evidence and record gaps activity?

Options:

- A- Map test and demonstration responses to CMMC practices.
- B- Conduct interviews to test process implementation knowledge.
- C- Determine the one-to-one relationship between a practice and an assessment object.
- D- Identify and describe differences between what the Assessment Team required and the evidence collected.

Answer:

D

Explanation:

Understanding the "Verify Evidence and Record Gaps" Activity in a CMMC Assessment

During a CMMC Level 2 Assessment, the Assessment Team follows a structured methodology to verify evidence and determine whether the Organization Seeking Certification (OSC) has met all required practices. One of the key activities in this process is 'Verify Evidence and Record Gaps', which ensures that the assessment findings accurately reflect any missing or inadequate compliance evidence.

Step-by-Step Breakdown:

1. Primary Intent: Identifying Gaps Between Required and Collected Evidence

The Assessment Team compares the evidence provided by the OSC against the CMMC practice requirements.

If evidence is missing, insufficient, or inconsistent, assessors must document the gap and describe what is lacking.

This ensures that compliance deficiencies are clearly identified, allowing the OSC to understand what must be corrected.

2. How This Process Works in a CMMC Assessment

Assessors review collected documentation, system configurations, policies, and interview responses.

They verify that the evidence matches the expected implementation of a practice.

If gaps exist, they are recorded for discussion and potential remediation before assessment completion.

3. Why the Other Answer Choices Are Incorrect:

(A) Map test and demonstration responses to CMMC practices.

Incorrect: While mapping evidence to CMMC practices is part of the assessment, the primary intent of the 'Verify Evidence and Record Gaps' step is to identify deficiencies, not just mapping responses.

(B) Conduct interviews to test process implementation knowledge.

Incorrect: Interviews are a method used during evidence collection, but they are not the primary focus of the verification and gap analysis step.

(C) Determine the one-to-one relationship between a practice and an assessment object.

Incorrect: The assessment team reviews multiple sources of evidence for each practice, and some practices require multiple assessment objects. The goal is not a strict one-to-one mapping but rather a holistic validation of compliance.

Final Validation from CMMC Documentation:

The CMMC Assessment Process Guide states that 'Verify Evidence and Record Gaps' is the step where assessors compare expected evidence against what has been provided and document discrepancies. This ensures transparent assessment findings and remediation planning.

Thus, the correct answer is:

D. Identify and describe differences between what the Assessment Team required and the evidence collected.

Question 9

Question Type: MultipleChoice

The Advanced Level in CMMC will contain Access Control (AC) practices from:

Options:

A- Level 1

B- Level 3

C- Levels 1 and 2

D- Levels 1, 2, and 3

Answer:

C

Explanation:

In the CMMC 2.0 Model, the 'Advanced Level' specifically refers to Level 2. The CMMC model is designed to be cumulative, meaning each level builds upon the requirements of the levels beneath it.

Cumulative Framework: To achieve a certification at a specific level, an Organization Seeking Certification (OSC) must demonstrate compliance with all practices at that level and all practices from the lower levels.

Access Control (AC) Domain: The Access Control domain is one of the 14 domains in CMMC Level 2. It consists of a total of 22 practices:

Level 1 (Foundational): Contains 4 basic safeguarding practices (mapped to FAR 52.204-21).

Level 2 (Advanced): Adds 18 additional practices (mapped to NIST SP 800-171), totaling 22 practices for the AC domain at this level.

Defining 'Advanced': The DoD defines the levels as Level 1 (Foundational), Level 2 (Advanced), and Level 3 (Expert). Therefore, the 'Advanced Level' (Level 2) contains the practices from Level 1 and Level 2, but does not include the 'Expert' (Level 3) practices, which are derived from NIST SP 800-172.

Why other options are incorrect:

Option A: While it contains Level 1 practices, it also includes Level 2 practices.

Option B: Level 3 is the 'Expert' level, which is separate and higher than the 'Advanced' level.

Option D: The Advanced level does not reach the requirements of Level 3.

Reference Documents:

CMMC Model Overview (v2.0): Section 3.2, 'Level 2: Advanced,' which describes the 110 practices derived from NIST SP 800-171.

32 CFR Part 170 (CMMC Program Rule): Details the structure of the levels and the requirement for cumulative compliance.

CMMC Level 2 Assessment Guide: Lists all 22 Access Control practices required for a Level 2 assessment, clearly identifying which are carried over from Level 1.

=====

Question 10

Question Type: MultipleChoice

On a Level 2 Assessment Team, what are the roles of the CCP and the CCA?

Options:

- A- The CCP leads the Level 2 Assessment Team, which consists of one or more CCAs.
- B- The CCA leads the Level 2 Assessment Team, which can include 3 CCP with US Citizenship.
- C- The CCA leads the Level 2 Assessment Team, which can include a CCP regardless of citizenship.
- D- The CCP leads the Level 2 Assessment Team, which can include a CCA. regardless of citizenship.

Answer:

C

Explanation:

Step 1: Define Roles -- CCP and CCA

CCP (Certified CMMC Professional):

Entry-level certification in the CMMC ecosystem.

Supports assessment activities under the supervision of a CCA.

May assist in consulting roles outside of formal assessments.

CCA (Certified CMMC Assessor):

Certified to lead assessments under the CMMC model.

Required for conducting Level 2 formal assessments.

Can be part of a C3PAO assessment team or lead it.

Source: CMMC Assessment Process (CAP) v1.0, Section 2.3 -- Assessment Team Composition

"Level 2 assessments must be led by a Certified CMMC Assessor (CCA), who may be supported by one or more CCPs."

Step 2: Citizenship Requirements

CAP v1.0 -- Appendix B: Team Composition and Clearance Requirements

"All team members performing Level 2 assessments must be U.S. citizens when handling CUI, regardless of role."

But for supporting team members who do not handle CUI or in FCI-only scoping, there is no automatic exclusion based on citizenship.

So:

The CCA leads the team.

CCPs can be team members regardless of citizenship, unless restricted by contract or CUI handling needs.

Why the Other Options Are Incorrect

A . The CCP leads the Level 2 Assessment Team...

Incorrect. CCPs cannot lead Level 2 assessments.

B . The CCA leads... includes 3 CCP with US Citizenship.

Incorrect. Citizenship is required only when handling CUI, not a universal requirement.

D . The CCP leads...

Again, CCPs do not have the authority to lead formal CMMC assessments.

Only a Certified CMMC Assessor (CCA) may lead a Level 2 Assessment Team, and they may include CCPs, even non-U.S. citizens, if citizenship is not a requirement based on contractual or data sensitivity scope.

Question 11

Question Type: MultipleChoice

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?

Options:

A- C3PAO

B- CMMC-AB

C- Assessment Team

D- Assessment Sponsor

Answer:

A

Explanation:

Who Has the Final Authority Over Assessment Results?

During a CMMC Level 2 assessment, the Certified Third-Party Assessment Organization (C3PAO) is responsible for conducting and finalizing the assessment results.

Key Responsibilities of a C3PAO

Leads the assessment and ensures it follows the CMMC Assessment Process (CAP).

Validates compliance with CMMC Level 2 requirements based on NIST SP 800-171 controls.

Finalizes the assessment results and submits them to the CMMC-AB and the DoD.

Handles disagreements from the OSC but has final decision-making authority on results.

Why 'C3PAO' is Correct?

The C3PAO has final authority over the assessment results after considering all evidence and findings.

The CMMC-AB (Option B) does not finalize assessments---it accredits C3PAOs and manages the certification ecosystem.

The Assessment Team (Option C) supports the C3PAO but does not have final decision authority.

The Assessment Sponsor (Option D) is a representative from the OSC and does not control the results.

Breakdown of Answer Choices

Option

Description

Correct?

A . C3PAO

Correct -- C3PAOs finalize and submit assessment results.

B . CMMC-AB

Incorrect--The CMMC-AB accredits C3PAOs but does not finalize results.

C . Assessment Team

Incorrect--They conduct the assessment, but the C3PAO makes final decisions.

D . Assessment Sponsor

Incorrect--This is a representative of the OSC, not the assessment authority.

Official Reference from CMMC 2.0 Documentation

CMMC Assessment Process Guide (CAP)-- Defines C3PAO authority over final assessment results.

Final Verification and Conclusion

The correct answer is A. C3PAO, as the C3PAO has final decision-making authority over CMMC assessment results.

Question 12

Question Type: Multiple Choice

An OSC has requested a C3PAO to conduct a Level 2 Assessment. The C3PAO has agreed, and the two organizations have collaborated to develop the Assessment Plan. Who agrees to and signs off on the Assessment Plan?

Options:

- A- OSC and Sponsor
- B- OSC and CMMC-AB
- C- Lead Assessor and C3PAO
- D- C3PAO and Assessment Official

Answer:

C

Explanation:

Understanding the CMMC Level 2 Assessment Process

When an Organization Seeking Certification (OSC) engages a Certified Third-Party Assessment Organization (C3PAO) to conduct a CMMC Level 2 Assessment, an Assessment Plan is developed to outline the scope, methodology, and logistics of the assessment.

Who Signs Off on the Assessment Plan?

According to the CMMC Assessment Process (CAP) Guide, the Assessment Plan must be formally agreed upon and signed off by:

Lead Assessor-- The individual responsible for overseeing the execution of the assessment.

C3PAO (Certified Third-Party Assessment Organization)-- The entity conducting the assessment.

Why 'C. Lead Assessor and C3PAO' is Correct?

The Lead Assessor ensures that the Assessment Plan aligns with CMMC-AB and DoD requirements, including methodology, objectives, and evidence collection.

The C3PAO provides organizational approval, confirming that the assessment is conducted according to CMMC-AB rules and contractual agreements.

Why Other Answers Are Incorrect?

A . OSC and Sponsor (Incorrect)

The OSC (Organization Seeking Certification) is involved in planning but does not sign off on the plan.

A sponsor is not part of the sign-off process in CMMC assessments.

B . OSC and CMMC-AB (Incorrect)

The OSC does not formally approve the Assessment Plan---this responsibility belongs to the assessment team.

The CMMC-AB does not sign off on individual Assessment Plans.

D . C3PAO and Assessment Official (Incorrect)

'Assessment Official' is not a defined role in the CMMC assessment process.

The C3PAO is involved, but it must be the Lead Assessor who signs off, not an unspecified official.

Conclusion

The correct answer is C. Lead Assessor and C3PAO.

The Lead Assessor ensures assessment integrity, while the C3PAO provides official authorization.

CMMC Assessment Process (CAP) Guide

CMMC 2.0 Level 2 Certification Procedures

The Cyber AB Assessment Guidelines

Question 13

Question Type: MultipleChoice

What are CUI protection responsibilities?

Options:

- A- Shielding
- B- Governing
- C- Correcting
- D- Safeguarding

Answer:

D

Explanation:

Understanding CUI Protection Responsibilities

Controlled Unclassified Information (CUI) is sensitive but not classified information that requires protection under DoD Instruction 5200.48 and DFARS 252.204-7012.

The primary responsibility for handling CUI is safeguarding it against unauthorized access, disclosure, or modification.

Why 'D. Safeguarding' is Correct?

The CUI Program (as per NARA and DoD) mandates safeguarding measures to protect CUI in both digital and physical forms.

CMMC 2.0 Level 2 (Advanced) practices align with NIST SP 800-171, which focuses on safeguarding CUI through access controls, encryption, and monitoring.

DFARS 252.204-7012 requires DoD contractors to implement cybersecurity safeguards to protect CUI.

Why Other Answers Are Incorrect?

A . Shielding (Incorrect)--Shielding is not a cybersecurity term associated with CUI protection.

B . Governing (Incorrect)--Governing refers to policy-making, not direct protection.

C . Correcting (Incorrect)--Correcting implies remediation, but the primary responsibility is to safeguard CUI proactively.

Conclusion

The correct answer is D. Safeguarding, as CUI protection focuses on implementing cybersecurity safeguards.

DoD Instruction 5200.48 (CUI Program)

DFARS 252.204-7012

CMMC 2.0 Level 2 Practices (NIST SP 800-171)



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