Exams4sure
Leaders in IT certification

Cyber AB

CMMC-CCP

Certified CMMC Professional (CCP) Exam

Version: 8.1

[Total Questions: 206]

Web: www.exams4sure.com

Email: support@exams4sure.com

IMPORTANT NOTICE

Feedback

We have developed quality product and state-of-art service to ensure our customers interest. If you have any suggestions, please feel free to contact us at feedback@exams4sure.com

Support

If you have any questions about our product, please provide the following items:

- exam code
- screenshot of the question
- login id/email

please contact us at support@exams4sure.com and our technical experts will provide support within 24 hours.

Copyright

Category Breakdown

Category	**Number of Questions**
CMMC Assessment Process (CAP)	49
CMMC Ecosystem	60
Implementation and Scoping	12
Roles and Responsibilities	8
CMMC Model Overview	63
Governance and Source Documents	14
TOTAL	206

Question #:1 - [CMMC Assessment Process (CAP)]

Which method facilitates understanding by analyzing gathered artifacts as evidence?

A. Test

B. Examine

C. Behavior

D. Interview

Answer: B

Explanation

The CMMC Assessment Process uses three methods: Examine, Interview, and Test. The method that involves analyzing artifacts (documents, system configurations, records, logs, etc.) is Examine.

Supporting Extracts from Official Content:

- CMMC Assessment Guide: “Examine consists of reviewing, inspecting, or analyzing assessment objects such as documents, system configurations, or other artifacts to evaluate compliance.”

Why Option B is Correct:

- Examine = analyzing artifacts.
- Interview = discussions with personnel.
- Test = executing technical checks.
- Behavior is not an assessment method.

References (Official CMMC v2.0 Content):

- CMMC Assessment Guide, Levels 1 and 2 — Assessment Methods (Examine, Interview, Test).

===========

Question #:2 - [CMMC Ecosystem]

SC.L2-3 13.14: Control and monitor the use of VoIP technologies is marked as NOT APPLICABLE for an OSC's assessment. How does this affect the assessment scope?

A. Any existing telephone system is in scope even if it is not using VoIP technology.

B. An error has been made and the Lead Assessor should be contacted to correct the error.

C. VoIP technology is within scope, and it uses FlPS-validated encryption, so it does not need to be assessed.

D. VoIP technology is not used within scope boundary, so no assessment procedures are specified for this practice.

Answer: D

Explanation

TheCMMC 2.0 Level 2requirementSC.L2-3.13.14comes fromNIST SP 800-171, Security Requirement 3.13.14, which mandates that organizations mustcontrol and monitor the use of VoIP (Voice over Internet Protocol) technologiesif used within their system boundary.

If a systemdoes not use VoIP technology, then this control isNot Applicable (N/A)because there is nothing to assess.

When a requirement is marked as Not Applicable (N/A), it means the OSC does not use the technology or process covered by that controlwithin its assessment boundary.

No assessment procedures are neededsince there is no VoIP system to evaluate.

Option A (Existing telephone system in scope)is incorrect becausetraditional (non-VoIP) telephone systems are not covered by SC.L2-3.13.14—only VoIP is within scope.

Option B (Error, contact the Lead Assessor)is incorrect because markingSC.L2-3.13.14 as N/A is valid if VoIP is not used. This is not an error.

Option C (VoIP in scope but using FIPS-validated encryption, so it doesn’t need to be assessed)is incorrect becauseeven if VoIP uses FIPS-validated encryption, the control would still need to be assessed to ensure monitoring and usage control are in place.

CMMC 2.0 Level 2 Assessment Guide – SC.L2-3.13.14

NIST SP 800-171, Security Requirement 3.13.14

CMMC Scoping Guidance – Determining Not Applicable (N/A) Practices

Understanding SC.L2-3.13.14 – Control and Monitor the Use of VoIP TechnologiesWhy Option D is CorrectOfficial CMMC Documentation ReferencesFinal VerificationIfVoIP is not used within the OSC's system boundary, the control does not require assessment, making Option D the correct answer.

Question #:3 - [Implementation and Scoping]

For the purpose of determining scope, what needs to be included as part of the assessment but would NOT receive a CMMC certification unless an enterprise assessment is conducted?

A. ESP

B. People

C. Test equipment

D. Government property

Answer: A

Explanation

Per the CMMC Scoping Guidance, External Service Providers (ESPs) must be included in scope if they process, store, or transmit CUI or FCI on behalf of the OSC. However, ESPs do not themselves receive a separate CMMC certification unless they undergo their own assessment or an enterprise-level certification is conducted. Their environment is assessed only as part of the OSC's scope.

Reference Documents:

- CMMC Scoping Guidance for Level 2
- CMMC Model v2.0 Overview

Question #:4 - [CMMC Assessment Process (CAP)]

What is the MOST common purpose of assessment procedures?

A. Obtain evidence.

B. Define level of effort.

C. Determine information flow.

D. Determine value of hardware and software.

Answer: A

Explanation

Theprimary goal of CMMC assessment proceduresis to determine whether anOrganization Seeking Certification (OSC)complies with the cybersecurity controls required for its certification level. Themost common purpose of assessment procedures is to obtain evidencethat verifies an organization has properly implemented security practices.

CMMC Assessments Require Evidence Collection

TheCMMC Assessment Process (CAP) Guideoutlines that assessors must use three methods to verify compliance:

Examine– Reviewing documentation, policies, and system configurations.

Interview– Speaking with personnel to confirm understanding and execution.

Test– Validating controls through operational or technical tests.

All these methods involve obtaining evidenceto support whether a security requirement has been met.

Alignment with NIST SP 800-171A

CMMC Level 2 assessments follow NIST SP 800-171A, which is designed for evidence-based verification.

Assessors rely on documented artifacts, system logs, configurations, and personnel testimony as evidence of compliance.

B. Define level of effort (Incorrect)

Thelevel of effortrefers to the time and resources needed for an assessment, but this is aplanningactivity, not the primary goal of an assessment.

C. Determine information flow (Incorrect)

While understandinginformation flowis important for security controls likedata protection and access control, themain purpose of an assessment is to gather evidence—not to determine information flow itself.

D. Determine value of hardware and software (Incorrect)

Asset valuation may be part of an organization’s risk management process, but CMMC assessmentsdo not focus on determining hardware or software value.

The correct answer isA. Obtain evidence, as theCMMC assessment process is evidence-drivento verify compliance with security controls.

References:

CMMC Assessment Process (CAP) Guide

NIST SP 800-171A (Assessment Procedures for CUI)

DoD CMMC 2.0 Scoping and Assessment Guidelines

Question #:5 - [CMMC Ecosystem]

When assessing SI.L1-3.14.2: Provide protection from malicious code at appropriate locations within organizational information systems, evidence shows that all of the OSC's workstations and servers have antivirus software installed for malicious code protection. A centralized console for the antivirus software management is in place and records show that all devices have received the most updated antivirus patterns. What is the BEST determination that the Lead Assessor should reach regarding the evidence?

A. It is sufficient, and the audit finding can be rated as MET.

B. It is insufficient, and the audit finding can be rated NOT MET.

C. It is sufficient, and the Lead Assessor should seek more evidence.

D. It is insufficient, and the Lead Assessor should seek more evidence.

Answer: A

Explanation

Understanding SI.L1-3.14.2: Provide Protection from Malicious CodeThe CMMC Level 1 practiceSI.L1-3.14.2is based onNIST SP 800-171 Requirement 3.14.2, which requires organizations to:

Implement malicious code protection(e.g., antivirus, endpoint security software).

Ensure coverage across all appropriate locations(e.g., workstations, servers, network entry points).

Keep protection mechanisms updated(e.g., regular signature updates, policy enforcement).

Assessment Criteria for a "MET" Rating:To determine whether the practice isMET, the Lead Assessor must confirm that:

#Antivirus or endpoint protection software is installedon all workstations and servers.

#The solution is centrally managed, ensuring consistent policy enforcement.

#Signature updates are current, meaning systems are protected against new threats.

#Logs or reports demonstrate active monitoring and updates.

Why is the Correct Answer "A. It is sufficient, and the audit finding can be rated as MET"?The provided evidenceconfirms all necessary requirementsfor SI.L1-3.14.2:

#All workstations and servers have antivirus installed#Meets installation requirement.

#A centralized management console is in place#Ensures consistent enforcement.

#Records show antivirus signatures are up to date#Confirms system protection is current.

Because the evidencemeets the requirement, the practice should berated as MET.

B. It is insufficient, and the audit finding can be rated NOT MET # Incorrect

The evidence providedmeets all necessary requirements, so the practiceshould not be rated as NOT MET.

C. It is sufficient, and the Lead Assessor should seek more evidence # Incorrect

Ifadequate evidence already exists,additional evidence is unnecessary.

D. It is insufficient, and the Lead Assessor should seek more evidence # Incorrect

The evidence providedmeets the control requirements, making itsufficient.

Why Are the Other Answers Incorrect?

CMMC Assessment Process (CAP) Document

Specifies that a practice can be marked asMET if sufficient evidence is provided.

NIST SP 800-171 (Requirement 3.14.2)

Defines the standard formalicious code protection, which ismet by antivirus with active updates.

CMMC 2.0 Level 1 (Foundational) Requirements

Clarifies that basic cybersecurity measures likeantivirus installation and updatesmeet compliance forSI.L1-3.14.2.

CMMC 2.0 References Supporting This Answer:

Final Answer:#A. It is sufficient, and the audit finding can be rated as MET.

Question #:6 - [Implementation and Scoping]

An OSC performing a CMMC Level 1 Self-Assessment uses a legacy Windows 95 computer, which is the only system that can run software that the government contract requires. Why can this asset be considered out of scope?

A. It handles CUI

B. It is a restricted IS

C. It is government property

D. It is operational technology

Answer: B

Explanation

A Restricted Information System (IS) is defined as an asset that cannot meet modern security controls but is still needed for contract performance. These systems may be declared out of scope if they are properly isolated, mitigated, and documented. A legacy Windows 95 computer meets the definition of a restricted IS.

Supporting Extracts from Official Content:

- CMMC Scoping Guide (Level 2): “Restricted IS assets are those that cannot reasonably apply security requirements due to legacy or operational constraints. They are not assessed but must be identified and protected by alternative methods.”

Why Option B is Correct:

- The Windows 95 system is an example of a restricted IS, so it can be scoped out.
- Option A is incorrect — the asset is not handling CUI in this case.
- Option C is incorrect — government property designation does not define scope.
- Option D is incorrect — while it is “legacy,” it is not classified as OT; the correct CMMC term is restricted IS.

References (Official CMMC v2.0 Content):

- CMMC Scoping Guide, Level 1 and Level 2 – Restricted IS definition.

===========

Question #:7 - [Roles and Responsibilities]

When executing a remediation review, the Lead Assessor should:

A. help OSC to complete planned remediation activities.

B. plan two consecutive remediation reviews for an OSC.

C. submit a delta assessment remediation package for C3PAO's internal quality review.

D. validate that practices previously listed on the POA&M have been removed on an updated Risk Assessment.

Answer: C

Explanation

In the context of the Cybersecurity Maturity Model Certification (CMMC) 2.0, the remediation review process is a critical phase where identified deficiencies from an initial assessment are addressed. The Lead Assessor, representing a Certified Third-Party Assessment Organization (C3PAO), plays a pivotal role in this process.

Role of the Lead Assessor in Remediation Reviews:

Validation of Remediation Efforts:

Objective:Ensure that the Organization Seeking Certification (OSC) has effectively addressed and corrected all deficiencies identified during the initial assessment.

Process:The Lead Assessor reviews the evidence provided by the OSC to confirm that each previously unmet practice now meets the required standards. This involves examining updated policies, procedures, system configurations, and other relevant artifacts.

Delta Assessment Remediation Package Submission:

Definition:A delta assessment focuses on evaluating only the components or practices that were previously found non-compliant or deficient.

Responsibility:After validating the remediation efforts, the Lead Assessor compiles a remediation package that includes:

Detailed documentation of the deficiencies identified in the initial assessment.

Evidence of the corrective actions taken by the OSC.

Findings from the reassessment of the remediated practices.

Internal Quality Review:This remediation package is then submitted for the C3PAO's internal quality review process. The purpose of this review is to ensure the accuracy, completeness, and consistency of the assessment findings before finalizing the certification decision.

Rationale for Selecting Answer C:

Alignment with CMMC Assessment Process:The submission of a delta assessment remediation package for internal quality review is a standard procedure outlined in the CMMC Assessment Process. This step ensures that all remediated items are thoroughly evaluated and validated, maintaining the integrity of the certification process.

Clarification of Incorrect Options:

Option A:"Help OSC to complete planned remediation activities."

The Lead Assessor's role is to assess and validate the OSC's compliance, not to assist in the implementation or completion of remediation activities. Providing such assistance could lead to a conflict of interest and compromise the objectivity of the assessment.

Option B:"Plan two consecutive remediation reviews for an OSC."

The standard process involves conducting a single remediation review after the OSC has addressed the identified deficiencies. Planning multiple consecutive remediation reviews is not a typical practice and could indicate a lack of proper remediation planning by the OSC.

Option D:"Validate that practices previously listed on the POA&M have been removed on an updated Risk Assessment."

While it's essential to ensure that deficiencies are addressed, the primary focus of the Lead Assessor during a remediation review is to validate the implementation of remediated practices. Updating the Risk Assessment is the responsibility of the OSC's internal risk management team, not the Lead Assessor.

References:

CMMC Assessment Process v2.0

CyberAB

CMMC Assessment Guide – Level 2

Defense Innovation Unit

These documents provide detailed guidelines on the roles and responsibilities of assessors, the remediation review process, and the procedures for submitting assessment findings for quality review within the CMMC framework.

Question #:8 - [CMMC Model Overview]

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

A. DoD

B. NARA

C. NIST

D. Department of Homeland Security

Answer: A

Explanation

TheU.S. Department of Defense (DoD)determines the requiredCMMC Levelbased on thesensitivity of the information involved in a contract.

The required CMMC Level isspecified in Requests for Information (RFIs) and Requests for Proposals (RFPs).

Reference:

DFARS 252.204-7021 (CMMC Requirements)

CMMC 2.0 Program Documentation

Step 2: Why Other Answer Choices Are IncorrectB. NARA (Incorrect):

TheNational Archives and Records Administration (NARA)overseesCUI program policiesbut does not assign CMMC levels.

C. NIST (Incorrect):

TheNational 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):

TheDepartment of Homeland Security (DHS)is responsible for cybersecurity at the national level, butCMMC applies specifically to DoD contractors.

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

Question #:9 - [Governance and Source Documents]

Which NIST SP discusses protecting CUI in nonfederal systems and organizations?

A. NIST SP 800-37

B. NIST SP 800-53

C. NIST SP 800-88

D. NIST SP 800-171

Answer: D

Explanation

Understanding the Role of NIST SP 800-171 in CMMCNIST Special Publication (SP)800-171is the definitive standard for protectingControlled Unclassified Information (CUI)innonfederal systems and organizations. It provides security requirements that organizations handling CUImust implementto protect sensitive government information.

This document isthe foundationofCMMC 2.0 Level 2compliance, which aligns directly withNIST SP 800-171 Rev. 2requirements.

Breakdown of Answer ChoicesNIST SP

Title

Relevance to CMMC

NIST SP 800-37

Risk Management Framework (RMF)

Focuses on risk assessment for federal agencies, not directly applicable to CUI in nonfederal systems.

NIST SP 800-53

Security and Privacy Controls for Federal Systems

Provides security controls forfederalinformation systems, not specifically tailored tononfederalorganizations handling CUI.

NIST SP 800-88

Guidelines for Media Sanitization

Covers secure data destruction and disposal, not overall CUI protection.

NIST SP 800-171

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

#Correct Answer – Directly addresses CUI protection in contractor systems.

Key Requirements from NIST SP 800-171The document outlines110 security controlsgrouped into14 families, including:

Access Control (AC)– Restrict access to authorized users.

Audit and Accountability (AU)– Maintain system logs and monitor activity.

Incident Response (IR)– Establish an incident response plan.

System and Communications Protection (SC)– Encrypt CUI in transit and at rest.

These controls serve as thebaseline requirementsfor organizations seekingCMMC Level 2 certificationto work withCUI.

CMMC 2.0 Level 2alignsdirectlywith NIST SP800-171 Rev. 2.

DoD contractors that handle CUImustcomply withall 110 controlsfrom NIST SP800-171.

Official Reference from CMMC 2.0 DocumentationFinal Verification and ConclusionThe correct answer isD. NIST SP 800-171, as this documentexplicitly definesthe cybersecurity requirements for protectingCUI in nonfederal systems and organizations.

Question #:10 - [CMMC Ecosystem]

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?

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: C

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.

Question #:11 - [CMMC Model Overview]

Where does the requirement to include a required practice of ensuring that personnel are trained to carry out their assigned information security-related duties and responsibilities FIRST appear?

A. Level 1

B. Level 2

C. Level 3

D. All levels

Answer: B

Explanation

Understanding Training Requirements in CMMCThe requirement for ensuring thatpersonnel are trained to carry out their assigned information security-related duties and responsibilitiesfirst appears inCMMC Level 2as part ofNIST SP 800-171 control AT.L2-3.2.1.

Key Details on the Training Requirement:#AT.L2-3.2.1: "Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities."

#This control is derived fromNIST SP 800-171and applies toCMMC Level 2 (Advanced).

#It ensures that employees handlingControlled Unclassified Information (CUI)understand theircybersecurity responsibilities.

A. Level 1 # Incorrect

CMMC Level 1 does not include this training requirement.Level 1 focuses on basic safeguarding ofFederal Contract Information (FCI)but doesnot require formal cybersecurity training.

B. Level 2 # Correct

The training requirement (AT.L2-3.2.1) first appears in CMMC Level 2, which aligns withNIST SP 800-171.

C. Level 3 # Incorrect

The training requirementalready exists in Level 2. Level 3 builds on Level 2 with additionalrisk management and advanced cybersecurity controls, but training is introduced at Level 2.

D. All levels # Incorrect

CMMC Level 1 does not include this requirement—it is first introduced in Level 2.

Why is the Correct Answer "B. Level 2"?

NIST SP 800-171 (Requirement 3.2.1)

Defines themandatory training requirementfor personnel handling CUI.

CMMC Assessment Guide for Level 2

ListsAT.L2-3.2.1as a required practice under Level 2.

CMMC 2.0 Model Overview

Confirms thatCMMC Level 2 aligns with NIST SP 800-171, which includes security training requirements.

CMMC 2.0 References Supporting This Answer:

Question #:12 - [CMMC Assessment Process (CAP)]

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

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

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 tolead assessmentsunder the CMMC model.

Requiredfor conductingLevel 2 formal assessments.

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

Step 1: Define Roles – CCP and CCASource: 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 RequirementsCAP 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 forsupporting team members who do not handle CUIor inFCI-only scoping, there is no automatic exclusion based on citizenship.

So:

TheCCA leadsthe team.

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

A. The CCP leads the Level 2 Assessment Team…# Incorrect. CCPscannot leadLevel 2 assessments.

B. The CCA leads… includes 3 CCP with US Citizenship.# Incorrect. Citizenship is requiredonly when handling CUI, not a universal requirement.

D. The CCP leads…# Again, CCPs donot have the authority to leadformal CMMC assessments.

#Why the Other Options Are Incorrect

Only aCertified CMMC Assessor (CCA)may lead aLevel 2 Assessment Team, and theymay include CCPs, evennon-U.S. citizens, if citizenship is not a requirement based on contractual or data sensitivity scope.

Question #:13 - [CMMC Ecosystem]

During an assessment, the Lead Assessor reviews the evidence for each CMMC in-scope practice that has been reviewed, verified, rated, and discussed with the OSC during the daily reviews. The Assessment Team records the final recommended MET or NOT MET rating and prepares to present the results to the assessment participants during the final review with the OSC and sponsor. As a part of this presentation, which document MUST include the attendee list, time/date, location/meeting link, results from all discussed topics, including any resulting actions, and due dates from the OSC or Assessment Team?

A. Final log report

B. Final CMMC report

C. Final and recorded OSC CMMC report

D. Final and recorded Daily Checkpoint log

Answer: D

Explanation

Understanding the Final Review Process in a CMMC AssessmentDuring aCMMC Level 2 Assessment, theAssessment Teamand theOrganization Seeking Certification (OSC)holddaily checkpoint meetingsto discuss progress, review evidence, and ensure transparency.

At theend of the assessment, afinal review meetingis conducted, during which theLead Assessor presents the results. Therecorded Daily Checkpoint logserves as theofficial document summarizing:

Theattendee list

Time, date, and locationof the final review

Final MET or NOT MET ratingsfor all practices

Discussion points, resulting actions, and due datesfor both the OSC and Assessment Team

TheCMMC Assessment Process (CAP) Guidespecifies that all assessment findings and discussions must bedocumented throughout the assessment in daily checkpoint logs.

TheFinal and Recorded Daily Checkpoint Logincludes all necessary details, such as attendee lists, discussion topics, and action items.

This document isused to ensure all discussed topics and agreed-upon actions are properly tracked and recordedbefore submission.

A. Final log report (Incorrect)

There isno specific "Final Log Report"required in CMMC assessments.

B. Final CMMC report (Incorrect)

TheFinal CMMC Reportdocuments the overall assessment results butdoes not serve as the official meeting logfor the final review discussion.

C. Final and recorded OSC CMMC report (Incorrect)

This documentdoes not include detailed discussion points from the daily checkpoint meetings.

The correct answer isD. Final and recorded Daily Checkpoint log, as this is the official document that captures thefinal meeting details, discussions, and action items.

References:

CMMC Assessment Process (CAP) Guide

CMMC 2.0 Scoping and Assessment Guidelines

Question #:14 - [CMMC Assessment Process (CAP)]

Recording evidence as adequate is defined as the criteria needed to:

A. verify, based on an assessment and organizational scope.

B. verify, based on an assessment and organizational practice.

C. determine if a given artifact, interview response, demonstration, or test meets the CMMC scope.

D. determine if a given artifact, interview response, demonstration, or test meets the CMMC practice.

Answer: D

Explanation

Understanding "Adequate Evidence" in the CMMC Assessment ProcessIn aCMMC assessment,adequate evidencerefers to the proof required to demonstrate that a specific cybersecurity practice has been implemented correctly. Evidence can come from:

Artifacts(e.g., security policies, system configurations, logs).

Interview responses(e.g., verbal confirmation from personnel about their responsibilities).

Demonstrations(e.g., showing how a security control is implemented in real time).

Testing(e.g., verifying technical security mechanisms such as multi-factor authentication).

Thegoalof evidence collection is to determinewhether a CMMC practice is met—not just whether the organization operates within the assessment scope.

A. Verify, based on an assessment and organizational scope # Incorrect

Theassessment scopedefineswhat is evaluated, but adequacy of evidence is based oncompliance with specific CMMC practices.

B. Verify, based on an assessment and organizational practice # Incorrect

CMMC assessments focus on cybersecurity practices defined in the CMMC framework, not just general organizational practices.

C. Determine if a given artifact, interview response, demonstration, or test meets the CMMC scope # Incorrect

Thescopedefines the assessment boundaries, but theassessment team's job is to confirm whether CMMC practices are satisfied.

D. Determine if a given artifact, interview response, demonstration, or test meets the CMMC practice # Correct

TheCMMC assessment process focuses on ensuring that required practices are implemented, making this the correct answer.

Why is the Correct Answer "Determine if a given artifact, interview response, demonstration, or test meets the CMMC practice" (D)?

CMMC Assessment Process (CAP) Document

Defines "adequate evidence" asproof that a CMMC practice has been correctly implemented.

CMMC 2.0 Assessment Criteria

Specifies that evidence must beevaluated against specific cybersecurity practices.

NIST SP 800-171A (Assessment Procedures for NIST SP 800-171)

Provides guidance on evaluating artifacts, interviews, demonstrations, and testing to confirm compliance with required practices.

CMMC 2.0 References Supporting this Answer:

Final Answer:#D. Determine if a given artifact, interview response, demonstration, or test meets the CMMC practice.

Question #:15 - [Implementation and Scoping]

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:

A. protect CUI.

B. transmit CUI.

C. store CUI.

D. generate CUI

Answer: C

Question #:16 - [CMMC Model Overview]

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?

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 CMMCMulti-function devices (MFDs), such asscanners, printers, and copiers,process, store, and transmit FCI, making them apotential attack surfacefor unauthorized access.

Thebest technical controlto limit MFD access to only authorized systems isVirtual LAN (VLAN) restrictions, whichsegment and isolate network traffic.

VLAN Restrictions Provide Network Segmentation

VLANsisolate the MFDfrom unauthorized systems, ensuringonly approved devicescan communicate with it.

Prevents unauthorized network access bylimiting connectionsto specific IPs or subnets.

Meets CMMC 2.0 Network Security Controls

Aligns withCMMC System and Communications Protection (SC) Practicesfor network segmentation and access control.

Reducesthe risk of unauthorized access to scanned and printed FCI.

B. Single administrative account#Incorrect

Asingle admin accountdoes not restrict accessbetween devices, only controlswho can configurethe MFD.

C. Documentation showing MFD configuration#Incorrect

Documentation helps with compliance butdoes not actively restrict access.

D. Access lists only known to the IT administrator#Incorrect

Access lists should besystem-enforced, not just "known" to the administrator.

CMMC Practice SC.3.192 (Network Segmentation)– Requires restricting access usingnetwork segmentation techniques such as VLANs.

NIST SP 800-171 (SC Family)– Supportsisolation of sensitive devicesusing VLANs and other segmentation controls.

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

Question #:17 - [CMMC Ecosystem]

During a Level 2 Assessment, an OSC provides documentation that attests that they utilize multifactor authentication on nonlocal remote maintenance sessions. The OSC feels that they have met the controls for the Level 2 certification. What additional measures should the OSC perform to fully meet the maintenance requirement?

A. Connections for nonlocal maintenance sessions should be terminated when maintenance is complete.

B. Connections for nonlocal maintenance sessions should be unlimited to ensure maintenance is performed properly

C. The nonlocal maintenance personnel complain that restrictions slow down their response time and should be removed.

D. The maintenance policy states multifactor authentication must have at least two factors applied for nonlocal maintenance sessions.

Answer: A

Explanation

UnderCMMC 2.0 Level 2, which aligns with the requirements ofNIST SP 800-171, maintaining robust control overnonlocal maintenance sessionsis critical. While multifactor authentication (MFA) is a required safeguard for secure access, additional measures must be implemented to fully meet the maintenance requirements as outlined inControl 3.3.5:

Key Requirements for Nonlocal Maintenance:

Termination of Nonlocal Maintenance Sessions:

To reduce the attack surface and prevent unauthorized access, nonlocal maintenance connectionsmust be terminated immediately after the maintenance activity is completed. This is a direct requirement to mitigate risks associated with lingering remote sessions that could be exploited by threat actors.

Supporting Reference:NIST SP 800-171, Control 3.3.5 states: "Ensure that remote maintenance is conducted in a controlled manner and disable connections immediately after use."

Multifactor Authentication (MFA):

OSCs are required to implement MFA for nonlocal remote maintenance sessions. MFA must includeat least two factors(e.g., something you know, something you have, or something you are).

While the OSC’s use of MFA satisfies part of the requirement, it does not complete the control unless proper termination procedures are in place.

Policy and Procedure Adherence:

The OSC must also document amaintenance policyand ensure it reflects the need for terminating connections post-maintenance. The policy should outline roles, responsibilities, and steps for ensuring secure nonlocal maintenance practices.

Incorrect Options:

B. Unlimited connections:Allowing unrestricted nonlocal maintenance sessions is a significant security risk and violates the principle of least privilege.

C. Removing restrictions:Removing restrictions for convenience directly undermines compliance and security.

D. Multifactor authentication details:While MFA is necessary, the question states the OSC already uses it. Termination of sessions is the missing requirement.

Conclusion:

The requirement toterminate nonlocal maintenance sessions after maintenance is complete(Option A) is critical for compliance withCMMC 2.0 Level 2andNIST SP 800-171, Control 3.3.5. This ensures that nonlocal maintenance activities are secured against unauthorized access and potential vulnerabilities.

Question #:18 - [CMMC Ecosystem]

A contractor provides services and data to the DoD. The transactions that occur to handle FCI take place over the contractor's business network, but the work is performed on contractor-owned systems, which must be configured based on government requirements and are used to support a contract. What type of Specialized Asset are these systems?

A. loT

B. Restricted IS

C. Test equipment

D. Government property

Answer: B

Explanation

Understanding Restricted Information Systems (IS) in CMMC ScopingInCMMC 2.0,Specialized Assetsrefer to assets that do not fit traditional IT system categories but still play a role inprocessing, storing, or transmitting Federal Contract Information (FCI) or Controlled Unclassified Information (CUI). The four categories ofSpecialized Assetsin theCMMC Scoping Guideinclude:

Internet of Things (IoT) Devices– Smart or network-connected devices.

Restricted Information Systems (Restricted IS)– Systems that arecontractually requiredto beconfigured to government specifications.

Test Equipment– Devices used for specialized testing or measurement.

Government Property– Equipment owned by theU.S. Governmentbut used by contractors.

The contractor-owned systems in question areconfigured based on government requirementsandused to support a DoD contract.

Restricted ISassets arecontractually requiredto meet government security requirements andhandle DoD-related information.

These systemsdo not fall under general IT assets but instead require special handling, making them a Restricted ISper theCMMC Scoping Guide.

A. IoT (Incorrect)

IoT devices includesmart devices, sensors, and embedded systems, but the contractor's business systems are not classified as IoT.

C. Test Equipment (Incorrect)

The contractor’s systems areused for handling FCI, not for testing or measurement.

D. Government Property (Incorrect)

The systems arecontractor-owned, not owned by theU.S. Government, so they do not qualify asGovernment Property.

The correct answer isB. Restricted IS, as the systems arecontractor-owned but must follow DoD security requirements.

References:

CMMC 2.0 Scoping Guide for Level 2

DoD CMMC Policy and DFARS 252.204-7012

Question #:19 - [Governance and Source Documents]

According to DFARS clause 252.204-7012, who is responsible for determining that Information in a given category should be considered CUI?

A. The NARA CUI Executive Agent

B. The contractor who generated the information

C. The DoD agency for whom the contractor is performing the work

D. The military personnel assigned to the contractor for that purpose

Answer: C

Explanation

DFARS clause 252.204-7012 establishes the safeguarding of Covered Defense Information (CDI), which aligns with CUI categories. The clause specifies that the DoD is responsible for determining whether information is Controlled Unclassified Information (CUI) and marking it accordingly before sharing it with contractors. Contractors do not make determinations about what constitutes CUI; they are responsible for safeguarding information once it is received and marked as CUI.

Reference Documents:

- DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting
- CMMC Model v2.0 Overview, December 2021

Question #:20 - [CMMC Model Overview]

Which document is the BEST source for descriptions of each practice or process contained within the various CMMC domains?

A. CMMC Glossary

B. CMMC Appendices

C. CMMC Assessment Process

D. CMMC Assessment Guide Levels 1 and 2

Answer: D

Explanation

Understanding the Best Source for CMMC Practice DescriptionsTheCMMC Assessment Guide (Levels 1 and 2)is theprimaryandmost authoritativedocument for detailed descriptions of each practice and process within the variousCMMC domains.

Step-by-Step Breakdown:#1. What is the CMMC Assessment Guide?

TheCMMC Assessment Guideprovides detailed explanations of:

EachCMMC practicewithin its respectivedomain.

Theassessment objectivesfor verifying implementation.

Examples ofevidence requiredto demonstrate compliance.

CMMC 2.0 includes two levels:

Level 1: 17 basic cybersecurity practices.

Level 2: 110 practices aligned withNIST SP 800-171.

TheAssessment Guidedefines howassessorsevaluate compliance.

#2. Why the Other Answer Choices Are Incorrect:

(A) CMMC Glossary#

TheGlossaryprovidesdefinitions of termsused in CMMC but does not describe specific practices in detail.

(B) CMMC Appendices#

Appendicesinclude supplementary information likereferences and scoping guidance, but they do not provide full descriptions of practices.

(C) CMMC Assessment Process#

TheAssessment Process Guideexplainshowassessments are conducted, but it doesnot describe each practicein detail.

Final Validation from CMMC Documentation:TheCMMC Assessment Guide (Levels 1 and 2)is theofficialsource for descriptions of eachCMMC practice and process, making it thebest referencefor understanding compliance requirements.

Question #:21 - [CMMC Assessment Process (CAP)]

When an OSC requests an assessment by a C3PAO, who selects the Lead Assessor for the assessment?

A. OSC

B. C3PAO

C. C3PAO and OSC

D. OSC and Lead Assessor

Answer: B

Explanation

The CAP specifies that the C3PAO is responsible for assigning the Lead Assessor to an OSC’s assessment. While the OSC contracts with the C3PAO, the authority to appoint the Lead Assessor resides solely with the C3PAO.

Supporting Extracts from Official Content:

- CAP v2.0, Assessment Team Composition (§2.10): “The C3PAO shall designate a qualified Lead Assessor to lead the assessment.”

Why Option B is Correct:

- Only the C3PAO has the authority to select and assign the Lead Assessor.
- The OSC may influence scheduling and planning but cannot appoint assessors.
- Options A, C, and D are inconsistent with CAP requirements.

References (Official CMMC v2.0 Content):

- CMMC Assessment Process (CAP) v2.0, Assessment Team Roles and Responsibilities (§2.10).

Question #:22 - [CMMC Ecosystem]

An assessor needs to get the most accurate answers from an OSC's team members. What is the BEST method to ensure that the OSC's team members are able to describe team member responsibilities?

A. Interview groups of people to get collective answers.

B. Understand that testing is more important that interviews.

C. Ensure confidentiality and non-attribution of team members.

D. Let team members know the questions prior to the assessment.

Answer: C

Explanation

During aCMMC assessment, assessors rely on interviews to validate the implementation of cybersecurity practices within anOrganization Seeking Certification (OSC). Ensuringconfidentiality and non-attributionallows employees to speak freely without fear of retaliation or bias, leading to more accurate and candid responses.

CMMC Assessment Process and the Role of Interviews

TheCMMC Assessment Guide(Level 2) states thatinterviews are a key methodto verify compliance with security controls.

Employees may hesitate to provide truthful information if they fear negative consequences.

To obtain accurate information, assessors must create an environment where team members feel safe.

Ensuring Non-Attribution for Accurate Responses

DoD Assessment Methodologyhighlights thatinterviewees should remain anonymousin reports.

Non-attribution reduces the risk of OSC leadership influencing responses or retaliating against employees.

Employees are more likely to provideaccurateandhonestdescriptions of their responsibilities when confidentiality is guaranteed.

Why the Other Answer Choices Are Incorrect:

(A) Interview groups of people to get collective answers:

Group interviews may limit honest responses due topeer pressure or management presence.

Employees mayhesitate to contradictsupervisors or peers in a group setting.

(B) Understand that testing is more important than interviews:

While testing (e.g., reviewing logs, configurations, and security settings) is crucial, interviews providecontexton how security practices are implemented and followed.

Interviewscomplementtesting rather than being less important.

(D) Let team members know the questions prior to the assessment:

Advanced notice may allow employees toprepare rehearsed answers, which might not reflect actual practices.

This couldreduce the effectivenessof the interview process.

Step-by-Step Breakdown:Final Validation from CMMC Documentation:TheCMMC Assessment Process Guideand DoDAssessment Methodologyemphasize the importance of confidentiality in interviews to ensure accuracy.Non-attribution protects employees and ensures assessors get honest, unfiltered answers.

Thus, the correct answer is:

C. Ensure confidentiality and non-attribution of team members.

Question #:23 - [Governance and Source Documents]

Companies that knowingly defraud the government by not being in compliance with cybersecurity regulations are at risk of being held liable for:

A. The contract value plus a penalty as stated in the Cyber Claims Act

B. The contract value plus a penalty as stated in the False Claims Act

C. Three times the contract value plus a penalty as stated in the Cyber Claims Act

D. Three times the contract value plus a penalty as stated in the False Claims Act

Answer: D

Explanation

The False Claims Act (31 U.S.C. §§ 3729–3733) imposes liability on companies that knowingly misrepresent compliance in order to receive or retain federal contracts. Penalties include treble damages (three times the government’s losses) plus additional penalties per claim.

Supporting Extracts from Official Content:

- False Claims Act: “Any person who knowingly submits false claims to the Government is liable for three times the Government’s damages plus a penalty.”

- DOJ Cyber-Fraud Initiative (2021): confirms the FCA is applied to cases of misrepresenting compliance with cybersecurity requirements.

Why Option D is Correct:

- The applicable law is the False Claims Act, not a “Cyber Claims Act” (which does not exist).

- The FCA specifies treble damages plus penalties, which exactly matches Option D.

References (Official CMMC v2.0 Governance and Source Documents):

- False Claims Act (31 U.S.C. §§ 3729–3733).

- DOJ Cyber-Fraud Initiative (2021), applied to CMMC-related compliance misrepresentation.

===========

Question #:24 - [Governance and Source Documents]

In accordance with NARA directives and Chapter 33 of Title 44 (Records Management Directive), which types of data MUST have policies and procedures for disposal?

A. All recorded digital documents

B. All digital and recorded paper documents

C. All digital documents and recorded media

D. All recorded information, regardless of form or characteristics

Answer: D

Explanation

Under Title 44 U.S.C. Chapter 33 (Records Management) and NARA directives, agencies and organizations must establish policies and procedures for the disposal of all recorded information, regardless of form or characteristics. This includes paper records, electronic documents, digital media, audiovisual files, and any other information format. The requirement ensures consistent handling, retention, and lawful disposal of both federal records and CUI.

Reference Documents:

- Title 44, U.S. Code, Chapter 33: Records Management
- NARA Records Management Directive

Question #:25 - [CMMC Assessment Process (CAP)]

The results package for a Level 2 Assessment is being submitted. What MUST a Final Report. CMMC Assessment Results include?

A. Affirmation for each practice or control

B. Documented rationale for each failed practice

C. Suggested improvements for each failed practice

D. Gaps or deltas due to any reciprocity model are recorded as met

Answer: B

Explanation

Understanding the CMMC Level 2 Final Report RequirementsFor aCMMC Level 2 Assessment, theFinal CMMC Assessment Results Reportmust include:

Assessment findings for each practice

Final ratings (MET or NOT MET) for each practice

A detailed rationale for each practice rated as NOT MET

The CMMC Assessment Process (CAP) Guidestates that if a practice is markedNOT MET, theassessors must provide a rationale explaining why it failed.

This rationale helps theOSC understand what needs remediationand, if applicable, whether the deficiency can be addressed via aPlan of Action & Milestones (POA&M).

TheFinal Report serves as an official recordand must be submitted as part of theresults package.

A. Affirmation for each practice or control (Incorrect)

While the report includes aMET/NOT MET ratingfor each practice,affirmation is not a required component.

C. Suggested improvements for each failed practice (Incorrect)

Assessors do not provide recommendations for improvement—they only document findings and rationale.

Providing suggestions would create aconflict of interestperCMMC-AB Code of Professional Conduct.

D. Gaps or deltas due to any reciprocity model are recorded as met (Incorrect)

If an organization isleveraging reciprocity (e.g., FedRAMP, Joint Surveillance Voluntary Assessments), gapsmust still be documented—not automatically marked as "MET."

The correct answer isB. Documented rationale for each failed practice, as this is amandatory requirement in the Final CMMC Assessment Results Report.

References:

CMMC Assessment Process (CAP) Guide

DFARS 252.204-7021

Question #:26 - [CMMC Ecosystem]

A machining company has been awarded a contract with the DoD to build specialized parts. Testing of the parts will be done by the company using in-house staff and equipment. For a Level 1 Self-Assessment, what type of asset is this?

A. CUI Asset

B. In-scope Asset

C. Specialized Asset

D. Contractor Risk Managed Asset

Answer: C

Explanation

This question deals withasset categorizationduring aCMMC Level 1 Self-Assessment. The organization is manufacturingspecialized partsfor the DoD, butLevel 1of CMMC only concernsFederal Contract Information (FCI)—notControlled Unclassified Information (CUI). Therefore, asset categorization should follow theCMMC Scoping Guidance for Level 1.

#Step 1: Understand CMMC Level 1 and FCI

Level 1 Objective:

Implement basic safeguarding requirements as perFAR 52.204-21.

Applies to systems thatstore, process, or transmit FCI.

Self-assessments are permitted and required annually.

Source Reference:

CMMC Scoping Guidance – Level 1 (v1.0)

https://dodcio.defense.gov/CMMC

#Step 2: What is an “In-scope Asset”?

CMMC Scoping Guidance – Level 1definesIn-scope assetsas:

“Assets that process, store, or transmit FCI or provide security protection for such assets.”

In this scenario:

The machining company isperforming contract work(manufacturing DoD parts).

Thetesting is done internally, implying the systems and equipment used in testing and documentation aredirectly supporting the contract.

These systems likely handleFCIsuch as technical specifications, purchase orders, or test reports.

##Therefore, the equipment and systems used in testing are consideredIn-scope Assetsunder Level 1.

#Why the Other Options Are Incorrect

A. CUI Asset

#Incorrect forLevel 1:

CUI is only in scope atCMMC Level 2 and Level 3.

Level 1 is concerned withFCI, not CUI.

C. Specialized Asset

#Incorrect definition:

Specialized assets(defined inCMMC Level 2 Scoping) include IoT, OT, ICS, GFE, and similar types of non-enterprise assets that may require alternative treatment.

This classification isnot used in Level 1 Scoping.

D. Contractor Risk Managed Asset

#Incorrect:

Also defined underCMMC Level 2 Scopingonly.

These are assets that are not security-protected but are managed via risk-based decisions.

This term isnot applicableforCMMC Level 1 assessments.

#Step 3: Alignment with Official Documentation

According to theCMMC Scoping Guidance for Level 1:

“The assets within the self-assessment scope are those that process, store, or transmit FCI. These assets are considered ‘in-scope.’”

No other asset categorization (such as CUI asset, specialized asset, or contractor risk managed asset) is used atLevel 1.

BLUF (Bottom Line Up Front):

For aCMMC Level 1 Self-Assessment, theonlyasset category officially recognized is theIn-scope Asset— any asset that handles or protects FCI. Since the company's internal testing operations are part of fulfilling the DoD contract, the systems and staff involved arein scope.

Question #:27 - [CMMC Assessment Process (CAP)]

A Lead Assessor is presenting an assessment kickoff and opening briefing. What topic MUST be included?

A. Gathering evidence

B. Review of the OSC's SSP

C. Overview of the assessment process

D. Examination of the artifacts for sufficiency

Answer: C

Explanation

What is Required in the CMMC Assessment Kickoff and Opening Briefing?Before starting aCMMC assessment, theLead Assessormust present anopening briefingto ensure that theOrganization Seeking Certification (OSC)understands the assessment process.

Step-by-Step Breakdown:#1. Overview of the Assessment Process

The Lead Assessormust explain the CMMC assessment methodology, including:

Theassessment objectives and scope

How theassessment team will review security controls

What to expectduring interviews, testing, and document review

This ensurestransparency and alignmentbetween the assessors and the OSC.

#2. Why the Other Answer Choices Are Incorrect:

(A) Gathering Evidence#

Evidence collection is part of the assessment butnot the primary topic of the opening briefing.

(B) Review of the OSC's SSP#

While theSSP is a key document, reviewing it is part of the assessment,not the kickoff briefing.

(D) Examination of the artifacts for sufficiency#

Artifact review happens laterin the assessment process,not during the kickoff.

TheCMMC Assessment Process Guidestates that theopening briefing must include an overview of the assessment process, ensuring the OSC understands the expectations and methodology.

Final Validation from CMMC Documentation:Thus, the correct answer is:

#C. Overview of the assessment process.

Question #:28 - [CMMC Ecosystem]

A CCP is providing consulting services to a company who is an OSC. The CCP is preparing the OSC for a CMMC Level 2 assessment. The company has asked the CCP who is responsible for determining the CMMC Assessment Scope and who validates its CMMC Assessment Scope. How should the CCP respond?

A. "The OSC determines the CMMC Assessment Scope, and the CCP validates the CMMC Assessment Scope."

B. "The OSC determines the CMMC Assessment Scope, and the C3PAO validates the CMMC Assessment Scope."

C. "The CMMC Lead Assessor determines the CMMC Assessment Scope, and the OSC validates the CMMC Assessment Scope."

D. "The CMMC C3PAO determines the CMMC Assessment Scope, and the Lead Assessor validates the CMMC Assessment Scope."

Answer: B

Explanation

In aCMMC Level 2 assessment, theOrganization Seeking Certification (OSC)is responsible for identifying theassessment scopebased on theCMMC Scoping Guidanceprovided by theCyber AB (Cyber Accreditation Body) and DoD.

The OSC must determine which assets and systems handleControlled Unclassified Information (CUI)and categorize them accordingly.

Reference:

CMMC Scoping Guidance for Level 2, which outlines asset categorization and scoping considerations.

Step 2: Role of the C3PAO in Scope ValidationOnce the OSC has determined itsCMMC assessment scope, aCMMC Third-Party Assessment Organization (C3PAO)is responsible forvalidatingthe scope during theassessment planning phase.

TheC3PAO reviewsthe OSC’s scope to ensure it aligns withDoD’s scoping guidance, ensuring that all relevant assets, networks, and policies required forCMMC Level 2 certificationare correctly identified.

If there are discrepancies, the C3PAO works with the OSC to adjust the scope before proceeding with the assessment.

Reference:

CMMC Assessment Process (CAP) Guide, which describes thescope validation responsibilities of a C3PAO.

Step 3: Why Other Answer Choices Are IncorrectChoice A (Incorrect):A CCP (Certified CMMC Professional) doesnothave the authority to validate the scope. Their role is to guide and consult, but final validation is the C3PAO's responsibility.

Choice C (Incorrect):TheCMMC Lead Assessor(part of the C3PAO team) does notdeterminethe scope; instead, the OSC does.

Choice D (Incorrect):TheC3PAO validates the scopebut doesnot determine it—this is the OSC’s responsibility.

Final Confirmation of Correct Answer:OSC determines the CMMC Assessment Scope.

C3PAO validates the CMMC Assessment Scope.

Thus, the correct answer isB. "The OSC determines the CMMC Assessment Scope, and the C3PAO validates the CMMC Assessment Scope."

Question #:29 - [CMMC Ecosystem]

The Lead Assessor interviews a network security specialist of an OSC. The incident monitoring report for the month shows that no security incidents were reported from OSC's external SOC service provider. This is provided as evidence for RA.L2-3.11.2: Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. Based on this information, the Lead Assessor should conclude that the evidence is:

A. inadequate because it is irrelevant to the practice.

B. adequate because it fits well for expected artifacts.

C. adequate because no security incidents were reported.

D. inadequate because the OSC's service provider should be interviewed.

Answer: A

Explanation

Understanding RA.L2-3.11.2: Vulnerability ScanningTheRA.L2-3.11.2practice requires organizations to:

#Regularly scan for vulnerabilitiesin systems and applications.

#Perform scans when new vulnerabilities are identified.

#Use vulnerability scanning tools or servicesto proactively detect security weaknesses.

Anincident monitoring reporttrackssecurity incidents, notvulnerability scanning activities.

Vulnerability scanning reportsshould include:#A list of vulnerabilities detected.#Remediation actions taken. #Scan frequency and schedule.

Theabsence of reported security incidentsdoesnotconfirm that vulnerability scans were performed.

Why Is an Incident Monitoring Report Irrelevant?

A. Inadequate because it is irrelevant to the practice # Correct

Alack of reported security incidents does not confirm that vulnerability scanning was performed.

B. Adequate because it fits well for expected artifacts # Incorrect

Incident monitoring reportsare not expected artifactsfor this control.Vulnerability scan reportsare required instead.

C. Adequate because no security incidents were reported # Incorrect

The absence of incidents does not mean the OSC is performing vulnerability scanning. This isnot valid evidence.

D. Inadequate because the OSC's service provider should be interviewed # Incorrect

While interviewing the provider may be useful, themain issue is that the provided evidence is irrelevant. Thecorrect evidence (vulnerability scan reports) is missing.

Why is the Correct Answer "A. Inadequate because it is irrelevant to the practice"?

NIST SP 800-171 (Requirement 3.11.2 – Vulnerability Scanning)

Defines the requirement toscan for vulnerabilities periodically and when new threats emerge.

CMMC Assessment Guide for Level 2

Specifies that evidence for RA.L2-3.11.2 should includevulnerability scan reports, not incident monitoring reports.

CMMC 2.0 Model Overview

Confirms that organizationsmust proactively identify vulnerabilities through scanning, not just rely on incident detection.

CMMC 2.0 References Supporting This Answer:

Question #:30 - [Roles and Responsibilities]

Which MINIMUM Level of certification must a contractor successfully achieve to receive a contract award requiring the handling of CUI?

A. Level 1

B. Level 2

C. Level 3

D. Any level

Answer: B

Explanation

1. Understanding CMMC 2.0 Levels and CUI Handling RequirementsUnderCMMC 2.0, contractors handlingControlled Unclassified Information (CUI)must meet aminimumcertification level to be eligible for contract awards involving CUI.

Level 1 (Foundational) – 17 Practices

Covers onlyFederal Contract Information (FCI)security.

Does NOT meet CUI handling requirements.

Level 2 (Advanced) – 110 Practices#

REQUIRED for handling CUI.

Aligns withNIST SP 800-171, which establishes security controls for protecting CUI.

Contractorsmust achieve Level 2for contracts requiring CUI protection.

Level 3 (Expert) – 110+ Practices

Required for contracts involvinghigh-value CUIandcritical national security information.

Includesadditionalprotections fromNIST SP 800-172.

CMMC 2.0 Levels:

TheCMMC 2.0 Model Overviewclearly states that Level 2 is required for contractorshandling CUI.

DFARS 252.204-7012mandates that contractors protecting CUI must implementNIST SP 800-171, which is thefoundation of CMMC Level 2.

TheDoD’s CMMC Assessment Guidefor Level 2 specifies thatorganizations handling CUI must demonstrate full implementation of 110 practices from NIST SP 800-171to qualify for contract awards.

2. Official CMMC 2.0 References Confirming Level 2 for CUI

A. Level 1#

Only covers FCI, not CUI.

Does notmeet DoD requirements for protectingCUI.

C. Level 3#

While Level 3 offersadditional protectionsfor high-risk CUI, it isnot the minimumrequirement.

Level 2 is the minimumneeded to handle CUI.

D. Any level#

OnlyLevel 2 and higherare eligible for contracts requiring CUI protection.

Level 1 doesnotmeet CUI security standards.

3. Why the Other Options Are Incorrect

Question #:31 - [Implementation and Scoping]

A server is used to store FCI with a cloud provider long-term. What is the server considered?

A. In scope, because the cloud provider will be storing the FCI data

B. Out of scope, because the cloud provider stores the FCI data long-term

C. In scope, because the cloud provider is required to be CMMC Level 2 certified

D. Out of scope, because encryption is always used when the cloud provider stores the FCI data

Answer: A

Explanation

Assets that store, process, or transmit FCI or CUI are always in scope for CMMC. If a server with a cloud provider is used for long-term storage of FCI, that server is considered in scope because it directly holds covered data.

Supporting Extracts from Official Content:

- CMMC Scoping Guide for Level 1: “Assets that store, process, or transmit FCI are in scope.”
- CMMC Scoping Guide for Level 2: confirms the same rule applies for CUI.

Why Option A is Correct:

- The server stores FCI, making it automatically in scope.
- Option B is incorrect because long-term storage does not make an asset out of scope.
- Option C is incorrect — Level 1 (FCI) does not require a Level 2 certified provider.
- Option D is incorrect because encryption does not remove scope requirements.

References (Official CMMC v2.0 Content):

- CMMC Scoping Guide, Level 1.
- CMMC Model v2.0, Scoping and Implementation guidance.

===========

Question #:32 - [CMMC Ecosystem]

When assessing an OSC for CMMC: the Lead Assessor should use the information from the Discussion and Further Discussion sections in each practice because it:

A. is normative for an OSC to follow.

B. contains examples that an OSC must implement.

C. is mandatory and aligns with FAR Clause 52.204-21.

D. provides additional information to facilitate the assessment of the practice.

Answer: D

Explanation

Understanding the Role of "Discussion" and "Further Discussion" Sections in CMMC AssessmentsWhen assessing anOrganization Seeking Certification (OSC)forCMMC compliance, theLead Assessorrelies on various sources of guidance.

Eachpracticein the CMMC model includes:

The Practice Statement– The official requirement the OSC must meet.

Discussion Section– Providesclarifications, interpretations, and guidancefor implementation.

Further Discussion Section– Expands on the practice,offering additional details, best practices, and examples.

These sections arenot mandatory, but they help assessorsinterpret and evaluatewhether an OSC has met the practice requirements.

TheDiscussion and Further Discussion sectionsprovidecontext, explanations, and examplesto assist theLead Assessorin understanding how an OSC might demonstrate compliance.

Theyhelp guide the assessment processbut arenot prescriptiveormandatoryfor an OSC.

Theassessor uses these sectionsto verify whether theOSC's implementation meets the intent of the requirement.

Why "Provides Additional Information to Facilitate the Assessment" is Correct?Breakdown of Answer ChoicesOption

Description

Correct?

A. Is normative for an OSC to follow.

#Incorrect–The sections areguidance, notnormative (mandatory)requirements.

B. Contains examples that an OSC must implement.

#Incorrect–Examples aresuggestions, notmandatory implementations.

C. Is mandatory and aligns with FAR Clause 52.204-21.

#Incorrect–The "Discussion" sections arenot mandatoryand arenot tied directlyto FAR 52.204-21.

D. Provides additional information to facilitate the assessment of the practice.

#Correct – These sections help the assessor evaluate compliance but do not mandate specific implementations.

TheCMMC Assessment Guidestates that theDiscussion and Further Discussion sections provide clarificationsto help both assessors and OSCs.

These sections arenot bindingbut serve asinterpretive guidanceto assist in assessments.

Official References from CMMC 2.0 DocumentationFinal Verification and ConclusionThe correct answer isD. Provides additional information to facilitate the assessment of the practice.This aligns withCMMC 2.0 documentation and assessment guidelines.

Question #:33 - [CMMC Ecosystem]

Which principles are included in defining the CMMC-AB Code of Professional Conduct?

A. Objectivity, classification, and information accuracy

B. Objectivity, confidentiality, and information integrity

C. Responsibility, classification, and information accuracy

D. Responsibility, confidentiality, and information integrity

Answer: B

Explanation

Understanding the CMMC-AB Code of Professional ConductTheCybersecurity Maturity Model Certification Accreditation Body (CMMC-AB), now referred to asThe Cyber AB, establishes aCode of Professional Conduct (CoPC)for all individuals involved in CMMC assessments, includingCertified Assessors (CAs), Certified Professionals (CPs), and C3PAOs (Certified Third-Party Assessment Organizations).

Thecore principlesoutlined in theCMMC-AB Code of Professional Conductinclude:

Responsibility

CMMC professionals must takefull accountabilityfor their actions, ensuring that assessments are conducted withintegrity and professionalism.

They mustadhere to all ethical and regulatory requirementsestablished by The Cyber AB and the DoD.

Confidentiality

CMMC professionals mustprotect sensitive information, includingControlled Unclassified Information (CUI) andFederal Contract Information (FCI).

They are required toadhere to non-disclosure agreements (NDAs)and avoid improper information sharing.

Information Integrity

All reports, findings, and recommendations in CMMC assessments must beaccurate, unbiased, and truthful.

Assessors mustavoid conflicts of interestand ensure that all data provided in an assessment isverifiable and free from misrepresentation.

Answer A (Incorrect): "Classification" is not a primary principle of the CMMC-AB CoPC. The focus is on protectingCUI and FCI, not on classification procedures.

Answer B (Incorrect): "Objectivity" is important, but it is not explicitly listed as one of the three core principles in theCMMC-AB Code of Professional Conduct.

Answer C (Incorrect): "Classification" is not a guiding principle in the CoPC.

Answer D (Correct):The Code of Professional Conduct explicitly emphasizes responsibility, confidentiality, and information integrity.

The correct answer isD. Responsibility, Confidentiality, and Information Integrity.

These principlesensure that all CMMC professionals maintain ethical standards and uphold the integrity of the certification process.

References:

CMMC-AB Code of Professional Conduct (CoPC)

The Cyber AB Ethical Guidelines

CMMC Assessment Process (CAP) Guide

Question #:34 - [CMMC Ecosystem]

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?

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 ProcessWhen anOrganization Seeking Certification (OSC) engages aCertified Third-Party Assessment Organization (C3PAO)to conduct aCMMC Level 2 Assessment, anAssessment Planis developed to outline the scope, methodology, and logistics of the assessment.

According to theCMMC Assessment Process (CAP) Guide, theAssessment 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.

TheLead Assessorensures that theAssessment Plan aligns with CMMC-AB and DoD requirements, including methodology, objectives, and evidence collection.

TheC3PAOprovides organizational approval, confirming that the assessment is conducted according toCMMC-AB rules and contractual agreements.

A. OSC and Sponsor (Incorrect)

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

Asponsoris not part of the sign-off process in CMMC assessments.

B. OSC and CMMC-AB (Incorrect)

TheOSCdoes not formally approve theAssessment Plan—this responsibility belongs to the assessment team.

TheCMMC-ABdoes not sign off on individualAssessment Plans.

D. C3PAO and Assessment Official (Incorrect)

"Assessment Official" isnot a defined rolein the CMMC assessment process.

TheC3PAOis involved, but it must be theLead Assessorwho signs off, not an unspecified official.

The correct answer isC. Lead Assessor and C3PAO.

TheLead Assessorensures assessment integrity, while theC3PAOprovides official authorization.

References:

CMMC Assessment Process (CAP) Guide

CMMC 2.0 Level 2 Certification Procedures

The Cyber AB Assessment Guidelines

Question #:35 - [CMMC Ecosystem]

An Assessment Team Member is conducting a CMMC Level 2 Assessment for an OSC that is in the process of inspecting Assessment Objects for AC.L1-3.1.1: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) to determine the adequacy of evidence provided by the OSC. Which Assessment Method does this activity fall under?

A. Test

B. Observe

C. Examine

D. Interview

Answer: C

Explanation

Understanding Assessment Methods in CMMC 2.0According to theCMMC Assessment Process (CAP) Guide, assessors usethree primary assessment methodsto determine compliance with security practices:

Examine– Reviewing documents, policies, configurations, and system records.

Interview– Speaking with personnel to gather insights into security processes.

Test– Performing technical validation of system functions and security controls.

TheAssessment Team Memberis inspectingAssessment Objects(e.g., system configurations, user access control settings, policies) to determine if the OSC's evidence is sufficient forAC.L1-3.1.1 (Access Control – Authorized Users).

This activity aligns directly with theExaminemethod, which involves reviewing artifacts such as:

Access control lists (ACLs)

System user authentication logs

Account management policies

Role-based access control settings

"Observe" (Option B)is incorrect because "observing" is not an official assessment method in CMMC.

"Test" (Option A)is incorrect because the assessment is not actively executing a function but ratherreviewingevidence.

"Interview" (Option D)is incorrect because no personnel are being questioned—only documentation is being reviewed.

CMMC Assessment Process (CAP) Guide, Section 3.5 – Assessment Methods

CMMC Level 2 Assessment Guide – Access Control Practices (AC.L1-3.1.1)

Why Option C (Examine) is CorrectOfficial CMMC Documentation ReferencesFinal VerificationSince the activity involves reviewing documents and records to verify access control measures, it falls under theExaminemethod, makingOption C the correct answer.

Question #:36 - [CMMC Model Overview]

Which phase of the CMMC Assessment Process includes developing the assessment plan?

A. Phase 1

B. Phase 2

C. Phase 3

D. Phase 4

Answer: A

Explanation

Understanding the Phases of the CMMC Assessment ProcessTheCMMC Assessment Process (CAP)consists of multiple phases, with each phase focusing on a different aspect of the assessment.Developing the assessment planoccurs inPhase 1, which is thePre-Assessment Phase.

Engagement Agreement: TheOSC (Organization Seeking Certification)and theCertified Third-Party Assessment Organization (C3PAO)formalize the assessment contract.

Developing the Assessment Plan: TheLead Assessorand the assessment team create anAssessment Plan, which outlines:

Scope of the assessment

CMMC Level requirements

Assessment methodology

Timeline and logistics

Initial Data Collection: Review of system documentation, policies, and relevant security controls.

Key Activities in Phase 1 – Pre-Assessment Phase

A. Phase 1 # Correct

Phase 1 is where the assessment plan is developed.

It ensuresclarity on scope, methodology, and logistics before the assessment begins.

B. Phase 2 # Incorrect

Phase 2 is theAssessment Conduct Phase, where assessorsexecutethe plan by examining evidence and interviewing personnel.

C. Phase 3 # Incorrect

Phase 3 is thePost-Assessment Phase, which involvesfinalizing findings and submitting reports, not developing the plan.

D. Phase (Incomplete Answer) # Incorrect

The question requires a specific phase, and the correct one isPhase 1.

Why is the Correct Answer "Phase 1" (A)?

CMMC Assessment Process (CAP) Document

DefinesPhase 1as the stage where the assessment plan is developed.

CMMC Accreditation Body (CMMC-AB) Guidelines

Specifies thatplanning and pre-assessment activities occur in Phase 1.

CMMC 2.0 Certification Workflow

Outlines the assessment planning process as part of theinitial engagementbetween theC3PAO and the OSC.

CMMC 2.0 References Supporting this Answer:

Question #:37 - [CMMC Ecosystem]

While developing an assessment plan for an OSC. it is discovered that the certified assessor will be interviewing a former college roommate. What is the MOST correct action to take?

A. Do not inform the OSC and the C3PAO of the possible conflict of interest, and continue as planned.

B. Inform the OSC and the C3PAO of the possible conflict of interest, and start the entire process over without the conflicted team member.

C. Inform the OSC and the C3PAO of the possible conflict of interest but since it has been an acceptable amount of time since college, no conflict of interest exists, and continue as planned.

D. Inform the OSC and the C3PAO of the possible conflict of interest, document the conflict and mitigation actions in the assessment plan, and if the mitigation actions are acceptable, continue with the assessment.

Answer: D

Explanation

TheCybersecurity Maturity Model Certification (CMMC) Assessment Process (CAP)outlines strict guidelines regardingconflicts of interest (COI)to ensure the integrity and impartiality of assessments conducted byCertified Third-Party Assessment Organizations (C3PAOs)andCertified Assessors (CAs).

The scenario presented involves apotential conflict of interestdue to a prior relationship (former college roommate) between thecertified assessorand an individual at theOrganization Seeking Certification (OSC). While this prior relationship does not automatically disqualify the assessor, it must bedisclosed, documented, and mitigated appropriately.

Inform the OSC and C3PAO of the Potential Conflict of Interest

TheCMMC Code of Professional Conduct (CoPC)requires assessors to disclose any potential conflicts of interest.

Transparency ensures that all parties, including theOSC and C3PAO, are aware of the situation.

Document the Conflict and Mitigation Actions in the Assessment Plan

PerCMMC CAP documentation, potential conflicts should be assessed based on their material impact on the objectivity of the assessment.

The conflict and proposed mitigation strategies must beformally recorded in the assessment planto provide an audit trail.

Determine If the Mitigation Actions Are Acceptable

If theOSC and C3PAOdetermine that the mitigation actions adequatelyeliminate or reduce the risk of bias, the assessment may proceed.

Common mitigation strategies include:

Assigning another assessor forinterviews with the conflicted individual.

Ensuring thatdecisions regarding the OSC’s compliance are reviewed independently.

Proceed with the Assessment If Mitigation Is Acceptable

If the mitigation actions sufficiently address the conflict, the assessment may continue understrict adherence to documented procedures.

CMMC Conflict of Interest Handling Process

A. Do not inform the OSC and the C3PAO of the possible conflict of interest, and continue as planned. #Incorrect. This violates CMMC’s integrity requirements and could result indisciplinary actions against the assessor or invalidation of the assessment. Transparency is mandatory.

B. Inform the OSC and the C3PAO of the possible conflict of interest, and start the entire process over without the conflicted team member.#Incorrect. The CAP doesnotmandate immediate reassignment unless the conflict isunresolvable. Instead, mitigation strategies should be considered first.

C. Inform the OSC and the C3PAO of the possible conflict of interest but since it has been an acceptable amount of time since college, no conflict of interest exists, and continue as planned.#Incorrect.The passage of time alone does not automatically eliminate a conflict of interest. Proper documentation and mitigation are still required.

Why the Other Answers Are Incorrect

CMMC Assessment Process (CAP) Document– Defines COI requirements and mitigation actions.

CMMC Code of Professional Conduct (CoPC)– Outlines ethical responsibilities of assessors.

CMMC Accreditation Body (Cyber-AB) Guidance– Provides rules on conflict resolution.

CMMC Official ReferencesThus,option D is the most correct choice, as it aligns with the official CMMC conflict of interest procedures.

Question #:38 - [CMMC Model Overview]

Which organization is the governmental authority responsible for identifying and marking CUI?

A. NARA

B. NIST

C. CMMC-AB

D. Department of Homeland Security

Answer: A

Explanation

Step 1: Define CUI (Controlled Unclassified Information)CUI is information thatrequires safeguarding or dissemination controlspursuant to and consistent with applicable law, regulations, and government-wide policies, butis not classifiedunder Executive Order 13526 or the Atomic Energy Act.

#Step 2: Authority over CUI — NARA’s RoleNARA – National Archives and Records Administration, specifically theInformation Security Oversight Office (ISOO), is thegovernment-wide executive agentresponsible for implementing the CUI program.

Source:

32 CFR Part 2002 – Controlled Unclassified Information (CUI)

Executive Order 13556 – Controlled Unclassified Information

CUI Registry – https://www.archives.gov/cui

NARA:

Maintains theCUI Registry,

Issuesmarking and handling guidance,

DefinesCUI categoriesand their authority under law or regulation,

Trains and informs Federal agencies and contractors on CUI policy.

B. NIST# NIST (National Institute of Standards and Technology) developstechnical standards(e.g., SP 800-171), but it doesnot define or mark CUI. It helps secure CUI once it's identified.

C. CMMC-AB (now Cyber AB)# The Cyber AB is theCMMC ecosystem's accreditation body, not a government agency, and hasno authority over CUI classification or marking.

D. Department of Homeland Security (DHS)# While DHS mayhandle and protect CUI internally, it is not the executive agent for the CUI program.

#Why the Other Options Are Incorrect

NARAis theofficial U.S. government authorityresponsible for defining, categorizing, and marking CUI via theCUI Registryand associated policies underExecutive Order 13556.

Question #:39 - [CMMC Ecosystem]

During the planning phase of the Assessment Process. C3PAO staff are reviewing the various entities associated with an OSC that has requested a CMMC Level 2 Assessment. Which term describes the people, processes, and technology external to the HQ Organization that participate in the assessment but will not receive a CMMC Level unless an enterprise Assessment is conducted?

A. Host Unit

B. Organization

C. Coordinating Unit

D. Supporting Organization/Unit

Answer: D

Explanation

In the context of the Cybersecurity Maturity Model Certification (CMMC) Assessment Process, understanding the roles of various entities associated with an Organization Seeking Certification (OSC) is crucial during the planning phase. When a Certified Third-Party Assessment Organization (C3PAO) staff reviews these entities for a CMMC Level 2 Assessment, it's essential to distinguish between internal components and external participants.

Step-by-Step Explanation:

Definition of the HQ Organization:

The HQ Organization refers to the entire legal entity delivering services under the terms of a Department of Defense (DoD) contract. This entity is responsible for ensuring compliance with CMMC requirements.

Identification of External Entities:

External entities encompass people, processes, and technology that are not part of the HQ Organization but support its operations. These entities participate in the assessment process due to their involvement in handling Controlled Unclassified Information (CUI) or Federal Contract Information (FCI) related to the DoD contract.

Role of Supporting Organizations/Units:

According to the CMMC Assessment Process documentation, Supporting Organizations are defined as "the people, procedures, and technology external to the HQ Organization that support the Host Unit." These external entities are integral to the operations of the Host Unit but are not encompassed within the HQ Organization's immediate structure.

Assessment Implications:

While Supporting Organizations/Units play a vital role in supporting the Host Unit, they do not receive a separate CMMC Level certification unless an enterprise assessment is conducted. In such cases, the assessment would encompass both the HQ Organization and its Supporting Organizations to ensure comprehensive compliance across all associated entities.

References:

CMMC Assessment Process documentation defines Supporting Organizations as external entities that support the Host Unit.

Cyberab

By accurately identifying and understanding the role of Supporting Organizations/Units, the C3PAO ensures that all relevant entities are considered during the assessment planning phase, thereby maintaining the integrity and comprehensiveness of the CMMC Level 2 Assessment.

Question #:40 - [CMMC Ecosystem]

Regarding the Risk Assessment (RA) domain, what should an OSC periodically assess?

A. Organizational operations, business assets, and employees

B. Organizational operations, business processes, and employees

C. Organizational operations, organizational assets, and individuals

D. Organizational operations, organizational processes, and individuals

Answer: C

Explanation

TheRisk Assessment (RA) domainaligns withNIST SP 800-171 control family 3.11 (Risk Assessment)and is designed to help organizationsidentify, assess, and manage cybersecurity risksthat could impact their operations.

TheRA.3.144 practice(which is a CMMC Level 2 requirement) explicitly states:

"Periodically assess therisktoorganizational operations (including mission, functions, image, or reputation), organizational assets, and individualsresulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI."

This means that OSCs (Organizations Seeking Certification) should regularly evaluate risks to:

#Organizational operations(e.g., mission, business continuity, functions)

#Organizational assets(e.g., data, IT systems, intellectual property)

#Individuals(e.g., employees, contractors, customers affected by security risks)

Thus, the correct answer isC. Organizational operations, organizational assets, and individuals.

A. Organizational operations, business assets, and employees#Incorrect."Business assets"is not the correct terminology used in CMMC/NIST SP 800-171. Instead,"organizational assets"is the proper term.

B. Organizational operations, business processes, and employees#Incorrect."Business processes"is not a part of the formal risk assessment requirement. The correct scope includesorganizational assetsandindividuals, not just processes.

D. Organizational operations, organizational processes, and individuals#Incorrect. While processes are important,organizational assetsmust be considered in the assessment, not just processes.

Why the Other Answers Are Incorrect

CMMC 2.0 Model (Level 2 - RA.3.144)– Specifies that risk assessments must coverorganizational operations, organizational assets, and individuals.

NIST SP 800-171 (3.11.1)– Reinforces the same risk assessment scope.

CMMC Official ReferencesThus,option C (Organizational operations, organizational assets, and individuals) is the correct answerbased on official CMMC risk assessment requirements.

Question #:41 - [CMMC Ecosystem]

An OSC has submitted evidence for an upcoming assessment. The assessor reviews the evidence and determines it is not adequate or sufficient to meet the CMMC practice. What can the assessor do?

A. Notify the CMMC-AB.

B. Cancel the assessment.

C. Postpone the assessment.

D. Contact the C3PAO for guidance.

Answer: D

Explanation

Step 1: Understand the Assessor’s Role and Chain of ResponsibilityDuring a CMMC assessment, the assessor ispart of the team organized by a C3PAO (Certified Third-Party Assessment Organization). If the assessor determines thatevidence is insufficient or inadequate, they arenot authorizedto act independently in terms of halting or postponing the assessment.

Source Reference: CMMC Assessment Process (CAP) v1.0 – Section 3.5.4 & 3.5.6

"If the Assessment Team identifies gaps in the sufficiency or adequacy of evidence, they must work with the Lead Assessor and C3PAO to determine the appropriate course of action."

The C3PAO is responsible for overseeing the assessment lifecycle.

If evidence isnot adequate, the assessor mustescalate within their organization(i.e., to the Lead Assessor or C3PAO point of contact) to:

Request clarifications from the OSC,

Determine if additional evidence can be requested,

Decide on continuing, pausing, or modifying the assessment schedule.

#Step 2: Why Contacting the C3PAO Is the Correct Action

A. Notify the CMMC-AB# Incorrect. The Cyber AB (formerly CMMC-AB) isnot involved in operational aspectsof assessments. They do not manage day-to-day assessment decisions.

B. Cancel the assessment# Incorrect. An assessorcannot unilaterally cancelan assessment. Only theC3PAO, in consultation with all parties, may take such action.

C. Postpone the assessment# Incorrect. Postponements are logistical decisions that must be managed through theC3PAO, not an individual assessor.

#Why the Other Options Are Incorrect

When an assessor determines that the evidence submitted by an OSC is inadequate or insufficient to meet a CMMC practice, thecorrect and required course of action is to consult with the C3PAO. The C3PAO will provide guidance or coordinate appropriate next steps.

Question #:42 - [CMMC Assessment Process (CAP)]

A Lead Assessor is preparing to conduct a Readiness Review during Phase 1 of the Assessment Process. How much evidence MUST be gathered for each practice?

A. A sufficient amount

B. At least 2 Assessment Objects

C. Evidence that is deemed adequate

D. Evidence to support at least 2 Assessment Methods

Answer: A

Explanation

During a Readiness Review (Phase 1), the purpose is to validate whether an OSC is prepared to move forward with a formal assessment. The CAP specifies that the Lead Assessor must collect sufficient evidence for each practice to make a preliminary determination of readiness.

Supporting Extracts from Official Content:

- CAP v2.0, Readiness Review (§2.14): “The Lead Assessor must collect a sufficient amount of evidence for each practice to determine the OSC’s readiness.”

Why Option A is Correct:

- The requirement is for sufficient evidence; CAP does not mandate a set number of assessment objects or methods.

- Options B, C, and D incorrectly suggest minimum counts or methods that are not part of the readiness review requirements.

References (Official CMMC v2.0 Content):

- CMMC Assessment Process (CAP) v2.0, Phase 1 Readiness Review.

===========

Question #:43 - [CMMC Model Overview]

Validation of findings is an iterative process usually performed during the Daily Checkpoints throughout the entire assessment process. As a validation activity, why are the preliminary findings important?

A. It allows the OSC to comment and provide additional evidence.

B. It determines whether the OSC will be rated MET or NOT MET on their assessment.

C. It confirms that the Assessment Team's findings are right and cannot be changed.

D. It corroborates the Assessment Team's understanding of the CMMC practices and controls.

Answer: A

Explanation

1. Understanding the Validation of Findings in CMMC AssessmentsValidation of findings is an essential part of theCMMC assessment process, ensuring that observations and preliminary conclusions drawn by the assessment team are accurate, fair, and based on complete evidence. This process occurs iteratively during theDaily Checkpointsand is fundamental in determining the overall compliance status of theOrganization Seeking Certification (OSC).

2. The Role of Preliminary Findings in the Assessment ProcessPreliminary findings arenot finalbut rather a mechanism for ensuring transparency, accuracy, and fairness. These findings serve several key purposes:

Allows for OSC Input & Clarification: The OSC has an opportunity to review andprovide additional evidencethat may address deficiencies identified by the assessment team.

Prevents Misinterpretations: By allowing the OSC to comment, the assessment team can refine or correct their understanding of the OSC's implementation of CMMC practices.

Supports Fair and Informed Ratings: Before finalizing MET or NOT MET determinations, the assessment team ensures they have considered all relevant evidence.

Encourages a Collaborative Assessment Process: This validation activity fosters open communication between assessors and the OSC, reducing disputes and misunderstandings.

The primary purpose of preliminary findings is to allow theOSC to comment and provide additional evidencebefore final determinations are made.

This aligns withCMMC Assessment Process guidance, which emphasizes iterative validation of findings throughDaily Checkpoints and Final Outbriefdiscussions.

The validation of findings ensures thatOSC responses and supplementary evidence are considered, making the assessment process more accurate and fair.

3. Why Answer Choice "A" is Correct4. Why Other Answer Choices Are IncorrectOption

Reason for Elimination

B. It determines whether the OSC will be rated MET or NOT MET on their assessment.

Incorrect: Preliminary findings do not directly determine the final rating. The assessment team reviews all collected evidence before making a final decision.

C. It confirms that the Assessment Team's findings are right and cannot be changed.

Incorrect: Findings arenot finalat the preliminary stage. The OSC has the opportunity to challenge findings by providing new or clarifying evidence.

D. It corroborates the Assessment Team's understanding of the CMMC practices and controls.

Partially Correct but Not the Best Answer: While validation helps refine understanding, itsprimary function is to allow OSC input, making optionA the most accurate choice.

CMMC Assessment Process (CAP) Document:

Section 5.3 – Validation of Findings: "The OSC is given the opportunity to provide additional evidence and comments to clarify or supplement preliminary assessment results."

Section 5.4 – Daily Checkpoints: "The assessment team discusses preliminary findings with the OSC, allowing the organization to address concerns in real time."

CMMC 2.0 Level 2 Scoping & Assessment Guide:

Confirms that the assessment process includes continuous dialogue with the OSC before final determinations are made.

5. Official CMMC References Supporting This Answer6. ConclusionPreliminary findings are acrucial validation stepin CMMC assessments, ensuring that organizations have the opportunity toprovide additional evidence and clarify potential misunderstandings. This iterative process improves accuracy and fairness in determining compliance with CMMC requirements. Therefore, the correct answer is:

A. It allows the OSC to comment and provide additional evidence.

Question #:44 - [CMMC Model Overview]

Which phase of the CMMC Assessment Process includes the task to identify, obtain inventory, and verify evidence?

A. Phase 1: Plan and Prepare Assessment

B. Phase 2: Conduct Assessment

C. Phase 3: Report Recommended Assessment Results

D. Phase 4: Remediation of Outstanding Assessment Issues

Answer: A

Explanation

Understanding the CMMC Assessment ProcessTheCMMC Assessment Process (CAP)consists offour phases, each with specific tasks and objectives.

Phase 1: Plan and Prepare Assessment– Planning, scheduling, and preparing for the assessment.

Phase 2: Conduct Assessment–Gathering and verifying evidence, conducting interviews, and evaluating compliance.

Phase 3: Report Recommended Assessment Results– Documenting findings and reporting results.

Phase 4: Remediation of Outstanding Assessment Issues– Allowing the organization to address any deficiencies.

Why "Phase 2: Conduct Assessment" is Correct?DuringPhase 2: Conduct Assessment, theAssessment Teamperforms key activities, including:

#Identifying required evidencefor compliance verification.

#Obtaining and reviewing artifacts(e.g., security policies, configurations, logs).

#Verifying the sufficiency of evidenceagainst CMMC practice requirements.

#Interviewing key personneland observing cybersecurity implementations.

Since the question specifically mentions"identify, obtain inventory, and verify evidence,"this task directly falls underPhase 2: Conduct Assessment.

Breakdown of Answer ChoicesOption

Description

Correct?

A. Phase 1: Plan and Prepare Assessment

#Incorrect–This phase focuses onscheduling, logistics, and planning, not evidence collection.

B. Phase 2: Conduct Assessment

#Correct – This phase involves gathering, verifying, and reviewing evidence.

C. Phase 3: Report Recommended Assessment Results

#Incorrect–This phasedocumentsresults but doesnotcollect evidence.

D. Phase 4: Remediation of Outstanding Assessment Issues

#Incorrect–This phase focuses oncorrective actions, not evidence collection.

CMMC Assessment Process Guide (CAP)–Phase 2: Conduct Assessmentexplicitly includes tasks such asgathering and verifying evidence.

Official References from CMMC 2.0 DocumentationFinal Verification and ConclusionThe correct answer isB. Phase 2: Conduct Assessment, as this phase includesidentifying, obtaining, and verifying evidence, which is critical for determining CMMC compliance.

Question #:45 - [CMMC Ecosystem]

Which document BEST determines the existence of FCI and/or CUI in scoping an assessment with an OSC?

A. OSC SSP

B. OSC POA&M

C. OSC Evidence

D. OSC Contract with DoD

Answer: D

Explanation

Understanding DFARS Clause 252.204-7012TheDefense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012is a mandatory cybersecurity clause required inall DoD contracts and solicitationsthat involveControlled Unclassified Information (CUI).

Key Requirements of DFARS 252.204-7012#Implements NIST SP 800-171security controls for contractors handlingCUI.

#Requirescyber incident reportingto theDoD Cyber Crime Center (DC3)within72 hours.

#Mandatesadequate security measuresto protectDoD information systems.

#Applies toall DoD contracts, except for those exclusively acquiring COTS items.

Option A (Correct):DFARS 252.204-7012must be included in all DoD contracts and solicitationswhen CUI is involved.

Option B (Incorrect):FAR Part 12 procedures apply tocommercial item acquisitions, but DFARS 7012 appliesregardless of procurement procedures.

Option C (Incorrect):Contractssolely for COTS (Commercial Off-the-Shelf) productsare exemptfrom DFARS 7012.

Option D (Incorrect):COTS itemssold without modificationsarenot requiredto include DFARS 7012.

DFARS Clause 252.204-7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting)

NIST SP 800-171– The required cybersecurity standard for contractors under DFARS 7012.

Why "All DoD Solicitations and Contracts" is Correct?Official References from DoD and DFARS DocumentationFinal Verification and ConclusionQUESTION NO: 128

A C3PAO Assessment Plan document captures the names of the interviewees, the facilities that will utilized, along with estimated costs and schedule of the assessment. What part of the assessment plan is this?

A. Identify resources and schedule.

B. Select Assessment Team members.

C. Identify and manage assessment risks.

D. Select and develop the evidence collection approach.

Answer: A

ACertified Third-Party Assessor Organization (C3PAO)is responsible for conductingCMMC Level 2 Assessments. Before the assessment begins, the C3PAO must develop anAssessment Plan, which includes several key elements.

The part of the plan that captures:

#Names of interviewees

#Facilities to be utilized

#Estimated costs

#Assessment schedule

falls under the"Identify Resources and Schedule"section of the plan.

Step-by-Step Breakdown:#1. Identify Resources and Schedule

This section of theCMMC Assessment Planoutlines:

Thepersonnelinvolved (e.g., interviewees, assessors).

Thelocationswhere the assessment will take place.

Thetimeline and scheduling details.

Theestimated costsassociated with the assessment.

This ensures that all necessaryresourcesare allocated and that the assessment proceeds as planned.

#2. Why the Other Answer Choices Are Incorrect:

(B) Select Assessment Team Members#

This section focuses onchoosing the assessorswho will conduct the evaluation, not listing interviewees and facilities.

(C) Identify and Manage Assessment Risks#

This part of the plandocuments risks(e.g., scheduling conflicts, data access issues), but it doesnot outline names, facilities, or costs.

(D) Select and Develop the Evidence Collection Approach#

This step defineshowevidence will be gathered (e.g., document reviews, interviews, system testing) but doesnot focus on logistics.

Final Validation from CMMC Documentation:TheCMMC Assessment Process Guidestates thatresource identification and schedulingare essential for organizing the assessment. Since this sectioncaptures interviewees, facilities, costs, and the schedule, the correct answer is:

#A. Identify resources and schedule.

Question #:46 - [CMMC Assessment Process (CAP)]

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

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 AssessmentDuring aCMMC Level 2 Assessment, theAssessment Teamfollows a structured methodology toverify evidenceand determine whether theOrganization 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

TheAssessment Teamcompares the evidence provided by the OSC against theCMMC practice requirements.

If evidence ismissing, insufficient, or inconsistent, assessors mustdocument the gapand 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

Assessorsreview collected documentation, system configurations, policies, and interview responses.

They verify that the evidencematches the expected implementationof a practice.

If gaps exist, they arerecordedfor 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, theprimary intentof the "Verify Evidence and Record Gaps" step is toidentify deficiencies, not just mapping responses.

(B) Conduct interviews to test process implementation knowledge.#

Incorrect:Interviews are a method used during evidence collection, but they arenot the primary focusof the verification and gap analysis step.

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

Incorrect:The assessment teamreviews multiple sources of evidencefor each practice, and some practices require multiple assessment objects. The goal isnot a strict one-to-one mappingbut rathera holistic validation of compliance.

Final Validation from CMMC Documentation:TheCMMC Assessment Process Guidestates that"Verify Evidence and Record Gaps"is the step where assessorscompare expected evidence against what has been provided and document discrepancies. This ensurestransparent 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 #:47 - [CMMC Assessment Process (CAP)]

A Lead Assessor is performing a CMMC readiness review. The Lead Assessor has already recorded the assessment risk status and the overall assessment feasibility. At MINIMUM, what remaining readiness review criteria should be verified?

A. Determine the practice pass/fail results.

B. Determine the preliminary recommended findings.

C. Determine the initial model practice ratings and record them.

D. Determine the logistics. Assessment Team, and the evidence readiness.

Answer: D

Explanation

Understanding the CMMC Readiness Review ProcessALead Assessorconducting aCMMC Readiness Reviewevaluates whether anOrganization Seeking Certification (OSC)is prepared for a formal assessment.

After recording theassessment risk statusandoverall assessment feasibility, theminimum remaining criteriato be verified include:

Logistics Planning– Ensuring that the assessment timeline, locations, and necessary resources are in place.

Assessment Team Preparation– Confirming that assessors and required personnel are available and briefed.

Evidence Readiness– Ensuring the OSC has gathered all required artifacts and documentation for review.

Breakdown of Answer ChoicesOption

Description

Correct?

A. Determine the practice pass/fail results.

Happensduringthe formal assessment, not the readiness review.

#Incorrect

B. Determine the preliminary recommended findings.

Findings are only madeafterthe full assessment.

#Incorrect

C. Determine the initial model practice ratings and record them.

Ratings are assigned during theassessment, not readiness review.

#Incorrect

D. Determine the logistics, Assessment Team, and the evidence readiness.

#Essential readiness criteria that must be confirmedbeforeassessment starts.

#Correct

TheCMMC Assessment Process Guide (CAP)states that readiness review ensureslogistics, assessment team availability, and evidence readinessare verified.

Official Reference from CMMC 2.0 DocumentationFinal Verification and ConclusionThe correct answer isD. Determine the logistics, Assessment Team, and the evidence readiness.This aligns withCMMC readiness review requirements.

Question #:48 - [CMMC Assessment Process (CAP)]

An assessor is collecting affirmations. So far, the assessor has collected interviews, demonstrations, emails, messaging, and presentations. Are these appropriate approaches to collecting affirmations?

A. No, emails are not appropriate affirmations.

B. No, messaging is not an appropriate affirmation.

C. Yes, the affirmations collected by the assessor are all appropriate.

D. Yes, the affirmations collected by the assessor are all appropriate, as are screenshots.

Answer: C

Explanation

Understanding Affirmations in a CMMC AssessmentAffirmations are a type ofevidencecollected during aCMMC assessmentto confirm compliance with required practices. Affirmations are typically collected from:

#Interviews– Conversations with personnel implementing security practices.

#Demonstrations– Observing the practice in action.

#Emails and Messaging– Written communications confirming compliance efforts.

#Presentations– Documents or briefings explaining security implementations.

#Screenshots–Visual evidenceof system configurations and security measures.

TheCMMC Assessment Process (CAP) Guidestates that assessors may collectaffirmations via various communication methods, including emails, messaging, and presentations.

Screenshotsare an additional valid form ofobjective evidenceto confirm compliance.

Options A and B are incorrectbecause emails and messaging are explicitlyallowedforms of affirmation.

Option C is incompletebecause it does not mention screenshots, which are also considered valid evidence.

Why "Yes, the affirmations collected by the assessor are all appropriate, as are screenshots" is Correct? Breakdown of Answer ChoicesOption

Description

Correct?

A. No, emails are not appropriate affirmations.

#Incorrect–Emailsarea valid affirmation method.

B. No, messaging is not an appropriate affirmation.

#Incorrect–Messagingisallowed for collecting affirmations.

C. Yes, the affirmations collected by the assessor are all appropriate.

#Incorrect–Screenshots should also be considered valid evidence.

D. Yes, the affirmations collected by the assessor are all appropriate, as are screenshots.

#Correct – Screenshots are also a valid form of affirmation.

CMMC Assessment Process Guide (CAP)– Defines allowable evidence collection methods, including affirmations through written communication.

Official References from CMMC 2.0 DocumentationFinal Verification and ConclusionThe correct answer isD. Yes, the affirmations collected by the assessor are all appropriate, as are screenshots.This aligns withCMMC 2.0 assessment proceduresfor collecting affirmations.

Question #:49 - [CMMC Model Overview]

While conducting a CMMC Level 2 Assessment, the Lead Assessor determines that the OSC has badge readers, pin code pads, and keys for various access points as well as documentation to demonstrate meeting the practice. Which CMMC practice has the OSC MET?

A. PE.L1-3.10.5: Control and manage physical access devices

B. MP.L2-3.8.5: Mark media with necessary CUI markings and distribution limitations

C. SI.L2-3.14.3: Monitor system security alerts and advisories and take action in response

D. PS.L2-3.9.2: Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers

Answer: A

Explanation

The presence of badge readers, PIN code pads, and keys directly corresponds to controlling and managing physical access devices, which maps to PE.L1-3.10.5 under the Physical Protection (PE) domain. This practice ensures that only authorized individuals have access to physical areas containing information systems.

The other options address unrelated requirements:

- MP.L2-3.8.5 addresses marking CUI media,

- SI.L2-3.14.3 addresses monitoring security alerts,
- PS.L2-3.9.2 addresses protections during personnel changes.

Reference Documents:

- CMMC Model v2.0, Level 1–3 Practices
- NIST SP 800-171 Rev. 2, Control PE-3

Question #:50 - [CMMC Ecosystem]

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?

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 conductingCMMC Level 2 assessments.

After completing theassessment, theC3PAO generates the Final Recommended Assessment Results, which include key documentation reviewed by theCMMC Quality Assurance Professional (CQAP)for quality control.

Reference:

CMMC Assessment Process (CAP) Guide

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

Before finalizing the assessment results, theC3PAO must include documentation for CQAP reviewto maintain compliance.

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

TheAssessment Planis developedbeforethe assessment begins, not during the final recommended results phase.

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

Daily Checkpointsare internal tracking tools usedduringassessments, but they are not mandatory for final results.

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

While acontract is requiredfor the assessment, it isnot 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 #:51 - [CMMC Ecosystem]

A Level 2 Assessment was conducted for an OSC, and the results are ready to be submitted. Prior to uploading the assessment results, what step MUST the C3PAO complete?

A. Pay an assessment submission fee.

B. Complete an internal review of the results.

C. Notify the CMMC-AB that submission is forthcoming.

D. Coordinate a final briefing between the Lead Assessor and the OSC.

Answer: B

Explanation

ACMMC Level 2 Assessmentis conducted by aC3PAO (Certified Third-Party Assessment Organization)to determine whether theOrganization Seeking Certification (OSC)meets all required110 NIST SP 800-171 controls.

Before submitting the results, theC3PAO must complete a final briefing between the Lead Assessor and the OSCto review findings and clarify any concerns.

A. Pay an assessment submission fee#Incorrect

There is no mandatory submission fee for assessment results.Fees apply to the assessment process, not submission.

B. Complete an internal review of the results#Incorrect

While internal reviews are encouraged, they arenot a required step before submissionin CMMC assessment procedures.

C. Notify the CMMC-AB that submission is forthcoming#Incorrect

TheC3PAO submits results to the CMMC-AB through the CMMC eMASS system, but prior notification isnot a required procedural step.

D. Coordinate a final briefing between the Lead Assessor and the OSC#Correct

According toCMMC Assessment Process (CAP) guidelines, theLead Assessor must conduct a final briefing with the OSCbefore submitting the results.

This briefing ensures transparency, provides OSC with insight into the findings, and allows for final clarifications.

CMMC Assessment Process (CAP) v1.0

Requires afinal briefing between the Lead Assessor and the OSC before submitting assessment results.

CMMC-AB and C3PAO Process Requirements

TheLead Assessor must communicate final findings with the OSC before submission to CMMC-AB.

Analysis of the Given Options:Official References Supporting the Correct Answer:Conclusion:The correct answer is:

#D. Coordinate a final briefing between the Lead Assessor and the OSC.

Question #:52 - [CMMC Ecosystem]

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?

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 theminimum evidence requirementsneeded by a CMMCAssessment Teamto score a practice asMETduring aLevel 2 Assessment.

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

#Step 1: Refer to the CMMC Assessment Process (CAP) Guide v1.0CAP 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 meansat least two typesof 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 METThe CAP explicitly states:

“A practice can only be scored MET when a minimum oftwo types of evidencefrom the E-I-T (Examine, Interview, Test) triad are successfully collected and evaluated.”

Theevidence 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 isimplemented, documented, and understoodby personnel — a core principle in assessing effective cybersecurity implementation.

#Why the Other Options Are IncorrectA. All three types of evidence are documented for every control#Incorrect:While collecting all three types (E-I-T) strengthens the assessment, theminimum requirementis onlytwo. Collecting all three isnot requiredfor a practice to be scoredMET.

B. Examine and accept evidence from one of the three evidence types#Incorrect:This fails to meet theminimum two-evidence-type requirementset 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 twotypes— not two instances of the same type.

#Why D is CorrectD. 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 theCAP’s requirement for collecting two different types of objective evidenceto determine a practice is MET.

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

Question #:53 - [CMMC Assessment Process (CAP)]

Which NIST SP defines the Assessment Procedure leveraged by the CMMC?

A. NIST SP 800-53

B. NISTSP800-53a

C. NIST SP 800-171

D. NISTSP800-171a

Answer: D

Explanation

Which NIST SP Defines the Assessment Procedures for CMMC?CMMC Level 2 isdirectly based on NIST SP 800-171, and the assessment procedures used in CMMC assessments are derived fromNIST SP 800-171A.

Step-by-Step Breakdown:#1. NIST SP 800-171A Defines Assessment Procedures

NIST SP 800-171Ais titled"Assessing Security Requirements for Controlled Unclassified Information (CUI)".

It providesdetailed assessment objectives and test proceduresfor evaluating compliance withNIST SP 800-171 security requirements, whichCMMC Level 2 is fully aligned with.

CMMC Assessors use 800-171Aas abaseline for assessing the effectiveness of security controls.

#2. Why the Other Answer Choices Are Incorrect:

(A) NIST SP 800-53#

800-53 defines security controlsfor federal information systems, but it doesnot provide assessment procedures specific to CMMC.

(B) NIST SP 800-53A#

800-53A provides assessment procedures for 800-53 controls, butCMMC is based on NIST SP 800-171, not 800-53.

(C) NIST SP 800-171#

800-171 defines security requirements, butit does not provide assessment procedures. Theassessment proceduresare in800-171A.

TheCMMC Assessment Guide (Level 2)explicitly states that assessment procedures are derived fromNIST SP 800-171A.

Final Validation from CMMC Documentation:Thus, the correct answer is:

Question #:54 - [CMMC Ecosystem]

Evidence gathered from an OSC is being reviewed. Based on the assessment and organizational scope, the Lead Assessor requests the Assessment Team to verify that the coverage by domain, practice. Host Unit. Supporting Organization/Unit, and enclaves are comprehensive enough to rate against each practice. Which criteria is the assessor referring to?

A. Adequacy

B. Capability

C. Sufficiency

D. Objectivity

Answer: A

Explanation

Step 1: Understand the Definitions of Evidence Evaluation CriteriaTheCMMC Assessment Process (CAP) introduces two key criteria for evaluating evidence:

Adequacy– Does the evidencealign with the practice?

Sufficiency– Is the evidencecomprehensive enoughin terms ofcoverage across systems, users, and scope?

CAP v1.0 – Section 3.5.4:

“Evidence must be evaluated for bothadequacy(is it the right evidence?) andsufficiency(is there enough of it across all in-scope assets and areas?) to score a practice as MET.”

#Step 2: Applying to the ScenarioIn the question, the Lead Assessor is asking the team toverify that evidence is sufficient across:

Domains

Practices

Host Units

Supporting Organizations

Enclaves

This is adirect reference to sufficiency, which evaluates whether thebreadth and depthof evidence is enough to make an informed judgment that the control is truly implemented across theentire assessed environment.

A. Adequacy# Adequacy refers to therelevanceof the evidence to the specific practice — not itscoverageacross scope.

B. Capability# Not a term used in evidence validation within CMMC CAP documentation.

D. Objectivity# While objectivity is important, it refers to theunbiased nature of assessment activities, not to theextent of evidence coverage.

#Why the Other Options Are Incorrect

When an assessor evaluates whether the evidence is broad enough across all necessary systems, units, and enclaves to score a practice as MET, they are evaluatingsufficiency— one of the two core criteria for evidence validity in a CMMC assessment.

Question #:55 - [CMMC Assessment Process (CAP)]

As part of CMMC 2.0, the change to Level 1 Self-Assessments supports "reduced assessment costs" allows all companies at Level 1 (Foundational) to:

A. to conduct self-assessments.

B. opt out of CMMC Assessments.

C. have assessment costs reimbursed by the DoD.

D. pay no more than $500.00 for their annual assessment.

Answer: A

Explanation

Step 1: Review CMMC 2.0 Reforms (Level 1 – Foundational)As part ofCMMC 2.0, the DoD announced changes toreduce burden and costsfor companies that only handleFederal Contract Information (FCI):

DoD Statement (CMMC 2.0 Overview):

“Level 1 (Foundational) will only require an annual self-assessment, affirming implementation of the 17 FAR 52.204-21 controls.”

#Step 2: Intent of “Reduced Assessment Costs”The move to allowself-assessments at Level 1was explicitly designed toeliminate the costof hiring third-party assessors for organizations that only handle FCI.

Level 1 self-assessments are:

Conductedinternally by the OSC,

Affirmed annuallyby a senior company official,

Submitted via SPRS(Supplier Performance Risk System).

B. Opt out of CMMC Assessments# Incorrect. Organizations must still perform aself-assessmentannually — they cannot opt out entirely.

C. Have assessment costs reimbursed by the DoD# No such reimbursement mechanism exists.

D. Pay no more than $500.00…# No such fixed cost is set or guaranteed in CMMC documentation.

#Why the Other Options Are Incorrect

UnderCMMC 2.0, all companies atLevel 1 (Foundational)are permitted toconduct self-assessmentsannually to demonstrate compliance, supporting the DoD’s goal ofreducing assessment costsfor low-risk contractors.

Question #:56 - [CMMC Model Overview]

According to the Configuration Management (CM) domain, which principle is the basis for defining essential system capabilities?

A. Least privilege

B. Essential concern

C. Least functionality

D. Separation of duties

Answer: C

Explanation

Understanding the Principle of Least Functionality in the CM DomainTheConfiguration Management (CM) domainin CMMC 2.0 focuses on maintaining the security and integrity of an organization’s systems through controlled configurations and restrictions on system capabilities.

The principle ofLeast Functionalityrefers to limiting a system’s features, services, and applications to only those necessary for its intended purpose. This principle reduces the attack surface by minimizing unnecessary components that could be exploited by attackers.

CMMC Practice CM.L2-3.4.6 (Use Least Functionality)explicitly states:"Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities."

Thegoalis to prevent unauthorized or unnecessary applications, services, and ports from running on the system.

Examples of Implementation:

Disabling unnecessary services, such as remote desktop access if not required.

Restricting software installation to approved applications.

Blocking unused network ports and protocols.

A. Least Privilege

This principle (associated with Access Control) ensures that users and processes have only the minimum level of access necessary to perform their jobs.

It is relevant to CMMC PracticeAC.L2-3.1.5 (Least Privilege)but does not define system capabilities.

B. Essential Concern

There is no officially recognized cybersecurity principle called "Essential Concern" in CMMC, NIST, or related frameworks.

D. Separation of Duties

This principle (covered under CMMCAC.L2-3.1.4) ensures that no single individual has unchecked control over critical functions, reducing the risk of fraud or abuse.

While important for security, it does not define essential system capabilities.

CMMC 2.0 Level 2 Assessment Guide – Configuration Management (CM) Domain

CM.L2-3.4.6 mandatesleast functionalityto enhance security by removing unnecessary features.

NIST SP 800-171 (which CMMC is based on) – Requirement 3.4.6

States:"Limit system functionality to only the essential capabilities required for organizational missions or business functions."

NIST SP 800-53 – Control CM-7 (Least Functionality)

Provides detailed recommendations on configuring systems to operate with only necessary features.

Justification for the Correct Answer: Least Functionality (C)Why Other Options Are IncorrectOfficial CMMC and NIST ReferencesConclusionTheprinciple of Least Functionality (C)is the basis for defining essential system capabilities in theConfiguration Management (CM) domainof CMMC 2.0. By applying this principle, organizations reduce security risks by ensuring that only the necessary functions, services, and applications are enabled.

Question #:57 - [Implementation and Scoping]

When are contractors required to achieve a CMMC certificate at the Level specified in the solicitation?

A. At the time of award

B. Upon solicitation submission

C. Thirty days from the award date

D. Before the due date of submission

Answer: A

Explanation

PerDFARS 252.204-7021, contractors must achieve the requiredCMMC certification levelbefore contract awardif the solicitation specifies it.

Key Requirements:#Contractorsmust be certified at the required CMMC levelprior to contract award.

#Thecertification must be conducted by a C3PAO(for Level 2) orthrough self-assessment(for Level 1).

#The certification must bevalid and registered in the Supplier Performance Risk System (SPRS)before award.

A. At the time of award # Correct

DFARS 252.204-7021requires CMMC certification before a contract can be awardedif the solicitation includes CMMC requirements.

B. Upon solicitation submission # Incorrect

Contractorsdo notneed to be CMMC-certified at thetime of bid submission, only by the time of award.

C. Thirty days from the award date # Incorrect

Contractorsmust already be certified before the award is granted. There isno grace period.

D. Before the due date of submission # Incorrect

While compliance planning is important,CMMC certification is only required before contract award, not before bid submission.

Why is the Correct Answer "At the Time of Award" (A)?

DFARS 252.204-7021 (CMMC Requirement Clause)

CMMC certification is required prior to contract awardif specified in the solicitation.

CMMC 2.0 Program Overview

States that certificationis not needed at bid submission but is required before award.

DoD Interim Rule & SPRS Guidance

Contractors must havea valid CMMC certification recorded in SPRSbefore award.

CMMC 2.0 References Supporting This Answer:

Question #:58 - [CMMC Ecosystem]

The director of sales, in a meeting, stated that the sales team received feedback on some emails that were sent, stating that the emails were not marked correctly. Which training should the director of sales refer the sales team to regarding information as to how to mark emails?

A. FBI CUI Introduction to Marking

B. NARA CUI Introduction to Marking

C. C3PAO CUI Introduction to Marking

D. CMMC-AB CUI Introduction to Marking

Answer: B

Explanation

The Controlled Unclassified Information (CUI) Program, established by Executive Order 13556, standardizes the handling and marking of unclassified information that requires safeguarding or dissemination controls across federal agencies and their contractors. The National Archives and Records Administration (NARA) serves as the Executive Agent responsible for implementing the CUI Program.

In the context of the Cybersecurity Maturity Model Certification (CMMC) 2.0, particularly at Level 2, organizations are required to protect CUI by adhering to the security requirements outlined in NIST Special Publication 800-171. This includes proper marking of CUI to ensure that all personnel recognize and handle such information appropriately.

The NARA CUI Introduction to Marking provides comprehensive guidance on the correct procedures for marking documents and communications containing CUI. This resource is essential for training purposes, as it offers detailed instructions and examples to help personnel understand and implement proper CUI markings. By referring the sales team to the NARA CUI Introduction to Marking, the director of sales ensures that the team receives authoritative and standardized training on how to appropriately mark emails and other documents containing CUI, thereby maintaining compliance with federal regulations and CMMC requirements.

Question #:59 - [CMMC Assessment Process (CAP)]

What is a PRIMARY activity that is performed while conducting an assessment?

A. Develop assessment plan.

B. Collect and examine evidence.

C. Verify readiness to conduct assessment.

D. Deliver recommended assessment results.

Answer: B

Explanation

Step 1: Understand the Assessment Phases (CAP v1.0)TheCMMC Assessment Process (CAP)outlines a structured lifecycle for assessments, including:

Plan and Prepare Phase– Develop the assessment plan (before the assessment starts).

Conduct Assessment Phase– Execute the actual assessment activities.

Report Results Phase– Finalize and deliver the assessment outcomes.

CAP v1.0 – Section 3.5 (Conduct Assessment):

“The assessment team collects, examines, and evaluates evidence to determine if practices are MET or NOT MET.”

During the“Conduct Assessment” phase, the main activity is to:

Collect evidence(documentation, interviews, testing),

Validate adequacy and sufficiency,

Score practicesas MET/NOT MET.

#Step 2: Why “Collect and Examine Evidence” Is the Primary ActivityThis is thecore responsibilityof assessorswhile conductingan assessment.

A. Develop assessment plan# This occurs in thePlan and Preparephasebeforeconducting the assessment.

C. Verify readiness to conduct assessment# Readiness verification is part ofpre-assessment activities, not during the assessment itself.

D. Deliver recommended assessment results# This is done during theReport Resultsphase after the assessment has been conducted.

#Why the Other Options Are Incorrect

Theprimary activity performed during the actual executionof a CMMC assessment iscollecting and examining evidenceto determine compliance with practices.

Question #:60 - [CMMC Ecosystem]

An OSC needs to be assessed on RA.L2-3.11.1: Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. What is in scope for a Level 2 assessment of RA.L2-3.11.1?

A. IT systems

B. Enterprise systems

C. CUI Marking processes

D. Processes, people, physical entities, and IT systems in which CUI processed, stored, or transmitted

Answer: D

Explanation

Understanding RA.L2-3.11.1 Risk Assessment Scope in CMMC Level 2TheCMMC Level 2 control RA.L2-3.11.1aligns withNIST SP 800-171, Requirement 3.11.1, which mandates that organizationsperiodically assess risks to operations, assets, and individuals arising from the processing, storage, or transmission of CUI.

What is Required for Compliance?

The organization must performrisk assessments on all assets and entities involved in handling CUI.

Risk assessments mustevaluate potential threats, vulnerabilities, and impacts on CUI security.

The scopemust include people, processes, physical locations, and IT systemsto ensure comprehensive risk management.

Why the Correct Answer is "Processes, people, physical entities, and IT systems in which CUI is processed, stored, or transmitted":

CUIcan be exposed to risk in multiple ways—not just IT systems but also human error, physical security gaps, and process weaknesses.

Risk assessmentsmust evaluate all areas that could impact CUI security, including:

Personnel security risks(e.g., insider threats, phishing attacks).

Process vulnerabilities(e.g., mishandling of CUI, policy weaknesses).

Physical security risks(e.g., unauthorized access to servers, storage rooms).

IT systems(e.g., networks, servers, cloud environments processing CUI).

A. "IT systems"#Too narrow.Risk assessmentmust cover more than just IT systems, includingpeople, physical assets, and processesaffecting CUI.

B. "Enterprise systems"#Too broad.While enterprise systems might be assessed, thefocus is specifically on areas handling CUI, not all enterprise operations.

C. "CUI Marking processes"#Incorrect focus.While marking CUI correctly is important,RA.L2-3.11.1 pertains to risk assessments, not data classification.

References:NIST SP 800-171 Rev. 2 – Requirement 3.11.1(NIST Official Site)

CMMC 2.0 Level 2 Assessment Guide – Risk Assessment Domain(Cyber AB)

#Final Answer: D. Processes, people, physical entities, and IT systems in which CUI is processed, stored, or transmitted.

Question #:61 - [CMMC Model Overview]

Which document is the BEST source for determining the sources of evidence for a given practice?

A. NISTSP 800-53

B. NISTSP 800-53A

C. CMMC Assessment Scope

D. CMMC Assessment Guide

Answer: D

Explanation

TheCMMC Assessment Guideis the best source for determining the sources of evidence for a given practice because it provides specific guidance on how organizations should implement and demonstrate compliance with CMMC practices. Each CMMC level has its own assessment guide (e.g.,CMMC Assessment Guide – Level 1, Level 2), detailing expected evidence and assessment procedures.

CMMC Assessment Guide (Primary Source for Evidence)

TheCMMC Assessment Guideexplicitly outlines the evidence required to verify compliance with each practice.

It provides detailed instructions on assessment objectives, clarifying what assessors should look for when determining compliance.

The guide breaks down each practice intoassessment objectives, helping organizations prepare appropriate documentation and artifacts.

Other Documents and Why They Are Not the Best Choice:

NIST SP 800-53 (Option A)

WhileNIST SP 800-53provides a comprehensive catalog of security and privacy controls, it does not focus on CMMC-specific evidence requirements.

It serves as a foundational cybersecurity framework but does not define the specific artifacts required for CMMC assessment.

NIST SP 800-53A (Option B)

NIST SP 800-53Aprovides guidance on assessing security controls but is not tailored to the CMMC framework.

It includes general control assessment procedures, but theCMMC Assessment Guideis more precise in defining the evidence needed for CMMC compliance.

CMMC Assessment Scope (Option C)

TheCMMC Assessment Scopedocument outlines which systems, assets, and processes are subject to assessment.

While important for defining boundaries, it does not provide details on specific evidence requirements for each practice.

CMMC Assessment Guide (Level 2) – Section on "Assessment Objectives"

This document details how evidence is collected and evaluated for each CMMC practice.

Example: ForAC.L2-3.1.1 (Access Control – Limit System Access), the guide specifies that assessors should verify documented policies, system configurations, and audit logs.

CMMC Model Overview (Official DoD Documents)

Emphasizes thatCMMC Assessment Guidesare the official reference for determining sources of evidence.

Detailed Justification:References from Official CMMC Documents:Conclusion:TheCMMC Assessment Guideis the most authoritative source for determining the required evidence for a given practice in CMMC assessments. It provides detailed breakdowns of assessment objectives, required artifacts, and verification steps necessary for compliance.

Question #:62 - [CMMC Assessment Process (CAP)]

Which assessment method compares actual-specified conditions with expected behavior?

A. Test

B. Examine

C. Compile

D. Interview

Answer: A

Explanation

Understanding CMMC Assessment MethodsTheCybersecurity Maturity Model Certification (CMMC) 2.0 follows theNIST SP 800-171A assessment methodology, which includesthree primary assessment methods:

Examine– Reviewing policies, procedures, system configurations, and documentation.

Interview– Engaging with personnel to validate their understanding and execution of security practices.

Test– Conducting actual technical or operational tests to determine whether security controls function as expected.

"Test" is the method that compares actual-specified conditions with expected behavior.

It involvesexecuting procedures, configurations, or automated toolsto see if thesystem behaves as required.

For example, if a policy states that multi-factor authentication (MFA) must be enforced, a test would involveattempting to log in without MFAto confirm whether access is blocked as expected.

TheNIST SP 800-171A Guide (Assessment Procedures for CUI)defines testing as an assessment method that:

Actively verifies a security control is functioning

Simulates real-world attack scenarios

Checks compliance through system actions rather than documentation

B. Examine (Incorrect)

Examining only involvesreviewing policies, procedures, or configurationsbut does not actively test system behavior.

C. Compile (Incorrect)

"Compile" is not an assessment method in CMMC 2.0 or NIST SP 800-171A.

D. Interview (Incorrect)

Interviews are used to gather insights from personnel, but they do not compare actual conditions with expected behavior.

The correct answer isA. Testbecause itactively verifies system performance against expected security conditions.

References:

NIST SP 800-171A, "Assessing Security Requirements for CUI"

CMMC 2.0 Assessment Process (CAP) Guide

DoD CMMC Scoping and Assessment Guidelines

Question #:63 - [Implementation and Scoping]

CMMC scoping covers the CUI environment encompassing the systems, applications, and services that focus on where CUI is:

A. received and transferred.

B. stored, processed, and transmitted.

C. entered, edited, manipulated, printed, and viewed.

D. located on electronic media, on system component memory, and on paper.

Answer: B

Explanation

TheCMMC Scoping Guide for Level 2outlines thatCUI assetsinclude systems, applications, and services thatstore, process, or transmitControlled Unclassified Information (CUI). These are the three core functions that defineCUI handlingwithin anOrganization Seeking Certification (OSC).

Step-by-Step Breakdown:#1. CUI Assets Defined in CMMC

Stored:CUI is saved on hard drives, cloud storage, or databases.

Processed:CUI is actively used, modified, or analyzed by applications and users.

Transmitted:CUI is sent between systems via email, file transfers, or network communication.

#2. Why the Other Answer Choices Are Incorrect:

(A) Received and transferred#

Whilereceiving and transferring CUIis part of handling CUI, it does not fully cover all CUI asset responsibilities.

(C) Entered, edited, manipulated, printed, and viewed#

These arespecific actionswithinprocessingbut do not coverstorage or transmission, which are also required for CMMC scoping.

(D) Located on electronic media, on system component memory, and on paper#

While CUI can exist inelectronic and physical forms, CMMC scoping focuses onhow CUI is actively managed (stored, processed, transmitted)rather than where it physically resides.

TheCMMC Level 2 Scoping Guideconfirms thatCUI Assets are categorized based on their role in storing, processing, or transmitting CUI.

NIST SP 800-171also defines these three functions as key components of CUI protection.

Final Validation from CMMC Documentation:

Question #:64 - [CMMC Ecosystem]

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

A. Verify the readiness to conduct the assessment.

B. Perform certification assessment readiness review.

C. Update the assessment plan and schedule as needed

D. Obtain and record commitment to the assessment plan.

Answer: A

Explanation

Last Step in Developing an Assessment Plan for an OSCDeveloping anassessment planinvolves:

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?#Theassessment cannot proceed unless the OSC agrees to the finalized plan.

#This ensuresOSC leadership understands the scope, timeline, and responsibilities.

#TheC3PAO must document this commitmentto formalize the agreement.

A. Verify the readiness to conduct the assessment # Incorrect

Readiness verification happens earlierin the planning process, not as the last step.

B. Perform certification assessment readiness review # Incorrect

Areadiness 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 theOSC must confirm agreement to the assessment plan before execution.

CMMC-AB Guidelines for C3PAOs

Specifies thatfinalizing the assessment plan requires documented commitment from the OSC.

CMMC Assessment Guide

Outlines thatassessments cannot begin without formal approval of the plan.

CMMC 2.0 References Supporting This Answer:

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

Question #:65 - [CMMC Ecosystem]

During a Level 2 Assessment, the OSC has provided an inventory list of all hardware. The list includes servers, workstations, and network devices. Why should this evidence be sufficient for making a scoring determination for AC.L2-3.1.19: Encrypt CUI on mobile devices and mobile computing platforms?

A. The inventory list does not specify mobile devices.

B. The interviewee attested to encrypting all data at rest.

C. The inventory list does not include Bring Your Own Devices.

D. The DoD has accepted an alternative safeguarding measure for mobile devices.

Answer: A

Explanation

In the context of a Cybersecurity Maturity Model Certification (CMMC) Level 2 Assessment, specific practices must be evaluated to ensure compliance with established security requirements. One such practice is AC.L2-3.1.19, which mandates the encryption of Controlled Unclassified Information (CUI) on mobile devices and mobile computing platforms.

Step-by-Step Explanation:

Requirement Overview:

Practice AC.L2-3.1.19 requires organizations to "Encrypt CUI on mobile devices and mobile computing platforms." This ensures that any CUI accessed, stored, or transmitted via mobile devices is protected through encryption, mitigating risks associated with data breaches or unauthorized access.

Assessment of Provided Evidence:

During the assessment, the Organization Seeking Certification (OSC) provided an inventory list encompassing servers, workstations, and network devices. Notably, this list lacks any mention of mobile devices or mobile computing platforms.

Implications of the Omission:

The absence of mobile devices in the inventory suggests that the OSC may not have accounted for all assets that process, store, or transmit CUI. Without a comprehensive inventory that includes mobile devices, it's challenging to verify whether the OSC has implemented the necessary encryption measures for CUI on these platforms.

Assessment Determination:

Given the incomplete inventory, the evidence is insufficient to make a definitive scoring determination for practice AC.L2-3.1.19. The OSC must provide a detailed inventory that encompasses all relevant devices, including mobile devices and computing platforms, to demonstrate compliance with the encryption requirements for CUI.

References:

CMMC Model Overview Version 2.13, which outlines the requirements for practice AC.L2-3.1.19.

Ensuring a complete and accurate inventory is a critical step in the assessment process, as it forms the basis for evaluating the implementation of security controls across all relevant assets within the organization.

Question #:66 - [CMMC Model Overview]

The IT manager is scoping the company's CMMC Level 1 Self-Assessment. The manager considers which servers, laptops. databases, and applications are used to store, process, or transmit FCI. Which asset type is being considered by the IT manager?

A. ESP

B. People

C. Facilities

D. Technology

Answer: D

Explanation

Understanding Asset Types in CMMC 2.0In CMMC 2.0, assets are categorized based on their role in handlingFederal Contract Information (FCI)orControlled Unclassified Information (CUI). TheCybersecurity Maturity Model Certification (CMMC) Scoping GuidanceforLevel 1andLevel 2provides asset definitions to help organizations identify what needs protection.

According toCMMC Scoping Guidance, there are five primary asset types:

Security Protection Assets (ESP - External Service Providers & Security Systems)

People (Personnel who interact with FCI/CUI)

Facilities (Physical locations housing FCI/CUI)

Technology (Hardware, software, and networks that store, process, or transmit FCI/CUI)

CUI Assets (For Level 2 assessments, assets specifically storing CUI)

Why "Technology" Is the Correct AnswerThe IT manager is evaluatingservers, laptops, databases, and applications—all of which aretechnology assetsused to store, process, or transmit FCI.

According toCMMC Scoping Guidance,Technology assetsinclude:

#Endpoints(Laptops, Workstations, Mobile Devices)

#Servers(On-premise or cloud-based)

#Networking Devices(Routers, Firewalls, Switches)

#Applications(Software, Cloud-based tools)

#Databases(Storage of FCI or CUI)

Since the IT manager is focusing on these components, the correct asset category isTechnology (Option D).

A. ESP (Security Protection Assets)#Incorrect. ESPs refer tosecurity-related assets(e.g., firewalls, monitoring tools, managed security services) thathelp protectFCI/CUI but do notstore, process, or transmitit directly.

B. People#Incorrect. While employees play a role in handling FCI, the question focuses onhardware and software—which falls underTechnology, not People.

C. Facilities#Incorrect. Facilities refer tophysical buildingsor secured areas where FCI/CUI is stored or processed. The question explicitly mentionsservers, laptops, and applications, which arenot physical facilities.

Why the Other Answers Are Incorrect

CMMC Level 1 Scoping Guide (CMMC-AB)– Defines asset categories, including Technology.

CMMC 2.0 Scoping Guidance for Assessors– Provides clarification on FCI assets.

CMMC Official ReferencesThus,option D (Technology) is the most correct choiceas per official CMMC 2.0 guidance.

Question #:67 - [Roles and Responsibilities]

Who is responsible for ensuring that subcontractors have a valid CMMC Certification?

A. CMMC-AB

B. OUSDA&S

C. DoD agency or client

D. Contractor organization

Answer: D

Explanation

The prime contractor (contractor organization)is responsible for ensuring thatits subcontractorshave the requiredCMMC certification levelbefore engaging them inDoD contracts that involve FCI or CUI.

This requirement is enforced throughflow-down clausesinDFARS 252.204-7021, which mandates that subcontractors handlingCUImeet the necessaryCMMC Level 2 or Level 3 requirements.

Reference:

DFARS 252.204-7021(CMMC Compliance)

CMMC 2.0 Program Documentation

Step 2: Why Other Answer Choices Are IncorrectA. CMMC-AB (Incorrect):

TheCyber AB (formerly CMMC-AB)is responsible foraccrediting C3PAOs and managing the assessment process, but it does not enforce subcontractor compliance.

B. OUSDA&S (Incorrect):

TheOffice of the Under Secretary of Defense for Acquisition & Sustainment (OUSD A&S)develops and overseesCMMC policy, but it does not monitor or enforce individual subcontractor compliance.

C. DoD agency or client (Incorrect):

While theDoD sets CMMC requirements, it relies onprime contractors to ensure compliance among their subcontractorsthrough contract flow-down requirements.

Final Confirmation of Correct Answer:Prime contractors must ensure their subcontractors have the required CMMC certification level to handle FCI or CUI.

Thus, the correct answer is:D. Contractor organization

Question #:68 - [CMMC Assessment Process (CAP)]

What type of criteria is used to answer the question "Does the Assessment Team have the right evidence?"

A. Adequacy criteria

B. Objectivity criteria

C. Sufficiency criteria

D. Subjectivity criteria

Answer: A

Explanation

In the context of CMMC 2.0 assessments, thesufficiency criteriaare used to determine whether the assessment team has gathered enough evidence to support their conclusions about compliance with a given requirement.

Definition of Sufficiency Criteria:

Sufficiency refers to thequantityandcompletenessof the evidence collected during an assessment.

This ensures that the evidence collected isenough to support an objective and valid determinationof compliance.

Why Sufficiency Matters in CMMC 2.0:

Assessors must ensure that the amount of evidence collected isadequate to substantiate findingswithout doubt or gaps.

This prevents situations where an organization might claim compliance but lacks thenecessary documentation, technical evidence, or procedural validationto prove it.

Official CMMC 2.0 References:

TheCMMC Assessment Process (CAP) Guidedefines sufficiency as a key factor in validating assessment findings.

According toCMMC 2.0 Level 2 Scoping Guidance, assessors must apply sufficiency criteria when reviewingartifacts, documentation, interviews, and system configurations.

TheDoD CMMC Assessment Guide(aligned with NIST SP 800-171A) emphasizes that compliance decisions must besupported by a sufficient amount of verifiable evidence.

Comparison with Other Criteria:

Adequacy Criteria# Focuses onqualityof the evidence, not the quantity.

Objectivity Criteria# Ensures evidence isunbiased and impartial, not necessarily complete.

Subjectivity Criteria# Not applicable in CMMC since assessments must beobjective and based on factual evidence.

Step-by-Step Breakdown:Conclusion:To verify compliance in CMMC 2.0 assessments, the assessment team must ensuresufficientevidence is available to support a determination. This makes"Sufficiency Criteria" (Option C)the correct answer.

Question #:69 - [CMMC Assessment Process (CAP)]

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?

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 ofConfidentialityunder theCMMC 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) References:

TheCMMC Code of Professional Conductstates that assessors and organizations must handle all collected information with discretion andensure 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 toexercise due carein 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.

TheCMMC Code of Professional ConductandNIST SP 800-171control requirements confirm thatConfidentialityis 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 isB. Confidentiality.

Question #:70 - [Implementation and Scoping]

In CMMC High-Level scoping, which definition BEST describes an HQ organization?

A. The entity that carries out the tasks under a contract

B. The unit to which a CMMC Level is applied for each contract

C. The teams, services, and technologies that provide support to a Host Unit

D. The entity legally responsible for the delivery of products or services under a contract

Answer: D

Explanation

In CMMC scoping terminology, an HQ Organization is the entity legally responsible for contract performance and delivery of products or services.

Supporting Extracts from Official Content:

- CMMC Scoping Guide: “HQ Organization is the legal entity responsible for the performance and delivery of contract requirements.”

Why Option D is Correct:

- The HQ Org is legally accountable, while Host Units (option A/B) are subordinate entities.

- Option C refers to shared services, not the HQ.

References (Official CMMC v2.0 Content):

- CMMC Scoping Guide, High-Level Scoping Definitions.

===========

Question #:71 - [CMMC Model Overview]

What are CUI protection responsibilities?

A. Shielding

B. Governing

C. Correcting

D. Safeguarding

Answer: D

Explanation

Understanding CUI Protection ResponsibilitiesControlled Unclassified Information (CUI)is sensitive butnot classifiedinformation that requires protection underDoD Instruction 5200.48andDFARS 252.204-7012.

Theprimary responsibilityfor handling CUIis safeguardingit against unauthorized access, disclosure, or modification.

TheCUI Program (as per NARA and DoD)mandatessafeguarding measuresto protectCUI in both digital and physical forms.

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

DFARS 252.204-7012requires DoD contractors to implementcybersecurity safeguardsto protect CUI.

A. Shielding (Incorrect)–Shieldingis 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 tosafeguardCUI proactively.

The correct answer isD. Safeguarding, asCUI protection focuses on implementing cybersecurity safeguards.

References:

DoD Instruction 5200.48 (CUI Program)

DFARS 252.204-7012

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

Question #:72 - [CMMC Ecosystem]

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

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

nderstanding Objectivity in CMMC-AB ActivitiesObjectivityin CMMC-AB activities refers to therequirement that assessors and C3PAOs remain impartial, unbiased, and free from conflicts of interestwhile conducting assessments and providing CMMC-related services.

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

#Unbiased reporting—Findings must bebased solely on evidence, with no external influence.

#Avoiding even the appearance of a conflict—If there isany perception of bias, it must be addressed.

A. Ensuring full disclosure # Incorrect

Full disclosure is importantbut doesnot define objectivity. Objectivity meansremaining neutral and free from conflicts.

B. Reporting results of CMMC services completely # Incorrect

Whileaccurate 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 thatassessments are credible and trustworthy.

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

Integrity is important, butobjectivity 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

Requiresassessors and C3PAOs to avoid conflicts of interestand maintainimpartiality.

CMMC Assessment Process (CAP) Document

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

ISO/IEC 17020 Requirements for Inspection Bodies

Definesobjectivity as avoiding conflicts of interest in the assessment process.

CMMC 2.0 References Supporting This Answer:

Question #:73 - [CMMC Ecosystem]

While conducting a CMMC Assessment, a Lead Assessor is given documentation attesting to Level 1 identification and authentication practices by the OSC. The Lead Assessor asks the CCP to review the documentation to determine if identification and authentication controls are met. Which documentation BEST satisfies the requirements of IA.L1-3.5.1: Identify system users. processes acting on behalf of users, and devices?

A. Procedures for implementing access control lists

B. List of unauthorized users that identifies their identities and roles

C. User names associated with system accounts assigned to those individuals

D. Physical access policy that states. "All non-employees must wear a special visitor pass or be escorted."

Answer: C

Explanation

Understanding IA.L1-3.5.1 (Identification and Authentication Requirements)TheCMMC 2.0 Level 1practiceIA.L1-3.5.1aligns withNIST SP 800-171, Requirement 3.5.1, which mandates that organizationsidentify system users, processes acting on behalf of users, and devicesto ensure proper access control.

To comply with this requirement, anOrganization Seeking Certification (OSC)must maintain documentation that demonstrates:

A unique identifier (username) for each system user

Mapping of system accounts to specific individuals

Identification of devices and automated processes that access systems

This documentation directly satisfies IA.L1-3.5.1because it showshow system users are uniquely identified and linked to specific accountswithin the environment.

Alist of users and their assigned accountsconfirms that the organization has a structured method oftracking access and authentication.

It allows auditors to verify thateach user has a distinct identityand that access control mechanisms are properly applied.

A. Procedures for implementing access control lists (Incorrect)

While access control lists (ACLs) are relevant for authorization, they do notidentify users or devicesspecifically, making them insufficient as primary evidence for IA.L1-3.5.1.

B. List of unauthorized users that identifies their identities and roles (Incorrect)

Identifying unauthorized users does not fulfill the requirement of trackingauthorizedusers, devices, and processes.

D. Physical access policy stating "All non-employees must wear a special visitor pass or be escorted" (Incorrect)

This pertains tophysical security, not system-baseduser identification and authentication.

The correct answer isC. User names associated with system accounts assigned to those individuals, as thisdirectly satisfies the identification requirement of IA.L1-3.5.1.

References:

CMMC 2.0 Level 1 Practice IA.L1-3.5.1

NIST SP 800-171, Requirement 3.5.1

Question #:74 - [CMMC Assessment Process (CAP)]

A company is working with a CCP from a contracted CMMC consulting company. The CCP is asked where the Host Unit is required to document FCI and CUI for a CMMC Assessment. How should the CCP respond?

A. "In the SSP. within the asset inventory, and in the network diagranY'

B. "Within the hardware inventory, data (low diagram, and in the network diagram"

C. "Within the asset inventory, in the proposal response, and in the network diagram"

D. "In the network diagram, in the SSP. within the base inventory, and in the proposal response'"

Answer: A

Explanation

ACertified CMMC Professional (CCP)advising anOrganization Seeking Certification (OSC)must ensure thatFederal Contract Information (FCI)andControlled Unclassified Information (CUI)are properly documented within required security documents.

Step-by-Step Breakdown:#1. System Security Plan (SSP)

CMMC Level 2requires anSSPto documenthow CUI is protected, including:

Security controlsimplemented

Asset categorization(CUI Assets, Security Protection Assets, etc.)

Policies and proceduresfor handling CUI

#2. Asset Inventory

Anasset inventorylistsall relevant IT systems, applications, and hardwarethat store, process, or transmitCUI or FCI.

TheCMMC Scoping Guiderequires OSCs to identifyCUI-relevant assetsas part of their compliance.

#3. Network Diagram

Anetwork diagramvisually representshow data flows across systems, showing:

WhereCUI is transmitted and stored

Security boundaries protectingCUI Assets

Connectivity betweenCUI Assets and Security Protection Assets

#4. Why the Other Answer Choices Are Incorrect:

(B) Within the hardware inventory, data flow diagram, and in the network diagram#

While adata flow diagramis useful,hardware inventory alone is insufficientto document CUI.

(C) Within the asset inventory, in the proposal response, and in the network diagram#

Aproposal responseis not a required document for CMMC assessments.

(D) In the network diagram, in the SSP, within the base inventory, and in the proposal response#

Base inventoryis not a specific CMMC documentation requirement.

TheCMMC Assessment Guideconfirms that FCI and CUI must be documented in:

The SSP

The asset inventory

The network diagram

Final Validation from CMMC Documentation:Thus, the correct answer is:

#A. "In the SSP, within the asset inventory, and in the network diagram."

Question #:75 - [CMMC Ecosystem]

Which government agency are DoD contractors required to report breaches of CUI to?

A. FBI

B. NARA

C. DoD Cyber Crime Center

D. Under Secretary of Defense for Intelligence and Security

Answer: C

Explanation

Who Do DoD Contractors Report CUI Breaches To?PerDFARS 252.204-7012, all DoD contractors handlingControlled Unclassified Information (CUI)must report cyber incidents to theDoD Cyber Crime Center (DC3).

Key Reporting Requirements#Cyber incidents involving CUI must be reported toDC3 within 72 hours.

#Reports must be submitted via theDoD's Cyber Incident Reporting Portal.

#Contractors mustpreserve forensic evidencefor potential investigation.

The FBI (Option A) handles criminal investigations, but DoD contractorsmust report cyber incidents to DC3.

NARA (Option B) oversees the CUI Registry, butis not responsible for breach reporting.

The Under Secretary of Defense for Intelligence and Security (Option D) is responsible for intelligence operations, not incident reporting.

Why "DoD Cyber Crime Center" is Correct?Breakdown of Answer ChoicesOption

Description

Correct?

A. FBI

#Incorrect–The FBI handlescriminal cases, not CUI breach reporting.

B. NARA

#Incorrect–NARA manages theCUI Registry, butdoes not handle breaches.

C. DoD Cyber Crime Center

#Correct – Per DFARS 252.204-7012, cyber incidents involving CUI must be reported to DC3.

D. Under Secretary of Defense for Intelligence and Security

#Incorrect–This office doesnothandle cyber incident reports.

DFARS 252.204-7012– Requires DoD contractors to report CUI-related cyber incidents toDC3.

DoD Cyber Crime Center (DC3) Website– The official platform forcyber incident reporting.

Official References from CMMC 2.0 and DFARS DocumentationFinal Verification and ConclusionThe correct answer isC. DoD Cyber Crime Center, as perDFARS 252.204-7012, which mandates that all DoD contractors reportCUI breaches to DC3 within 72 hours.

Question #:76 - [CMMC Ecosystem]

A CMMC Assessment Team arrives at an OSC to begin a CMMC Level 2 Assessment. The team checks in at the front desk and lets the receptionist know that they are here to conduct the assessment. The receptionist is aware that the team is arriving today and points down a hallway where the conference room is. The receptionist tells the Lead Assessor to wait in the conference room. as someone will be there shortly. The receptionist fails to check for credentials and fails to escort the team. The receptionist's actions are in direct violation of which CMMC practice?

A. PE.L1-3.10.3: Escort visitors and monitor visitor activity

B. PE.L1-3.10.5: Control and manage physical access devices

C. PS.L2-3.9.1; Screen individuals prior to authorizing access to organizational systems containing CUI

D. PS.L2-3 9.2: Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers

Answer: A

Explanation

ThePhysical Protection (PE) domaininCMMC 2.0 Level 1includes the requirementPE.L1-3.10.3, which mandates that organizationsescort visitors and monitor their activity.

TheCMMC Assessment Teamarrives at the OSC.

Thereceptionist acknowledges their arrival but does not verify credentials or escort themto the appropriate location.

Failing to verify visitor identity and failing to escort them is a violation of PE.L1-3.10.3.

A. PE.L1-3.10.3: Escort visitors and monitor visitor activity##Correct

This requirement ensures that visitorsdo not have unsupervised access to sensitive areas.

The receptionistshould have checked credentials and escorted the assessment team.

B. PE.L1-3.10.5: Control and manage physical access devices##Incorrect

This requirement refers to managingkeys, access badges, and security devices, which isnot the issue in this scenario.

C. PS.L2-3.9.1: Screen individuals prior to authorizing access to organizational systems containing CUI##Incorrect

This control applies to personnel screeningsbefore granting access to CUI systems, not physical visitor access.

D. PS.L2-3.9.2: Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers##Incorrect

This requirement deals withoffboarding employees and ensuring they no longer have system access. It isnot relevant to visitor escorting.

CMMC 2.0 Level 1 - PE.L1-3.10.3 (Physical Protection)

Requires organizations toescort visitors and monitor visitor activityat facilities containingFCI or CUI.

NIST SP 800-171 Rev. 2, Control 3.10.3

States thatvisitors must be escorted and monitored at all timesto prevent unauthorized access.

Breaking Down the Scenario:Analysis of the Given Options:Official References Supporting the Correct Answer:Conclusion:Since the receptionist failed to verify credentials and escort the visitors, this violatesPE. L1-3.10.3.

#Correct Answer: A. PE.L1-3.10.3: Escort visitors and monitor visitor activity

Question #:77 - [CMMC Assessment Process (CAP)]

The evidence needed for each practice and/or process is weighed for:

A. Adequacy and sufficiency

B. Adequacy and thoroughness

C. Sufficiency and thoroughness

D. Sufficiency and appropriateness

Answer: A

Explanation

The CAP makes clear that evidence collected during the assessment is evaluated for both adequacy (does the evidence align with the requirement) and sufficiency (is there enough evidence to make a confident determination).

Supporting Extracts from Official Content:

- CAP v2.0, Evidence Collection Guidance: “Evidence must be evaluated for adequacy… and for sufficiency, to ensure enough information is available to support the assessor’s determination.”

Why Option A is Correct:

- Evidence is assessed based on two qualities only: adequacy and sufficiency.
- “Thoroughness” and “appropriateness” are not official CAP terms for evidence evaluation.

References (Official CMMC v2.0 Content):

- CMMC Assessment Process (CAP) v2.0, Evidence Evaluation section.

===========

Question #:78 - [CMMC Ecosystem]

Prior to initiating an OSC's CMMC Assessment, the Lead Assessor briefed the team on the most important requirements of the assessment. The assessor also insisted that the same results of the findings summary, practice ratings, and Level recommendations must be submitted to the C3PAO for initial processes and review. After several weeks of assessment, the C3PAO completes the internal review, the recommended results are then submitted through the C3PAO for final quality review and rating approval. Which document stipulates these reporting requirements?

A. CMMC Assessment reporting requirements

B. DFARS 52.204-21 assessment reporting requirements

C. NISTSP 800-171 Revision 2 assessment reporting requirements

D. DFARS clause 252.204-7012 assessment reporting requirements

Answer: A

Explanation

The correct answer isA. CMMC Assessment Reporting Requirementsbecause this document specifically outlines thestructured processthat Certified Third-Party Assessment Organizations (C3PAOs) must follow when conducting and reporting CMMC assessments.

Understanding the CMMC Assessment Process

TheLead Assessorbriefs the team on theassessment requirementsand theevaluation criteriabefore the assessment begins.

Throughout the assessment,findings summaries, practice ratings, and level recommendationsare documented and reported.

These findings are internally reviewed by theC3PAObefore they are formally submitted forquality review and final rating approval.

Key Document Stipulating Reporting Requirements: CMMC Assessment Reporting Requirements

This documentspecifically details how assessments must be reportedwithin theCMMC ecosystem.

It describes the structured process for assessment submission, internalC3PAO reviews, andquality checks by the CMMC-ABbefore an organization can receive a final certification decision.

It ensures thatresults are consistent, transparent, and aligned with DoD cybersecurity compliance expectations.

Why Other Options Are Incorrect:

B. DFARS 52.204-21 Assessment Reporting Requirements

This clause only specifiesbasic safeguardingof Federal Contract Information (FCI) but doesnotdictate the reporting process for CMMC assessments.

C. NIST SP 800-171 Revision 2 Assessment Reporting Requirements

WhileNIST SP 800-171 Rev. 2outlines security controls, it doesnotdefine how CMMC assessments must be conducted and reported.

D. DFARS Clause 252.204-7012 Assessment Reporting Requirements

This DFARS clause focuses onincident reportingandcyber incident response requirementsbut does not detail theCMMC assessment reporting process.

CMMC Assessment Reporting Requirements, issued byThe Cyber ABandDoD, governs how C3PAOs must report assessment results.

CMMC Assessment Process (CAP)also outlines reporting workflows for certification.

Step-by-Step Breakdown:Official Reference:Thus, theCMMC Assessment Reporting Requirementsdocument is the authoritative source that dictates the reporting procedures for CMMC assessments.

Question #:79 - [Governance and Source Documents]

What is DFARS clause 252.204-7012 required for?

A. All DoD solicitations and contracts

B. Solicitations and contracts that use FAR part 12 procedures

C. Procurements solely for the acquisition of commercial off-the-shelf

D. Commercial off-the-shelf sold in the marketplace without modifications

Answer: A

Question #:80 - [CMMC Model Overview]

A company has a government services division and a commercial services division. The government services division interacts exclusively with federal clients and regularly receives FCI. The commercial services division interacts exclusively with non-federal clients and processes only publicly available information. For this company's CMMC Level 1 Self-Assessment, how should the assets supporting the commercial services division be categorized?

A. FCI Assets

B. Specialized Assets

C. Out-of-Scope Assets

D. Operational Technology Assets

Answer: C

Explanation

Understanding CMMC Asset CategorizationTheCMMC 2.0 Scoping Guidedefines how assets are categorized based on their involvement withFederal Contract Information (FCI)andControlled Unclassified Information (CUI).

In this scenario:

Thegovernment services divisioninteracts withfederal clientsandreceives FCI, making its assetsin-scopefor CMMC Level 1.

Thecommercial services divisioninteractsonly with non-federal clientsanddoes not handle FCI—this means its assets arenot subject to CMMC Level 1 requirementsand should be classified asOut-of-Scope Assets.

CMMC 2.0 Definition of Out-of-Scope AssetsAs per theCMMC Scoping Guide, assets that:

#Do not store, process, or transmit FCI/CUI

#Do not directly impact the security of in-scope assets

#Are completely segregated from the FCI/CUI environment are classified asOut-of-Scope Assets.

Since thecommercial services divisiononly processespublicly available information and has no interaction with FCI, its assets areout-of-scopefor CMMC Level 1 assessment.

A. FCI Assets#Incorrect. FCI assets areonly those that store, process, or transmit FCI. The commercial services division doesnothandle FCI, so its assets donotqualify.

B. Specialized Assets#Incorrect. Specialized assets refer toInternet of Things (IoT), Operational Technology (OT), and test equipment. These donot applyto a general commercial services division.

D. Operational Technology Assets#Incorrect.Operational Technology (OT) Assetsinvolveindustrial control systems, SCADA, and manufacturing equipment—which are not relevant to this scenario.

Why the Other Answers Are Incorrect

CMMC 2.0 Scoping Guide – Level 1 & Level 2

CMMC Assessment Process (CAP) Document

CMMC Official ReferencesThus,option C (Out-of-Scope Assets) is the correct answerbased on official CMMC scoping guidance.

Question #:81 - [CMMC Assessment Process (CAP)]

A Lead Assessor is planning an assessment and scheduling the test activities. Who MUST perform tests to obtain evidence?

A. OSC personnel who normally perform that work as the CCP observes

B. Military personnel and the CCP and/or Lead Assessor to test the adequacy of the written procedure(s)

C. Military personnel assigned to the contractor for that contract to ensure the confidentiality of the CUI

D. OSC personnel who do not ordinarily perform that work to evaluate the accuracy of the written procedure(s)

Answer: A

Explanation

Understanding Who Must Perform Tests in a CMMC AssessmentDuring aCMMC Level 2 Assessment, assessorsmust observe operational activities and security practicesto verify compliance. This process involves:

#Testing security controls and proceduresas part of the assessment.

#Observation of standard work practicesto ensure controls are properly implemented.

#Using operational personnel (OSC employees) who regularly perform the taskto ensure realistic assessment conditions.

Operational personnel (OSC employees) must conduct the actual work while assessors observe.

Certified CMMC Professionals (CCPs) or Lead Assessorsoversee and document the testing process.

Who Performs Tests?

A. OSC personnel who normally perform that work as the CCP observes # Correct

CMMC assessments require actual users (OSC personnel) to perform their regular duties while assessors observeto verify security practices.

B. Military personnel and the CCP and/or Lead Assessor to test the adequacy of the written procedure(s) # Incorrect

Military personnel are not responsible for testing contractor security controls.

Assessors observe and evaluate but do not perform testing themselves.

C. Military personnel assigned to the contractor for that contract to ensure the confidentiality of the CUI # Incorrect

Military personnel do not perform the testing.

The contractor (OSC) is responsible for implementing and demonstrating security controls.

D. OSC personnel who do not ordinarily perform that work to evaluate the accuracy of the written procedure (s) # Incorrect

Personnel unfamiliar with the job should not be used for testing.

Theassessment must reflect real-world conditions, so theactual employees who perform the work must demonstrate the process.

Why is the Correct Answer "A" (OSC personnel who normally perform that work as the CCP observes)?

CMMC Assessment Process (CAP) Document

Specifies thatassessments must observe real operational activities to determine compliance.

CMMC-AB Assessment Methodology

Requirestesting of security controls in a realistic operational environment, meaning actual OSC personnel must perform the tasks.

NIST SP 800-171A (Assessment Procedures for NIST SP 800-171)

Specifies thatinterviews and observations should be conducted with personnel who regularly perform the work.

Question #:82 - [CMMC Assessment Process (CAP)]

Which statement BEST describes an assessor's evidence gathering activities?

A. Use interviews for assessing a Level 2 practice.

B. Test all practices or objectives for a Level 2 practice

C. Test certain assessment objectives to determine findings.

D. Use examinations, interviews, and tests to gather sufficient evidence.

Answer: D

Explanation

Under theCMMC Assessment Process (CAP)andCMMC 2.0 guidelines, assessors must gather objective evidence to validate that an organization meets the required security practices and processes. This evidence collection is performed throughthree primary assessment methods:

Examination– Reviewing documents, records, system configurations, and other artifacts.

Interviews– Speaking with personnel to verify processes, responsibilities, and understanding of security controls.

Testing– Observing system behavior, performing technical validation, and executing controls in real-time to verify effectiveness.

TheCMMC Assessment Process (CAP)states that an assessor must use acombinationof evidence-gathering methods (examinations, interviews, and tests) to determine compliance.

CMMC 2.0 Level 2(Aligned withNIST SP 800-171) requires assessors to verify not only that policies and procedures exist but also that they are implemented and effective.

Solely relying ononemethod (like interviews in Option A) is insufficient.

Testing all practices or objectives (Option B)is unnecessary, as assessors followscoping guidanceto determine which objectives need deeper examination.

Testing only "certain" objectives (Option C)does not fully align with the requirement of gatheringsufficient evidencefrom multiple methods.

CMMC Assessment Process (CAP) Guide, Section 3.5 – Assessment Methodsexplicitly defines the use of examinations, interviews, and tests as the foundation of an effective assessment.

CMMC 2.0 Level 2 Practices and NIST SP 800-171require assessors to validate the presence, implementation, and effectiveness of security controls.

CMMC Appendix E: Assessment Proceduresstates that an assessor should use multiple sources of evidence to determine compliance.

Why Option D is CorrectCMMC 2.0 and Official Documentation ReferencesFinal VerificationTo ensure compliance withCMMC 2.0 guidelines and official documentation, an assessor must useexaminations, interviews, and teststo gather evidence effectively, makingOption D the correct answer.

Question #:83 - [CMMC Model Overview]

Where can a listing of all federal agencies' CUI indices and categories be found?

A. 32 CFR Section 2002

B. Official CUI Registry

C. Executive Order 13556

D. Official CMMC Registry

Answer: B

Explanation

Understanding the Official CUI RegistryTheControlled Unclassified Information (CUI) Registryis theauthoritative sourcefor all federal agencies'CUI categories and indices. It is maintained by theNational Archives and Records Administration (NARA)and provides:

#Acomprehensive listof CUI categories and subcategories.

#Details onwho can handle, store, and share CUI.

#Guidance onCUI marking and safeguarding requirements.

TheOfficial CUI Registryis theonly federal resourcethat listsall CUI categories and agencies that use them.

32 CFR Section 2002(Option A) definesCUI policiesbut doesnotprovide a full listing of CUI categories.

Executive Order 13556(Option C) established theCUI Programbut doesnotmaintain an active list of categories.

The "Official CMMC Registry" (Option D) does not exist—CMMC is a security framework, not a CUI classification system.

Why "Official CUI Registry" is Correct?Breakdown of Answer ChoicesOption

Description

Correct?

A. 32 CFR Section 2002

#Incorrect–Defines CUI program rules butdoes not listcategories.

B. Official CUI Registry

#Correct – The registry contains the full list of CUI categories.

C. Executive Order 13556

#Incorrect–Established the CUI program butdoes not maintain a category list.

D. Official CMMC Registry

#Incorrect–No such registry exists; CMMC is a cybersecurity framework, not a CUI classification system.

National Archives (NARA) CUI Registry– The authoritative source forall federal agency CUI categories.

32 CFR 2002– Provides CUIpolicy guidancebut refers agencies to theOfficial CUI Registryfor classification.

Official References from CMMC 2.0 and Federal DocumentationFinal Verification and ConclusionThe correct answer isB. Official CUI Registry, as it is theonly official source listing all federal agencies' CUI indices and categories.

Question #:84 - [CMMC Assessment Process (CAP)]

Contractor scoping requirements for a CMMC Level 2 Assessment to document the asset in an inventory, in the SSP and on the network diagram apply to:

A. GUI Assets.

B. CUI and Security Protection Asset categories.

C. all asset categories except for the Out-of-scope Assets.

D. Contractor Risk Managed Assets and Specialized Assets.

Answer: B

Explanation

UnderCMMC Level 2, contractors are required toidentify, document, and categorize assetsinvolved in handlingControlled Unclassified Information (CUI). This is part of thescoping process, which ensures that all security-relevant assets are properly protected and accounted for in the System Security Plan (SSP), asset inventory, and network diagram.

CMMC Scoping Requirements for Level 2 Assessments:

TheCMMC Scoping Guide(CMMC v2.0) identifies four asset categories:

CUI Assets:Systems that store, process, or transmit CUI.

Security Protection Assets (SPA):Systems providing security functions for CUI Assets (e.g., firewalls, SIEMs).

Contractor Risk Managed Assets (CRMA):Assets that interact with CUI but arenot directly controlledby the organization (e.g., personal devices).

Specialized Assets:These include IoT devices, OT systems, and Government Furnished Equipment (GFE) thatmay require specific security controls.

Where Documentation is Required:

The contractor mustdocument all assets (except out-of-scope assets)in:

The System Security Plan (SSP):A key document detailing security controls and asset categorization.

An asset inventory:Lists all in-scope assets (CUI Assets, SPAs, CRMA, and Specialized Assets).

The network diagram:Provides a visual representation of system connectivity and security boundaries.

Why Out-of-Scope Assets Are Excluded:

TheCMMC Scoping Guidespecifically states that Out-of-Scope Assets arenot required to be documentedin these compliance artifacts because they haveno direct or indirect interaction with CUI.

These assets do not require CMMC controls because they are completely isolated from CUI handling environments.

Why the Other Answer Choices Are Incorrect:

(A) GUI Assets:There is no specific "GUI Asset" category in CMMC scoping.

(B) CUI and Security Protection Asset categories:While these are included, this answerexcludesContractor Risk Managed and Specialized Assets, which are also required.

(D) Contractor Risk Managed Assets and Specialized Assets:These assetsare included in scopingbut this answer excludes CUI Assets and Security Protection Assets, making it incomplete.

Step-by-Step Breakdown:Final Validation from CMMC Documentation:According to theCMMC Assessment Scope Level 2 Guide, allin-scope assetsmust be documented in the SSP, inventory, and network diagram.The only assets excluded are Out-of-Scope Assets.

Thus, the correct answer is:

C. All asset categories except for the Out-of-Scope Assets.

Question #:85 - [Implementation and Scoping]

A dedicated local printer is used to print out documents with FCI in an organization. This is considered an FCI Asset Which function BEST describes what the printer does with the FCI?

A. Encrypt

B. Manage

C. Process

D. Distribute

Answer: C

Explanation

Understanding the Role of an FCI Asset in CMMCAdedicated local printer used to print Federal Contract Information (FCI)is considered anFCI Asset. UnderCMMC Level 1, FCI assets are required to meetbasic cybersecurity controlsto ensure that FCI is properlyprotected from unauthorized access.

Step-by-Step Breakdown:#1. Why "Process" is the Best Answer

The printerreceives digital FCI, converts it into a physical format (paper), and outputs the document.

This aligns with thedefinition of "processing" in CMMC, which includes:

Transforming or modifying data

Generating output (e.g., printed documents)

Using systems to interpret or manipulate information

#2. Why the Other Answer Choices Are Incorrect:

(A) Encrypt#

Aprinter does not encryptFCI—it simply prints it. Encryption applies todigital storage and transmission, not printing.

(B) Manage#

Managing FCI typically refers togovernance, access control, and oversight, which is not the function of a printer.

(D) Distribute#

While a printed documentcould be distributed, theprinter itself is not responsible for distributing FCI—it only processes the data for output.

CMMC Assessment Guide (Level 1)confirms thatprocessing FCI includes using systems that convert or transform information, such as printers.

NIST SP 800-171definesprocessingas an action thatchanges or manipulates information, which applies to printing.

Final Validation from CMMC Documentation:

Question #:86 - [CMMC Assessment Process (CAP)]

In scoping a CMMC Level 1 Self-Assessment, all of the computers and digital assets that handle FCI are identified. A file cabinet that contains paper FCI is also identified. What can this file cabinet BEST be determined to be?

A. In scope, because it is an asset that stores FCI

B. In scope, because it is part of the same physical location

C. Out of scope, because they are all only paper documents

D. Out of scope, because it does not process or transmit FCI

Answer: D

Explanation

Does a File Cabinet Containing Paper FCI Fall Within CMMC Scope?CMMConly applies to digital systems and assetsthatprocess, store, or transmitFederal Contract Information (FCI)andControlled Unclassified Information (CUI).Physical storage (such as paper documents) is not included in CMMC scoping.

Step-by-Step Breakdown:#1. CMMC Scope Covers Only Digital Systems and Assets

According to theCMMC Scoping Guide (Level 1),only digital assetsthat handleFCIarein scopefor aLevel 1 Self-Assessment.

Afile cabinetisnot a digital system; therefore, it isnot in scopefor CMMC compliance.

#2. Why the Other Answer Choices Are Incorrect:

(A) In scope, because it is an asset that stores FCI#

Incorrect:While the file cabinetdoes store FCI,CMMC only applies to digital systems.

(B) In scope, because it is part of the same physical location#

Incorrect:CMMCdoes notconsiderphysical proximitywhen determining scope—only digital data handling matters.

(D) Out of scope, because it does not process or transmit FCI#

Partially correct, but incomplete: Themain reasonit is out of scope is that itcontains only paper documents, not that it doesn’t process/transmit data.

TheCMMC Level 1 Scoping Guideexplicitly states thatpaper-based storage of FCI does not fall within scope.

Final Validation from CMMC Documentation:Thus, the correct answer is:

#C. Out of scope, because they are all only paper documents.

Question #:87 - [CMMC Ecosystem]

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

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, theOrganization Seeking Certification (OSC)may suggest personnel for interviews. However, the person interviewedmustbe someone who:

#Implementsthe practice (directly responsible for executing it).

#Performsthe practice (carries out day-to-day security operations).

#Supportsthe practice (provides necessary resources or oversight).

Theassessor needs direct insightsfrom individuals actively involved in the practice.

Funding (Option A)does not providetechnical or operationalinsight into practice execution.

Auditing (Option B)focuses on compliance checks, but auditorsdo not implementthe practice.

Supporting, auditing, and performing (Option C)includesauditors, who arenot necessarily the right interviewees.

Why "Implements, Performs, or Supports That Practice" is Correct?Breakdown of Answer ChoicesOption

Description

Correct?

A. Funds that practice.

#Incorrect–Funding is important but doesnot mean direct involvement.

B. Audits that practice.

#Incorrect–Auditors check compliance but donot implementpractices.

C. Supports, audits, and performs that practice.

#Incorrect–Auditing isnot a requirementfor 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 bedirectly responsiblefor implementing, performing, or supporting the practice.

Official References from CMMC 2.0 DocumentationFinal Verification and ConclusionThe correct answer isD. Implements, performs, or supports that practice, as the interviewee mustactively contribute to the execution of the practice.

Question #:88 - [CMMC Ecosystem]

During the review of information that was published to a publicly accessible site, an OSC correctly identifies that part of the information posted should have been restricted. Which item did the OSC MOST LIKELY identify?

A. FCI

B. Change of leadership in the organization

C. Launching of their new business service line

D. Public releases identifying major deals signed with commercial entities

Answer: A

Explanation

Understanding Federal Contract Information (FCI) and Publicly Accessible InformationFederal Contract Information (FCI)isnon-public informationprovided by or generated for the U.S. governmentunder a contractthat isnot intended for public release.

Key Characteristics of FCI:#FCI includesdetails related togovernment contracts, project specifics, and performance data.

#It must be protected under FAR 52.204-21, which requiresbasic safeguarding measuresto prevent unauthorized access.

#Posting FCI on a public site is a security violationsince it ismeant to be restrictedfrom public disclosure.

A. FCI # Correct

FCI must be protected from unauthorized access, and if it wasincorrectly published online, it should have been restricted.

B. Change of leadership in the organization # Incorrect

Leadership changes are typically public informationand do not require restriction unless they involve sensitive government-related security clearances.

C. Launching of their new business service line # Incorrect

Marketing and business announcementsare generallypublicly availableandnot restricted information.

D. Public releases identifying major deals signed with commercial entities # Incorrect

Commercial contracts and business deals are not considered FCIunless they involvegovernment contracts.

Why is the Correct Answer "A. FCI (Federal Contract Information)"?

FAR 52.204-21 (Basic Safeguarding of Covered Contractor Information Systems)

DefinesFCI as sensitive but unclassified informationthat must beprotected from public disclosure.

CMMC 2.0 Level 1 Requirements

Requires contractors toprotect FCI under basic cybersecurity standardsto prevent unauthorized exposure.

DoD Guidance on FCI Protection

States thatpublishing FCI on public websites violates federal cybersecurity requirements.

CMMC 2.0 References Supporting This Answer:

Question #:89 - [CMMC Model Overview]

Before submitting the assessment package to the Lead Assessor for final review, a CCP decides to review the Media Protection (MP) Level 1 practice evidence to ensure that all media containing FCI are sanitized or destroyed before disposal or release for reuse. After a thorough review, the CCP tells the Lead Assessor that all supporting documents fully reflect the performance of the practice and should be accepted because the evidence is:

A. official.

B. adequate.

C. compliant.

D. subjective.

Answer: B

Explanation

CMMC Level 1 includes 17 practices derived fromFAR 52.204-21. Among them, theMedia Protection (MP) practicerequires organizations to ensure thatmedia containing FCI is sanitized or destroyed before disposal or release for reuseto prevent unauthorized access.

This requirement ensures that any storage devices, hard drives, USBs, or physical documents containingFederal Contract Information (FCI)areproperly disposed of or sanitizedto prevent data leakage.

The evidence collected for this practice should demonstrate that an organization has established and followed propermedia sanitization or destruction procedures.

Why the Correct Answer is "B. Adequate"?TheCMMC Assessment Process (CAP) Guideoutlines that for an assessment to be considered complete, all submitted evidence must meet the standard ofadequacybefore it is accepted by the Lead Assessor.

Definition of "Adequate" Evidence in CMMC:

Evidence isadequatewhen itfully demonstrates that a practice has been performed as requiredby CMMC guidelines.

TheLead Assessorevaluates whether the submitted documentation meets the CMMC 2.0 Level 1 requirements.

If the evidenceaccurately and completely demonstrates the sanitization or destruction of media containing FCI, then it meets the standard ofadequacy.

Why Not the Other Options?

A. Official– While the evidence may come from an official source, the CMMCdoes not require evidence to be "official", only that it beadequateto confirm compliance.

C. Compliant– Compliance is the final result of an assessment, but before compliance is determined, the evidence must first beadequatefor evaluation.

D. Subjective– CMMC evidence isobjective, meaning it should be based on verifiable documents, policies, logs, and procedures—not opinions or interpretations.

CMMC 2.0 Scoping Guide (Nov 2021)– Specifies that Media Protection (MP) at Level 1 applies only to assets that process, store, or transmit FCI.

CMMC Assessment Process (CAP) Guide– Definesadequate evidenceas documentation that completely and clearly supports the implementation of a required security practice.

FAR 52.204-21– The source of the Level 1 requirements, which includessanitization and destruction of media containing FCI.

Relevant CMMC 2.0 References:Final Justification:The CCP’s statement that the evidence"fully reflects the performance of the practice"aligns with the definition ofadequate evidenceunder CMMC. Since adequacy is the key standard used before final compliance decisions are made, the correct answer isB. Adequate.

Question #:90 - [CMMC Model Overview]

A client uses an external cloud-based service to store, process, or transmit data that is reasonably believed to qualify as CUI. According to DFARS clause 252.204-7012. what set of established security requirements MUST that cloud provider meet?

A. FedRAMP Low

B. FedRAMP Moderate

C. FedRAMP High

D. FedRAMP Secure

Answer: B

Explanation

UnderDFARS 252.204-7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting), if acontractoruses acloud-based serviceto store, process, or transmitControlled Unclassified Information (CUI), the cloud providermustmeet the security requirements ofFedRAMP Moderate or equivalent.

CUI stored in the cloud must be protected according to FedRAMP Moderate (or higher) requirements.

The cloud provider must meetFedRAMP Moderate baseline security controls, which align withNIST SP 800-53moderate impact level requirements.

The cloud provider must also ensure compliance withincident reportingandcyber incident response requirementsin DFARS 252.204-7012.

Key Requirements from DFARS 252.204-7012 (c)(1):

A. FedRAMP Low # Incorrect

FedRAMP Lowis intended for systems withlow confidentiality, integrity, and availability risks, making itinadequate for CUI protection.

B. FedRAMP Moderate # Correct

FedRAMP Moderate is the minimum required level for CUIunder DFARS 252.204-7012.

It provides a security baseline for protectingsensitive but unclassified government data.

C. FedRAMP High # Incorrect

FedRAMP Highapplies to systems handlinghighly sensitive information (e.g., classified or national security data), which is not necessarily required for CUI.

D. FedRAMP Secure # Incorrect

There isno official FedRAMP Secure categoryin FedRAMP guidelines.

Why is the Correct Answer "FedRAMP Moderate" (B)?

DFARS 252.204-7012(c)(1)

Specifies thatcontractors using external cloud services for CUI must meet FedRAMP Moderate or equivalent.

CMMC 2.0 Level 2 Requirements

CUI must be protected using NIST SP 800-171 security requirements, whichalign with FedRAMP Moderate controls.

FedRAMP Security Baselines

FedRAMP Moderateis designed for systems that handlesensitive government data, including CUI.

CMMC 2.0 References Supporting this Answer:

Question #:91 - [CMMC Model Overview]

A CCP is on their first assessment for CMMC Level 2 with an Assessment Team and is reviewing the CMMC Assessment Process to understand their responsibilities. Which method gathers information from the subject matter experts to facilitate understanding and achieve clarification?

A. Test

B. Examine

C. Interview

D. Assessment

Answer: C

Explanation

Understanding CMMC Assessment MethodsTheCMMC Assessment Process (CAP)definesthree primary assessment methodsused to verify compliance with cybersecurity practices:

Examine– Reviewing documents, policies, configurations, and logs.

Interview– Engaging with subject matter experts (SMEs) to clarify processes and verify implementation.

Test– Observing technical implementations, such as system configurations and security measures.

Since the question asks for a method thatgathers information from SMEs to facilitate understanding and achieve clarification, the correct method isInterview.

Why "Interview" is Correct?#Interviewsare specifically designed togather information from SMEsto confirm understanding and clarify security processes.

#TheCMMC Assessment Guiderequires assessors tointerview key personnelresponsible for cybersecurity practices.

#Examine (Option B)andTest (Option A)are also valid assessment methods, but they donot focus on gathering insights directly from SMEs.

Breakdown of Answer ChoicesOption

Description

Correct?

A. Test

#Incorrect–This method involvestechnical verification, not gathering SME insights.

B. Examine

#Incorrect–This method focuses ondocument review, not SME interaction.

C. Interview

#Correct – The method used to gather information from SMEs and achieve clarification.

D. Assessment

#Incorrect–This is a general term,not a specific assessment method.

CMMC Assessment Process Guide (CAP)– DefinesInterviewas the method for obtaining information from SMEs.

Official References from CMMC 2.0 DocumentationFinal Verification and ConclusionThe correct answer isC. Interview, as this methodgathers insights from subject matter expertsto verify cybersecurity implementations.

Question #:92 - [CMMC Assessment Process (CAP)]

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

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 broaderproject 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 #:93 - [CMMC Ecosystem]

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. C3PAO

B. CMMC-AB

C. Assessment Team

D. Assessment Sponsor

Answer: A

Explanation

Who Has the Final Authority Over Assessment Results?During aCMMC Level 2 assessment, theCertified Third-Party Assessment Organization (C3PAO)is responsible for conducting and finalizing the assessment results.

Key Responsibilities of a C3PAO#Leads the assessmentand ensures it follows the CMMC Assessment Process (CAP).

#Validates compliancewith CMMC Level 2 requirements based onNIST SP 800-171controls.

#Finalizes the assessment resultsand submits them to theCMMC-ABand theDoD.

#Handles disagreementsfrom the OSC but hasfinal decision-making authorityon results.

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

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

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

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

Why "C3PAO" is Correct?Breakdown of Answer ChoicesOption

Description

Correct?

A. C3PAO

#Correct – C3PAOs finalize and submit assessment results.

B. CMMC-AB

#Incorrect–The CMMC-AB accredits C3PAOs but doesnot finalize results.

C. Assessment Team

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

D. Assessment Sponsor

#Incorrect–This is arepresentative of the OSC, not the assessment authority.

CMMC Assessment Process Guide (CAP)– DefinesC3PAO authorityover final assessment results.

Official References from CMMC 2.0 DocumentationFinal Verification and ConclusionThe correct answer isA. C3PAO, as theC3PAO has final decision-making authority over CMMC assessment results.

Question #:94 - [CMMC Ecosystem]

A CMMC Assessment is being conducted at an OSC's HQ. which is a shared workspace in a multi-tenant building. The OSC is renting four offices on the first floor that can be locked individually. The first-floor conference room is shared with other tenants but has been reserved to conduct the assessment. The conference room has a desk with a drawer that does not lock. At the end of the day, an evidence file that had been sent by email is reviewed. What is the BEST way to handle this file?

A. Review it. print it, and put it in the desk drawer.

B. Review it, and make notes on the computer provided by the client.

C. Review it, print it, make notes, and then shred it in cross-cut shredder in the print room.

D. Review it. print it, and leave it in a folder on the table together with the other documents.

Answer: C

Explanation

In the context of the Cybersecurity Maturity Model Certification (CMMC) 2.0, particularly at Level 2, organizations are required to implement stringent controls to protect Controlled Unclassified Information (CUI). This includes adhering to specific practices related to media protection and physical security.

Media Protection (MP):

MP.L2-3.8.1 – Media Protection:Organizations must protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. This ensures that sensitive information is not accessible to unauthorized individuals.

Defense Innovation Unit

MP.L2-3.8.3 – Media Disposal:It is imperative to sanitize or destroy information system media containing CUI before disposal or release for reuse. This practice prevents potential data breaches from discarded or repurposed media.

Defense Innovation Unit

Physical Protection (PE):

PE.L2-3.10.2 – Monitor Facility:Organizations are required to protect and monitor the physical facility and support infrastructure for organizational systems. This includes ensuring that areas where CUI is processed or stored are secure and access is controlled.

Defense Innovation Unit

Application to the Scenario:

Given that the Organization Seeking Certification (OSC) operates within a shared, multi-tenant building and utilizes a common conference room for assessments, the following considerations are crucial:

Reviewing the Evidence File:The evidence file, which contains CUI, should be reviewed on a secure, authorized device to prevent unauthorized access or potential data leakage.

Printing the Evidence File:If printing is necessary, ensure that the printer is located in a secure area, and the printed documents are retrieved immediately to prevent unauthorized viewing.

Making Notes:Any notes derived from the evidence file should be treated with the same level of security as the original document, especially if they contain CUI.

Disposal of Printed Materials:After the assessment, all printed materials and notes containing CUI must be destroyed using a cross-cut shredder. Cross-cut shredding ensures that the information cannot be reconstructed, thereby maintaining confidentiality.

totem.tech

Options A and D are inadequate as they involve leaving sensitive information in unsecured locations, which violates CMMC physical security requirements. Option B, while secure in terms of digital handling, does not address the proper disposal of any physical copies that may have been made. Therefore, Option C is the best practice, aligning with CMMC 2.0 guidelines by ensuring that all physical media containing CUI are properly reviewed, securely stored during use, and thoroughly destroyed when no longer needed.

Question #:95 - [CMMC Ecosystem]

Within how many days from the Assessment Final Recommended Findings Brief should the Lead Assessor and Assessment Team Members, if necessary, review the accuracy and validity of (he OSC's updated POA&M with any accompanying evidence or scheduled collections?

A. 90 days

B. 180 days

C. 270 days

D. 360 days

Answer: B

Explanation

In theCMMC 2.0 Assessment Process, after theAssessment Final Recommended Findings Brief, theLead Assessor and Assessment Team Membersmustreview the accuracy and validity of the Organization Seeking Certification (OSC)’s updated Plan of Action & Milestones (POA&M) and any accompanying evidence or scheduled collectionswithin180 days.

TheCMMC Assessment Process (CAP)outlines that organizations haveup to 180 daysto address identifieddeficienciesafter their initial assessment.

During this time, the OSC can update itsPOA&M with additional evidenceto demonstrate compliance.

Relevant CMMC 2.0 Reference:

A. 90 days # Incorrect

The CMMC CAP does not impose a90-day limiton POA&M updates; instead,180 daysis the standard timeframe.

B. 180 days # Correct

PerCMMC Assessment Process guidelines, theLead Assessor and Teammust review updateswithin 180 days.

C. 270 days # Incorrect

No official CMMC documentation mentions a270-dayreview period.

D. 360 days # Incorrect

The process must be completedfar sooner than 360 daysto maintain compliance.

Why is the Correct Answer 180 Days (B)?

CMMC Assessment Process (CAP) Document

Defines the180-day windowfor the OSC to update itsPOA&M and submit evidencefor review.

CMMC 2.0 Official Guidelines

Specifies that organizations are givenup to 180 daysto remediate deficiencies before reassessment.

CMMC 2.0 References Supporting this Answer:

Question #:96 - [CMMC Model Overview]

Which domains are a part of a Level 1 Self-Assessment?

A. Access Control (AC), Risk Management <RM), and Media Protection (MP)

B. Risk Management (RM). Access Control (AC), and Physical Protection (PE)

C. Access Control (AC), Physical Protection (PE), and Identification and Authentication (IA)

D. Risk Management (RM). Media Protection (MP), and Identification and Authentication (IA)

Answer: C

Explanation

CMMCLevel 1focuses onbasic cyber hygieneand includes17 practicesderived fromNIST SP 800-171 Rev. 2butonly covers the protection of Federal Contract Information (FCI)—not Controlled Unclassified Information (CUI).

UnlikeLevel 2, which aligns fully withNIST SP 800-171,Level 1 does not require third-party certificationand can beself-assessedby the organization.

Domains Covered in a Level 1 Self-AssessmentCMMC Level 1 practices fall underthree specific domains:

Access Control (AC)– Ensures that only authorized individuals can access FCI.

Physical Protection (PE)– Protects physical access to systems and facilities storing FCI.

Identification and Authentication (IA)– Verifies the identity of users accessing systems containing FCI.

These domains focus on foundational security controls necessary toprotect FCI from unauthorized access.

CMMC Model v2.0states thatLevel 1 includes only 17 practicesmapped toNIST SP 800-171requirements specific toAccess Control (AC), Physical Protection (PE), and Identification and Authentication (IA).

CMMC Assessment Guide, Level 1confirms thatRisk Management (RM) and Media Protection (MP) are not included in Level 1, as they pertain to more advanced security measures needed for handlingCUI (Level 2).

A. Access Control (AC), Risk Management (RM), and Media Protection (MP)# Incorrect.Risk Management (RM) and Media Protection (MP) are Level 2 domains.

B. Risk Management (RM), Access Control (AC), and Physical Protection (PE)# Incorrect.Risk Management (RM) is not part of Level 1.

C. Access Control (AC), Physical Protection (PE), and Identification and Authentication (IA)#Correct.These are thethree domains covered in CMMC Level 1 self-assessments.

D. Risk Management (RM), Media Protection (MP), and Identification and Authentication (IA)# Incorrect. Risk Management (RM) and Media Protection (MP) are Level 2 domains.

Official CMMC 2.0 Documentation ReferencesBreakdown of Answer ChoicesConclusionThecorrect answer is C. Access Control (AC), Physical Protection (PE), and Identification and Authentication (IA), as these are theonly three domains included in a CMMC Level 1 Self-Assessmentaccording toCMMC 2.0 documentation and NIST SP 800-171 mapping.

CMMC 2.0 Model Overview – DoD Official Documentation

CMMC Assessment Guide, Level 1

NIST SP 800-171 Rev. 2 (Basic Security Requirements for FCI)

Reference Documents for Further Reading

Question #:97 - [CMMC Ecosystem]

In preparation for a CMMC Level 1 Self-Assessment, the IT manager for a DIB organization is documenting asset types in the company's SSP The manager determines that identified machine controllers and assembly machines should be documented as Specialized Assets. Which type of Specialized Assets has the manager identified and documented?

A. loT

B. Restricted IS

C. Test equipment

D. Operational technology

Answer: D

Explanation

Understanding Specialized Assets in a CMMC Self-AssessmentDuringCMMC Level 1 Self-Assessments, organizations must classify theirassetsin theSystem Security Plan (SSP).

Operational Technology (OT)includesmachine controllers, industrial control systems (ICS), and assembly machines.

Thesesystems control physical processesin manufacturing, energy, and industrial environments.

OT assets are distinct from traditional IT systemsbecause they haveunique security considerations(e.g., real-time control, legacy system constraints).

Specialized Asset Type: Operational Technology (OT)

A. IoT (Internet of Things) # Incorrect

IoT devicesinclude smart home systems, connected sensors, and networked appliances, butmachine controllers and assembly machines fall under OT, not IoT.

B. Restricted IS # Incorrect

Restricted Information Systems (IS) refer to classified or highly controlled systems, whichdoes not apply to standard industrial machines.

C. Test Equipment # Incorrect

Test equipment includes diagnostic tools or measurement devicesused forquality assurance, not industrial machine controllers.

D. Operational Technology # Correct

Machine controllers and assembly machinesare part ofindustrial automation and control systems, which are classified asOperational Technology (OT).

Why is the Correct Answer "D. Operational Technology"?

CMMC Scoping Guidance for Level 1 & Level 2 Assessments

DefinesOperational Technology (OT) as a category of Specialized Assetsthat requirespecific security considerations.

NIST SP 800-82 (Guide to Industrial Control Systems Security)

Identifiesmachine controllers and assembly machinesas part ofOperational Technology (OT).

CMMC 2.0 Asset Classification Guidelines

Specifies thatOT systems should be documented separately in an organization's SSP.

CMMC 2.0 References Supporting This Answer:

Question #:98 - [CMMC Assessment Process (CAP)]

When planning an assessment, the Lead Assessor should work with the OSC to select personnel to be interviewed who could:

A. Have a security clearance

B. Be a senior person in the company

C. Demonstrate expertise on the CMMC requirements

D. Provide clarity and understanding of their practice activities

Answer: D

Explanation

Per the CMMC Assessment Process (CAP), when planning an assessment, the Lead Assessor must coordinate with the Organization Seeking Certification (OSC) to select interview participants who can provide clarity and understanding of their practice activities. The intent is to interview individuals directly involved with and knowledgeable about the processes and practices under review, rather than selecting personnel based solely on rank, clearance, or formal expertise in CMMC.

This ensures the assessment is evidence-based and grounded in how practices are actually performed within the OSC.

Reference Documents:

- CMMC Assessment Process (CAP), v1.0

Question #:99 - [Implementation and Scoping]

What is the MINIMUM required marking for a document containing CUI?

A. "CUI" must be placed in the header and footer of the document

B. "WCUI" must be placed in the header and footer of the document

C. Portion marks must be placed on all sections, parts, paragraphs, etc. known to contain CUI

D. A cover page must be placed to obscure content with the acronym "CUI" prominently placed

Answer: A

Explanation

Per DoDI 5200.48, Controlled Unclassified Information (CUI), the minimum marking requirement is that the word “CUI” must appear in the header and footer of each page of a document containing CUI. Additional markings such as portion markings or cover sheets may be applied depending on the situation, but the minimum baseline requirement is header and footer placement of "CUI".

Reference Documents:

- DoDI 5200.48, Controlled Unclassified Information (CUI)

Question #:100 - [CMMC Ecosystem]

While conducting a CMMC Assessment, an individual from the OSC provides documentation to the assessor for review. The documentation states an incident response capability is established and contains information on incident preparation, detection, analysis, containment, recovery, and user response activities. Which CMMC practice is this documentation attesting to?

A. IR.L2-3.6.1: Incident Handling

B. IR.L2-3.6.2: Incident Reporting

C. IR.L2-3.6.3: Incident Response Testing

D. IR.L2-3.6.4: Incident Spillage

Answer: A

Explanation

Understanding CMMC 2.0 Incident Response PracticesTheIncident Response (IR) domaininCMMC 2.0 Level 2aligns withNIST SP 800-171, Section 3.6, which defines requirements forestablishing and maintaining an incident response capability.

The documentation provideddescribes an incident response capability that includes preparation, detection, analysis, containment, recovery, and user response activities.

IR.L2-3.6.1specifically requires organizations toestablish an incident handling processcovering:

Preparation

Detection & Analysis

Containment

Eradication & Recovery

Post-Incident Response

B. IR.L2-3.6.2: Incident Reporting (Incorrect)

Incident reporting focuses on reporting incidents to external parties (e.g., DoD, DIBNet),which isnot what the provided documentation describes.

C. IR.L2-3.6.3: Incident Response Testing (Incorrect)

Incident response testing ensures that the response process is regularly tested and evaluated,which isnot the primary focus of the documentation provided.

D. IR.L2-3.6.4: Incident Spillage (Incorrect)

Incident spillage specifically refers to CUI exposure or handling unauthorized CUI incidents,which isnot the scenario described.

The correct answer isA. IR.L2-3.6.1: Incident Handling, as the documentationattests to the establishment of an incident response capability.

References:

CMMC 2.0 Level 2 Practices (NIST SP 800-171, Section 3.6)

CMMC Assessment Process (CAP) Guide

Question #:101 - [CMMC Ecosystem]

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

A. DoD OUSD

B. Authorized holder

C. Information Disclosure Official

D. Presidential authorized Original Classification Authority

Answer: B

Explanation

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

Definition of an Authorized Holder

PerDoDI 5200.48, Section 3.4, anauthorized holderis anyone who has beengranted accessto CUI and is responsible for handling, safeguarding, and marking it according toDoD CUI policy.

The authorized holder may be:

ADoD employee

Acontractorhandling CUI

Anyorganization or individual authorizedto access and manage CUI

DoD Guidance on CUI Marking Responsibilities

DoDI 5200.48, Section 4.2:

The individual creating or handling CUImust apply the appropriate markings as per the DoD CUI Registry guidelines.

DoDI 5200.48, Section 5.2:

Themarking responsibility is NOT limited to a specific positionlike an Information Disclosure Official or a high-level DoD office.

Instead, it is theresponsibility of the person or entity generating, handling, or disseminatingthe CUI.

Why the Other Answer Choices Are Incorrect:

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

The OUSD plays apolicy-setting rolebut doesnot directly mark CUI.

(C) Information Disclosure Official:

This role is responsible forpublic release of information, but marking CUI is the duty of theauthorized holdermanaging the data.

(D) Presidential authorized Original Classification Authority (OCA):

OCAs classifynational security information (Confidential, Secret, Top Secret), not CUI, which isnot classified information.

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

Question #:102 - [Governance and Source Documents]

A cyber incident is discovered that affects a covered contractor IS and the CDI residing therein. How long does the contractor have to inform the DoD?

A. 24 hours

B. 48 hours

C. 72 hours

D. 96 hours

Answer: C

Explanation

Contractors that handle Covered Defense Information (CDI) are required to report cyber incidents to the Department of Defense within 72 hours of discovery.

Supporting Extracts from Official Content:

- DFARS 252.204-7012(c)(1): "When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, the Contractor shall conduct a review… and rapidly report the cyber incident to DoD within 72 hours of discovery."

Why Option C is Correct:

- The regulation explicitly specifies 72 hours.
- Options A (24 hrs), B (48 hrs), and D (96 hrs) do not align with DFARS requirements.

References (Official CMMC v2.0 Content and Source Documents):

- DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting.
- CMMC v2.0 Governance – Source Documents list includes DFARS 252.204-7012.

===========

Question #:103 - [CMMC Ecosystem]

A Level 2 Assessment of an OSC is winding down and the final results are being prepared to present to the OSC. When should the final results be delivered to the OSC?

A. At the end of every day of the assessment

B. Daily and during a final separately scheduled review

C. Either at the final Daily Checkpoint, or during a separately scheduled findings and recommendation review

D. Either after approval from the C3PAO. or during a separately scheduled final recommended findings review

Answer: C

Explanation

Understanding the Reporting Process in a CMMC 2.0 Level 2 AssessmentACMMC Level 2 Assessmentconducted by aCertified Third-Party Assessor Organization (C3PAO)follows a structured approach to gathering evidence, evaluating compliance, and reporting findings to theOrganization Seeking Certification (OSC). The reporting process is outlined in theCMMC Assessment Process (CAP) Guide, which specifies how findings should be communicated.

Daily Checkpoints:

Throughout the assessment, the assessor team holdsdaily checkpoint meetingswith the OSC to provide updates on progress, observations, and preliminary findings.

These checkpoints help ensure transparency and allow the OSC to address minor issues as they arise.

Final Results Delivery:

Thefinal assessment resultsare typically shared during thefinal daily checkpointOR in aseparately scheduled findings and recommendations reviewmeeting.

This ensures that the OSC receives a structured and complete summary of the assessment findings before the official report is submitted.

TheCMMC Assessment Process (CAP) Guide, Section 4.5clearly states that assessment findings should be presentedeither at the last daily checkpoint or during a separately scheduled final review.

This aligns with best practices formaintaining transparency and ensuring the OSC has clarity on their assessment resultsbefore the final report submission.

Option A (End of every day)is incorrect because while assessors do provide updates, they do not deliver the "final results" daily.

Option B (Daily and a separate final review)is misleading, as the CAP Guide allows assessors tochoosebetween the final daily checkpoint OR a separate findings review—not both.

Option D (After C3PAO approval)is incorrect because theC3PAO does not approve findings before they are communicated to the OSC. The assessment team directly presents the results first.

CMMC Assessment Process (CAP) Guide, Section 4.5: Reporting and Findings Communication

CMMC 2.0 Level 2 Assessment Process Overview

CMMC Assessment Final Report Guidelines

Assessment Communication StructureWhy Option C is CorrectOfficial CMMC Documentation ReferencesFinal VerificationBased on officialCMMC 2.0 documentation, thefinal assessment results should be presented to the OSC either at the last daily checkpoint or in a separately scheduled review session, making Option C the correct answer.

Question #:104 - [CMMC Model Overview]

In the Code of Professional Conduct, what does the practice of Professionalism require?

A. Do not copy materials without permission to do so.

B. Do not make assertions about assessment outcomes.

C. Refrain from dishonesty in all dealings regarding CMMC.

D. Ensure the security of all information discovered or received.

Answer: C

Explanation

What Does the Practice of Professionalism Require in the CMMC Code of Professional Conduct?TheCMMC Code of Professional Conduct (CoPC)sets ethical and professional standards forCertified CMMC Assessors (CCAs) and Certified CMMC Professionals (CCPs).Professionalismrequireshonesty and integrity in all CMMC-related activities.

Step-by-Step Breakdown:#1. Professionalism Requires Ethical Behavior

TheCoPC states that professionalismincludes:

Acting with integrityin all assessment-related activities.

Providing truthful and objective assessmentsof cybersecurity practices.

Avoiding deceptive or misleading claimsabout assessments or compliance.

#2. Why the Other Answer Choices Are Incorrect:

(A) Do not copy materials without permission to do so#

This falls underIntellectual Property (IP) protection, notProfessionalism.

(B) Do not make assertions about assessment outcomes#

Assessorsmustprovide findings based on evidence. The rule is aboutnot making false or misleading claims, not about avoiding assertions altogether.

(D) Ensure the security of all information discovered or received#

This falls underConfidentiality, notProfessionalism.

TheCMMC Code of Professional Conduct (CoPC)definesProfessionalism as requiring honesty and integrityin allCMMC-related activities.

Final Validation from CMMC Documentation:Thus, the correct answer is:

#C. Refrain from dishonesty in all dealings regarding CMMC.

Question #:105 - [Roles and Responsibilities]

Who is responsible for ensuring that subcontractors have a valid CMMC Certification?

A. CMMC-AB

B. OUSD A&S

C. DoD agency or client

D. Contractor organization

Answer: D

Explanation

Under DFARS and CMMC requirements, the prime contractor is responsible for ensuring its subcontractors meet the required CMMC level. Neither the DoD, The Cyber AB, nor OUSD A&S directly manages subcontractor certification.

Supporting Extracts from Official Content:

- DFARS 252.204-7021: “The contractor shall ensure that its subcontractors have the appropriate CMMC level certification for the information they will handle.”

Why Option D is Correct:

- Compliance responsibility flows through the contractor supply chain.
- CMMC-AB (The Cyber AB) accredits assessors but does not police subcontractors.
- OUSD A&S sets policy, not enforcement at contract level.
- DoD agencies only require compliance at award/contract oversight level.

References (Official CMMC v2.0 Content):

- DFARS 252.204-7021.
- CMMC Model v2.0 governance guidance.

===========

Question #:106 - [Governance and Source Documents]

Which document specifies the CMMC Level 1 practices that correspond to basic safeguarding requirements?

A. NIST SP 800-171

B. NIST SP 800-171b

C. 48 CFR 52.204-21

D. DFARS 252.204-7012

Answer: C

Explanation

CMMC Level 1 practices correspond directly to the basic safeguarding requirements for Federal Contract Information (FCI), which are codified in FAR clause 48 CFR 52.204-21. These 15 requirements form the foundation for Level 1 compliance.

Supporting Extracts from Official Content:

- 48 CFR 52.204-21: “Contractors shall apply the following 15 basic safeguarding requirements to protect Federal Contract Information (FCI).”
- CMMC Model v2.0 Overview: “Level 1 corresponds to the 15 basic safeguarding requirements in FAR 52.204-21.”

Why Option C is Correct:

- FAR 52.204-21 is the source for Level 1 practices.
- NIST SP 800-171 applies to CUI and Level 2, not Level 1.
- NIST SP 800-171b is the precursor to NIST SP 800-172 (used for Level 3).
- DFARS 252.204-7012 covers CUI safeguarding and incident reporting, not Level 1 FCI requirements.

References (Official CMMC v2.0 Content):

- FAR 48 CFR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems.
- CMMC Model v2.0, Level 1 Overview.

Question #:107 - [CMMC Assessment Process (CAP)]

A Lead Assessor is ensuring all actions have been completed to conclude a Level 2 Assessment. The final Assessment Results Package has been properly reviewed and is ready to be uploaded. What other materials is the Lead Assessor responsible for maintaining and protecting?

A. Any additional notes and information from the Assessment

B. A final assessment plan, and a Quality Control report from C3PAO

C. A final assessment plan, and a letter from the Lead Assessor explaining the process

D. A final assessment plan, a letter from the Lead Assessor explaining the results, and a Quality Control report from C3PAO

Answer: A

Explanation

The Lead Assessor is responsible for protecting and maintaining all assessment records, notes, and information gathered during the assessment process. This includes working papers and supplemental documentation that may be needed for auditability or dispute resolution.

Supporting Extracts from Official Content:

- CAP v2.0, Post-Assessment Responsibilities (§3.17): “The Lead Assessor must ensure that all assessment artifacts, notes, and information are archived or disposed of in accordance with C3PAO policy.”

Why Option A is Correct:

- The CAP specifies that notes and information from the assessment must be preserved or disposed of according to policy.
- Options B, C, and D list items not required in the CAP. The “letter” and “quality control report” are not part of the Lead Assessor’s required maintained materials.

References (Official CMMC v2.0 Content):

- CMMC Assessment Process (CAP) v2.0, Phase 3 Post-Assessment (§3.17).

===========

Question #:108 - [CMMC Model Overview]

When scoping the organizational system, the scope of applicability for the cybersecurity CUI practices applies to the components of:

A. federal systems that process, store, or transmit CUI.

B. nonfederal systems that process, store, or transmit CUI.

C. federal systems that process, store, or transmit CUI. or that provide protection for the system components.

D. nonfederal systems that process, store, or transmit CUI. or that provide protection for the system components.

Answer: D

Explanation

TheCMMC 2.0 framework applies to nonfederal systemsthat process, store, or transmitCUI.

Scoping determineswhich system components must comply with CMMC practices.

If a systemprocesses, stores, or transmits CUI, orprovides security for those systems, itmust be included in the assessment scope.

CMMC Applies to Contractors, Not Federal Systems

CMMC isdesigned for Department of Defense (DoD) contractors, notfederal systems.

Federal systems arealready governed by NIST SP 800-53and other regulations.

Scope Includes Systems That Process CUI AND Those That Protect Them

Systemsprocessing, storing, or transmitting CUIare in scope.

Systems thatprovide protection for CUI systems(e.g., firewalls, monitoring tools, security appliances) arealso in scope.

A. Federal systems that process, store, or transmit CUI.#Incorrect

CMMCdoes not apply to federal systems.

B. Nonfederal systems that process, store, or transmit CUI.#Partially correct but incomplete

Itexcludes security systemsthat protect CUI assets, whichare also in scope.

C. Federal systems that process, store, or transmit CUI, or that provide protection for the system components. #Incorrect

CMMConly applies to nonfederal systems.

CMMC Scoping Guide (Nov 2021)– Confirms that CMMCapplies to nonfederal systemsprocessingCUI.

NIST SP 800-171 Rev. 2– Specifies security requirements fornonfederal systemshandling CUI.

DFARS 252.204-7012– Requires DoD contractors to implementNIST SP 800-171onnonfederal systemshandling CUI.

Understanding Scoping in CMMC 2.0Why the Correct Answer is "D. Nonfederal systems that process, store, or transmit CUI, or that provide protection for the system components"?Why Not the Other Options?Relevant CMMC 2.0 References:Final Justification:SinceCMMC applies to nonfederal systems that process CUI or protect those systems, the correct answer isD. Nonfederal systems that process, store, or transmit CUI, or that provide protection for the system components.

Question #:109 - [CMMC Ecosystem]

Within the CMMC Ecosystem which organization ultimately will manage and oversee the training, testing, authorization, and certification of candidate assessors and instructors?

A. DoD OUSD

B. DIB Collaborative Information Sharing Environment

C. Committee on National Security Systems Instructions

D. CMMC Assessors and Instructors Certification Organization

Answer: D

Explanation

Understanding the Role of CAICO in the CMMC EcosystemTheCMMC Ecosystemconsists of multiple organizations that manage, implement, and oversee different aspects of theCybersecurity Maturity Model Certification (CMMC)program.

One of the key organizations is theCMMC Assessors and Instructors Certification Organization (CAICO), which is responsible for:

Training and certifying assessors and instructors.

Managing testing, authorization, and certificationfor CMMC professionals.

Ensuring assessors meet qualification and compliance standards.

TheCAICO is explicitly taskedwith thetraining, testing, authorization, and certification of candidate assessors and instructors.

Option A (DoD OUSD)is incorrect because theDoD Office of the Under Secretary of Defense(OUSD) provides policy oversight butdoes not handle certification of assessors.

Option B (DIB Collaborative Information Sharing Environment)is incorrect because theDIB CISfocuses on information sharing within the Defense Industrial Base, not assessor certification.

Option C (Committee on National Security Systems Instructions)is incorrect because CNSSI provides security standards butdoes not manage assessor training or certification.

CMMC Ecosystem Overview – Role of the CAICO

CMMC Assessment Process (CAP) Guide – Assessor Certification and Training

Why Option D (CAICO) is CorrectOfficial CMMC Documentation ReferencesFinal VerificationSinceCAICO is responsible for training, testing, and certifying CMMC assessors and instructors, the correct answer isOption D: CMMC Assessors and Instructors Certification Organization.

Question #:110 - [CMMC Assessment Process (CAP)]

An assessment is being conducted at a remote client site. For the duration of the assessment, the client has provided a designated hoteling space in their secure facility which consists of a desk with access to a shared printer. After noticing that the desk does not lock, a locked cabinet is requested but the client does not have one available. At the end of the day, the client provides a printout copy of an important network diagram. The diagram is clearly marked and contains CUI. What should be done NEXT to protect the document?

A. Take it with them to review in the evening.

B. Leave it on the desk for review the following day.

C. Put it in the unlocked desk drawer for review the following morning.

D. Take a picture with the personal phone before securely shredding it.

Answer: D

Explanation

Understanding CUI Handling and Storage RequirementsControlled Unclassified Information (CUI) must beprotected from unauthorized access and properly storedperCMMC 2.0 Level 2 requirementsandNIST SP 800-171 controls. Key requirements include:

NIST SP 800-171 (Requirement 3.8.3)– CUI must bephysically protectedwhen not in use.

NIST SP 800-171 (Requirement 3.1.3)– CUI access should berestricted to authorized personnel only.

DoD CUI Program Guidance– Ifproper storage (e.g., locked cabinets or controlled access areas) is unavailable, CUI should be returned to an authorized individual or secure facility.

A. Take it with them to review in the evening # Incorrect

CUI should never be removed from a secure facility unless explicitly authorizedand handled in accordance with security policies (e.g., encrypted electronic transport, secure physical storage).

B. Leave it on the desk for review the following day # Incorrect

Leaving CUI unattendedon an open desk violatesCUI physical protection requirements.

C. Put it in the unlocked desk drawer for review the following morning # Incorrect

Anunlocked drawer does not meet CUI physical security storage requirements.

D. Take a picture with the personal phone before securely shredding it # Incorrect

Storing CUI on an unauthorized personal device is a serious security violationandunauthorized reproduction of CUI is prohibited.

Why None of the Provided Answers Are Fully Correct

What Should Be Done Instead?#Return the document to the client for secure storage.

Since nosecure storage optionis available, thedocument must be returnedto the client, who should store it in anapproved secure location (e.g., a locked cabinet or classified storage area).

Theassessment team should not retain CUI unless they have an approved method of safeguarding it.

NIST SP 800-171 (Requirement 3.8.3 – Media Protection)

RequiresCUI to be physically securedwhen not in use.

DFARS 252.204-7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting)

Establishes CUIstorage and handling protections.

CMMC 2.0 Level 2 (Advanced) Requirements

Requires organizations toimplement physical security controlsto protect CUI.

DoD CUI Program Guidelines

Clearly state thatCUI must be stored in locked cabinets or controlled-access areaswhen not actively in use.

CMMC 2.0 References Supporting This Answer:

Final Answer:#None of the provided answers fully comply with CUI protection requirements.Thebest course of action is to return the document to the client for secure storage.

Question #:111 - [CMMC Assessment Process (CAP)]

In late September. CA.L2-3.12.1: Periodically assess the security controls in organizational systems to determine if the controls are effective in their application is assessed. Procedure specifies that a security control assessment shall be conducted quarterly. The Lead Assessor is only provided the first quarter assessment report because the person conducting the second quarter's assessment is currently out of the office and will return to the office in two hours. Based on this information, the Lead Assessor should determine that the evidence is;

A. sufficient, and rate the audit finding as MET

B. insufficient, and rate the audit finding as NOT MET.

C. sufficient, and re-rate the audit finding after a quarter two assessment report is examined.

D. insufficient, and re-rate the audit finding after a quarter two assessment report is examined.

Answer: B

Explanation

CA.L2-3.12.1:"Periodically assess the security controls in organizational systems to determine if the controls are effective in their application."

This control is derived fromNIST SP 800-171, Requirement 3.12.1, which mandates organizations to performregular security control assessmentsto ensure compliance and effectiveness.

Evidence Review & Assessment Timeline:

The organization's procedureexplicitly statesthat security control assessments must be conductedquarterly (every three months).

Since the Lead Assessor only has access to thefirst-quarter report, the second-quarter report is missing at the time of assessment.

CMMC Audit Requirements:

For an assessor to rate a control asMET, sufficient evidence must bereadily availableat the time of evaluation.

Since the second-quarter report is missingat the time of assessment, the Lead Assessorcannot verify compliancewith the organization's own stated frequency of assessment.

Why the Answer is NOT A, C, or D:

A (Sufficient, MET)#Incorrect: The control assessment frequency is quarterly, but the evidence for Q2 is not available. Compliance cannot be confirmed.

C (Sufficient, and re-rate later)#Incorrect: If evidence is not available during the audit, the controlcannot be rated as MET initially. There is no provision in CMMC 2.0 to "conditionally" pass a control pending future evidence.

D (Insufficient, but re-rate later)#Incorrect: Once a control is ratedNOT MET, it staysNOT METuntil a re-assessment is conducted in a new audit cycle. The assessordoes not adjust ratings retroactivelybased on future evidence.

Control Reference: CA.L2-3.12.1Assessment Criteria & Justification for the Correct Answer:

CMMC Assessment Process (CAP) Guide (2023):

"For a control to be rated as MET, the assessed organization must provide sufficient evidence at the time of the assessment."

"If evidence is missing or incomplete, the finding shall be rated as NOT MET."

NIST SP 800-171A (Security Requirement Assessment Guide):

"Evidence must be current, relevant, and sufficient to demonstrate compliance with stated periodicity requirements."

Since the procedure mandatesquarterly assessments, missing evidence means compliancecannot be validated.

DoD CMMC Scoping Guidance:

"Assessors shall base their determination on the evidence provided at the time of assessment. If required evidence is not available, the control shall be rated as NOT MET."

Official CMMC 2.0 References Supporting the Answer:

Final Conclusion:Thecorrect answer is Bbecause the required evidence (the second-quarter report) is not availableat the time of assessment, making itinsufficientto validate compliance. The Lead Assessormust rate the control as NOT METin accordance with CMMC 2.0 assessment rules.

Question #:112 - [CMMC Model Overview]

A defense contractor needs to share FCI with a subcontractor and sends this data in an email. The email system involved in this process is being used to:

A. manage FCI.

B. process FCI.

C. transmit FCI.

D. generate FCI

Answer: C

Explanation

Federal Contract Information (FCI) is defined inFAR 52.204-21as information provided by or generated for the government under contract but not intended for public release. UnderCMMC 2.0, organizations handling FCI must implementFAR 52.204-21 Basic Safeguarding Requirements, ensuring proper protection inprocessing, storing, and transmittingFCI.

Analyzing the Given OptionsThe question involves an email system that is used tosendFCI to a subcontractor. Let’s break down the possible answers:

A. Manage FCI# Incorrect

Managing FCI involves activities like organizing, storing, and maintaining access to FCI. Sending an email does not fall under management; it is an act of transmission.

B. Process FCI# Incorrect

Processing refers to actively using FCI for operational or analytical purposes, such as analyzing, modifying, or computing data. Simply sending an email does not constitute processing.

C. Transmit FCI# Correct

Transmission refers to the act of sending FCI from one entity to another. Since the contractor issendingFCI via email, this falls undertransmittingthe data.

Reference:NIST SP 800-171 Rev. 2, 3.1.3– "Control CUI (or FCI) by transmitting it using authorized mechanisms."

D. Generate FCI# Incorrect

Generating FCI means creating new contract-related information. The contractor is not creating FCI in this scenario but merely transmitting it.

Official References Supporting the Correct AnswerCMMC 2.0 Level 1 Practices (FAR 52.204-21 Basic Safeguarding Controls)

3.1.3: "Control CUI (or FCI) by transmitting it using authorized mechanisms."

This confirms that email transmission falls under"transmitting" FCI, not managing or processing.

NIST SP 800-171 Rev. 2 (Protecting CUI in Non-Federal Systems)

Requirement 3.13.8: "Implement cryptographic methods to protect CUI when transmitted."

While this applies more to CUI, FCI should also be protected during transmission, confirming that email is a form oftransmittinginformation.

ConclusionSince the contractor issendingFCI via email, the correct answer isC. Transmit FCI.This aligns withCMMC 2.0 Level 1practices underFAR 52.204-21andNIST SP 800-171, which emphasize securing transmitted data.

Question #:113 - [CMMC Model Overview]

When scoping a Level 2 assessment, which document is useful for understanding the process to successfully implement practices required for the various Levels of CMMC?

A. NISTSP 800-53

B. NISTSP 800-88

C. NISTSP 800-171

D. NISTSP 800-172

Answer: C

Explanation

CMMC 2.0 Level 2 is directly aligned withNIST Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations."Organizations seeking certification (OSC) at Level 2 must demonstrate compliance with the 110 security requirements specified inNIST SP 800-171, as mandated byDFARS 252.204-7012.

Defines the Security Requirements for Protecting CUI:

NIST SP 800-171 outlines 110 security controls that contractors must implement to protectControlled Unclassified Information (CUI)in nonfederal systems.

These controls are categorized under14 families, including access control, incident response, and risk management.

Establishes the Baseline for CMMC Level 2 Compliance:

CMMC 2.0 Level 2 assessments areentirely based on NIST SP 800-171requirements.

Every practice assessed in a Level 2 certification maps directly to a requirement fromNIST SP 800-171 Rev. 2.

Provides Guidance for Implementation & Assessment:

TheNIST SP 800-171A "Assessment Guide"provides detailed assessment objectives that guide OSCs in preparing for CMMC evaluations.

It helps define the scope of an assessment by clarifying how each control should be implemented and verified.

Referenced in CMMC and DFARS Regulations:

DFARS 252.204-7012requires contractors to implementNIST SP 800-171security requirements.

TheCMMC 2.0 Level 2modeldirectly incorporates all 110 requirementsfromNIST SP 800-171, ensuring consistency with DoD cybersecurity expectations.

A. NIST SP 800-53 ("Security and Privacy Controls for Federal Information Systems and Organizations")

This documentapplies to federal systems, not nonfederal entities handling CUI.

While it is the foundation for other security standards, it isnot the basis of CMMC Level 2assessments.

B. NIST SP 800-88 ("Guidelines for Media Sanitization")

This documentfocuses on secure data destructionand media sanitization techniques.

While data disposal is important, this standarddoes not define security controls for protecting CUI.

D. NIST SP 800-172 ("Enhanced Security Requirements for Protecting CUI")

This documentbuilds on NIST SP 800-171and applies to systems needingadvanced cybersecurity protections (e.g., targeting Advanced Persistent Threats).

It isnot required for standard CMMC Level 2 assessments, which only mandateNIST SP 800-171 compliance.

NIST SP 800-171 Rev. 2(NIST Official Site)

NIST SP 800-171A (Assessment Guide)(NIST Official Site)

CMMC 2.0 Level 2 Scoping Guide(Cyber AB)

Why NIST SP 800-171 is Essential for Level 2 Scoping:Explanation of Incorrect Answers:Key References for CMMC Level 2 Scoping:Conclusion:SinceCMMC 2.0 Level 2 assessments are based entirely on NIST SP 800-171, this document is the most relevant resource for scoping Level 2 assessments. Therefore, the correct answer is:

#C. NIST SP 800-171

Question #:114 - [CMMC Model Overview]

How does the CMMC define a practice?

A. A business transaction

B. A condition arrived at by experience or exercise

C. A series of changes taking place in a defined manner

D. An activity or activities performed to meet defined CMMC objectives

Answer: D

Explanation

Understanding the Definition of a "Practice" in CMMC 2.0In CMMC 2.0, the term"practice"refers to specific cybersecurity activities that organizations must implement to achieve compliance with defined security objectives.

Definition from CMMC Documentation:

According to theCMMC Model Overview, apracticeis defined as:

Step-by-Step Breakdown:"An activity or activities performed to meet defined CMMC objectives."

This means that practices are theactions and implementations required to protect Controlled Unclassified Information (CUI) and Federal Contract Information (FCI).

How Practices Fit into CMMC 2.0:

CMMC 2.0 Level 1 consists of17 practices, which align withFAR 52.204-21 (Basic Safeguarding of Covered Contractor Information Systems).

CMMC 2.0 Level 2 consists of110 practices, aligned directly withNIST SP 800-171 Rev. 2.

Each practice has anobjectivethat must be met to demonstrate compliance.

Official CMMC 2.0 References:

TheCMMC 2.0 Model Documentationdefines practices as "the fundamental cybersecurity activities necessary to achieve security objectives."

TheCMMC Assessment Process (CAP) Guideoutlines how assessors verify the implementation of these practices during an assessment.

TheNIST SP 800-171A Guideprovidesassessment objectivesfor each practice to ensure they are implemented effectively.

Comparison with Other Answer Choices:

A. A business transaction# Incorrect. CMMC practices focus on cybersecurity activities, not financial or operational transactions.

B. A condition arrived at by experience or exercise# Incorrect. While practices evolve over time, they are defined activities, not just experience-based conditions.

C. A series of changes taking place in a defined manner# Incorrect. A practice is a set of security actions, not just a process of change.

Conclusion:ACMMC practicerefers to specificcybersecurity activities performed to meet defined CMMC objectives. This makesOption Dthe correct answer.

Question #:115 - [CMMC Assessment Process (CAP)]

The CMMC Level 2 assessment methods include examination and can include:

A. documents, mechanisms, or activities.

B. specific hardware, software, or firmware safeguards employed within a system.

C. policies, procedures, security plans, penetration tests, and security requirements.

D. observation of system backup operations, exercising a contingency plan, and monitoring network traffic.

Answer: D

Explanation

CMMC Level 2 Assessment MethodsCMMC Level 2 assessments focus on verifying compliance withNIST SP 800-171 requirements. TheCMMC Assessment Process (CAP) Documentspecifies that assessments at this level include:

Examination– Reviewing documents, mechanisms, and activities.

Interview– Speaking with personnel to validate implementation.

Testing– Observing and verifying security controls in action.

What Does "Examination" Include?According toCMMC Assessment Methodology, examination involves reviewing:

#Documents(Policies, procedures, security plans)

#Mechanisms(Security controls, authentication systems)

#Activities(Backup operations, network monitoring, security training)

Sinceexamination includes reviewing documents, mechanisms, and activities, the correct answer isA.

B. Specific hardware, software, or firmware safeguards employed within a system.#Incorrect. While safeguardsmaybe examined, CMMC does not limit examination to only hardware, software, or firmware. The definition is broader.

C. Policies, procedures, security plans, penetration tests, and security requirements.#Incorrect. Whilesome of these itemsare examined, penetration tests arenot requiredin a CMMC Level 2 assessment.

D. Observation of system backup operations, exercising a contingency plan, and monitoring network traffic. #Incorrect. These activities fall undertesting and interviews, not just examination.

Why the Other Answers Are Incorrect

CMMC Assessment Process (CAP) Document– Defines "examination" as reviewingdocuments, mechanisms, and activities.

CMMC Official ReferencesThus,option A (documents, mechanisms, or activities) is the correct answer, as it aligns with CMMC Level 2 assessment methodology.

Question #:116 - [CMMC Model Overview]

The Assessment Team has completed Phase 2 of the Assessment Process. In conducting Phase 3 of the Assessment Process, the Assessment Team is reviewing evidence to address Limited Practice Deficiency Corrections. How should the team score practices in which the evidence shows the deficiencies have been corrected?

A. MET

B. POA&M

C. NOT MET

D. NOT APPLICABLE

Answer: A

Explanation

Understanding the CMMC Assessment Process (CAP) PhasesTheCMMC Assessment Process (CAP)consists ofthree primary phases:

Phase 1 - Planning(Pre-assessment activities)

Phase 2 - Conducting the Assessment(Evidence collection and analysis)

Phase 3 - Reporting and Finalizing Results

DuringPhase 3, the Assessment Teamreviews evidenceto confirm if anyLimited Practice Deficiency Correctionshave been successfully implemented.

Scoring Practices in Phase 3The CAP document specifies that a practice can bescored as METif:

#The deficiency identified in Phase 2 has been fully corrected before final scoring.

#Sufficient evidence is provided to demonstrate compliance with the CMMC requirement.

#The correction is notmerely plannedbutfully implemented and validatedby the assessors.

Since the evidence shows thatdeficiencies have been corrected, the correct score isMET.

B. POA&M (Plan of Action & Milestones)#Incorrect. APOA&M (Plan of Action and Milestones)is usedonly when a deficiency remains unresolved. Since the deficiency is already corrected, this option does not apply.

C. NOT MET#Incorrect. A practice is scoredNOT METonly if the deficiency hasnotbeen corrected by the end of the assessment.

D. NOT APPLICABLE#Incorrect. A practice is markedNOT APPLICABLE (N/A)only if it doesnot apply to the organization’s environment, which is not the case here.

Why the Other Answers Are Incorrect

CMMC Assessment Process (CAP) Document– Defines scoring criteria for MET, NOT MET, and POA&M.

CMMC Official ReferencesThus,option A (MET) is the correct answer, as the deficiencies have been corrected before final scoring.

Question #:117 - [Roles and Responsibilities]

Ethics is a shared responsibility between:

A. DoD and CMMC-AB.

B. OSC and sponsors.

C. CMMC-AB and members of the CMMC Ecosystem.

D. members of the CMMC Ecosystem and Lead Assessors.

Answer: C

Explanation

Understanding Ethical Responsibility in the CMMC EcosystemEthics in theCMMC ecosystemis ashared responsibilitybetween theCMMC Accreditation Body (CMMC-AB)and itsmembers. TheCMMC-AB Code of Professional Conductoutlines ethical obligations forassessors, consultants, and other ecosystem participantsto ensure integrity, fairness, and professionalism.

CMMC-AB ensures the accreditation process remains fair, unbiased, and ethical.

CMMC ecosystem members (assessors, consultants, and organizations) are responsible for upholding ethical practices in assessments and implementations.

Ethical violations can result indisciplinary actions, revocation of certification, or legal consequences.

Key Ethical Responsibilities Include:

A. DoD and CMMC-AB # Incorrect

TheDoD oversees CMMC implementation, butit is not responsible for the ethical conduct of CMMC assessments.

B. OSC and Sponsors # Incorrect

TheOrganization Seeking Certification (OSC)is responsible for compliance but doesnot oversee ethics in the CMMC ecosystem.

C. CMMC-AB and Members of the CMMC Ecosystem # Correct

Ethics is explicitly stated as ajoint responsibility of the CMMC-AB and its ecosystem membersin official CMMC guidance.

D. Members of the CMMC Ecosystem and Lead Assessors # Incorrect

Lead Assessors are part of theCMMC ecosystem, butCMMC-AB is the governing body responsible for ethical oversight.

Why is the Correct Answer "CMMC-AB and Members of the CMMC Ecosystem" (C)?

CMMC-AB Code of Professional Conduct

Defines ethical responsibilities forassessors, consultants, and ecosystem members.

CMMC Ecosystem Governance Policies

Ethics isjointly managed by CMMC-AB and its accredited ecosystem members.

CMMC Assessment Process (CAP) Document

Outlines ethical expectations forassessors and consultantsduring certification assessments.

CMMC 2.0 References Supporting this Answer:

Question #:118 - [CMMC Model Overview]

During the planning phase of a CMMC Level 2 Assessment, the Lead Assessor is considering what would constitute the right evidence for each practice. What is the Assessor attempting to verify?

A. Adequacy

B. Sufficiency

C. Process mapping

D. Assessment scope

Answer: B

Explanation

Understanding Evidence Sufficiency in CMMC Level 2 AssessmentsDuring aCMMC Level 2 Assessment, theLead Assessormust determine whether the evidence collected for each practice issufficientto support an assessment finding. This aligns with theCMMC Assessment Process (CAP) Guide, which requires assessors to evaluate:

Examinations– Reviewing documents, configurations, and system records.

Interviews– Speaking with personnel to confirm implementation and understanding.

Testing– Observing security controls in action to validate effectiveness.

To determine whether evidence issufficient, the assessor ensures that it:

Directly supports the assessment objective.

Demonstrates that the practice is consistently implemented.

Can be independently verified.

Sufficiencyrefers to whetherenoughevidence has been collected to make an accurate determination about compliance.

Option A (Adequacy)is incorrect because adequacy relates tothe qualityof evidence, while sufficiency focuses on whetherenoughevidence exists.

Option C (Process Mapping)is incorrect because process mapping is used for understanding workflows but is not an assessment verification method.

Option D (Assessment Scope)is incorrect because defining the scope happensbeforeevidence collection, during the planning phase.

CMMC Assessment Process (CAP) Guide – Section 3.6 (Determining Sufficiency of Evidence)

CMMC Level 2 Assessment Guide – Evidence Collection and Evaluation

Why Option B (Sufficiency) is CorrectOfficial CMMC Documentation ReferencesFinal VerificationSince theLead Assessor is ensuring enough evidence is available to verify compliance, the correct answer isOption B: Sufficiency.

Question #:119 - [CMMC Model Overview]

Which domain references the requirements needed to handle physical or digital assets containing CUI?

A. Media Protection (MP)

B. Physical Protection (PE)

C. System and Information Integrity (SI)

D. System and Communications Protection (SC)

Answer: A

Explanation

Understanding the Media Protection (MP) DomainTheMedia Protection (MP) domaininCMMC 2.0focuses on the security requirements needed to handlephysical or digital mediacontainingControlled Unclassified Information (CUI).

This domain includes controls for:

Protecting digital and physical mediathat store CUI.

Sanitizing and destroying mediabefore disposal or reuse.

Restricting access to CUI mediato authorized personnel only.

TheMP domaindirectly addresses the requirements for handlingCUI media, includingencryption, access control, storage, and disposal.

CMMC 2.0Level 2aligns withNIST SP 800-171, which includesMP controlsfor managing media containing CUI.

B. Physical Protection (PE)#Incorrect

PEfocuses onphysical security(e.g., facility access, visitor logs, physical barriers),not the handling of CUI on media.

C. System and Information Integrity (SI)#Incorrect

SIdeals withsystem monitoring, vulnerability management, and incident response, not media protection.

D. System and Communications Protection (SC)#Incorrect

SCcoversnetwork security, encryption, and secure communications, but does not specifically focus on media handling.

CMMC Level 2 Practice MP.3.125– Protects CUI by ensuring proper handling ofmedia containing CUI.

NIST SP 800-171 (MP Family)– Establishes security requirements for handlingdigital and physical mediacontaining CUI.

CMMC Scoping Guide (Nov 2021)– ConfirmsMP controls apply to all media that store, process, or transmit CUI.

Why the Correct Answer is "A. Media Protection (MP)"?Why Not the Other Options?Relevant CMMC 2.0 References:Final Justification:SinceMedia Protection (MP) directly addresses the handling of assets containing CUI, the correct answer isA. Media Protection (MP).

Question #:120 - [CMMC Ecosystem]

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

A. Union

B. Accord

C. Alliance

D. Agreement

Answer: D

Explanation

Understanding the Definition of an Agreement in the CMMC-AB Code of Professional ConductTheCMMC-AB Code of Professional Conductdefines anagreementasany contract between two legal entities. This includes:

#Contracts between an OSC and a C3PAOfor CMMC assessments.

#Service agreements between cybersecurity providers and defense contractors.

#Any formal, legally binding arrangement related to CMMC compliance.

A. Union # Incorrect

Auniontypically refers to anorganization representing workersand is not used to describe acontractual relationship.

B. Accord # Incorrect

While anaccordcan mean an agreement, it isnot the standard legal term for a binding contractin CMMC documentation.

C. Alliance # Incorrect

Analliancerefers to astrategic partnership, but does not necessarily imply alegally binding contract.

D. Agreement # Correct

TheCMMC-AB Code of Professional Conductdefines anagreementas anylegally binding contract between two entities.

Why is the Correct Answer "D. Agreement"?

CMMC-AB Code of Professional Conduct

Defines"Agreement"as alegally binding contract between two parties.

CMMC-AB Licensed Training and Assessment Provider Guidelines

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

DFARS and CMMC Certification Contracts

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

CMMC 2.0 References Supporting This Answer:

Question #:121 - [Governance and Source Documents]

What is the BEST description of the purpose of FAR clause 52 204-21?

A. It directs all covered contractors to install the cyber security systems listed in that clause.

B. It describes all of the safeguards that contractors must take to secure covered contractor IS.

C. It describes the minimum standard of care that contractors must take to secure covered contractor IS.

D. It directs covered contractors to obtain CMMC Certification at the level equal to the lowest requirement of their contracts.

Answer: C

Explanation

Understanding FAR Clause 52.204-21TheFederal Acquisition Regulation (FAR) Clause 52.204-21is titled" Basic Safeguarding of Covered Contractor Information Systems."This clause establishesminimum cybersecurity requirementsforfederal contractorsthat handleFederal Contract Information (FCI).

Key Purpose of FAR Clause 52.204-21Theprimary objectiveof FAR 52.204-21 is to ensure that contractors applybasic cybersecurity protectionsto theirinformation systemsthat process, store, or transmitFCI. Theseminimum safeguarding requirementsserve as abaseline security standardfor contractors doing business with theU.S. government.

FAR 52.204-21 doesnotrequire contractors to install specific cybersecurity tools (eliminating option A).

Itoutlines only the minimum safeguards, notallcybersecurity controls needed for complete security (eliminating option B).

CMMC certification isnotmandated by this clause alone (eliminating option D).

Instead, it establishesa baseline "standard of care"that all federal contractorsmust followto protectFCI(making option C correct).

Why "Minimum Standard of Care" is Correct?Breakdown of Answer ChoicesOption

Description

Correct?

A. It directs all covered contractors to install the cybersecurity systems listed in that clause.

#Incorrect–The clause doesnotspecify tools or require specific cybersecurity systems.

B. It describes all of the safeguards that contractors must take to secure covered contractor IS.

#Incorrect–It only setsminimumrequirements, notall possiblesecurity measures.

C. It describes the minimum standard of care that contractors must take to secure covered contractor IS.

#Correct – The clause defines basic safeguards as a minimum security standard.

D. It directs covered contractors to obtain CMMC Certification at the level equal to the lowest requirement of their contracts.

#Incorrect–FAR 52.204-21 doesnot mandateCMMC certification; that requirement comes from DFARS 252.204-7012 and 7021.

Minimum Safeguarding Requirements Under FAR 52.204-21The clause defines15 basic security controls, which align withCMMC Level 1. Some examples include:

#Access Control– Limit access to authorized users.

#Identification & Authentication– Authenticate system users.

#Media Protection– Sanitize media before disposal.

#System & Communications Protection– Monitor and control network connections.

FAR 52.204-21– Establishes thebasic safeguarding requirementsfor FCI.

CMMC 2.0 Level 1– Directly aligns withFAR 52.204-21 controls.

Official References from CMMC 2.0 and FAR DocumentationFinal Verification and ConclusionThe correct answer isC. It describes the minimum standard of care that contractors must take to secure covered contractor IS.This aligns withFAR 52.204-21 requirementsas abaseline security standard for FCI.

Question #:122 - [CMMC Model Overview]

Which statement BEST describes a LTP?

A. Creates DoD-licensed training

B. Instructs a curriculum approved by CMMC-AB

C. May market itself as a CMMC-AB Licensed Provider for testing

D. Delivers training using some CMMC body of knowledge objectives

Answer: B

Explanation

Understanding Licensed Training Providers (LTPs) in CMMCALicensed Training Provider (LTP)is an entity that is authorized by theCybersecurity Maturity Model Certification Accreditation Body (CMMC-AB) todeliver CMMC trainingbased on anapproved curriculum.

Provides CMMC-AB-approved training programsfor individuals seeking CMMC certifications.

Uses an official CMMC curriculumthat aligns with theCMMC Body of Knowledge (BoK)and other CMMC-AB guidance.

Prepares students for CMMC roles, such asCertified CMMC Assessors (CCA) and Certified CMMC Professionals (CCP).

Key Responsibilities of an LTP:

A. Creates DoD-licensed training # Incorrect

TheCMMC-AB, not the DoD, manages LTP licensing. LTPsdo not create new training contentbut mustfollow an approved curriculum.

B. Instructs a curriculum approved by CMMC-AB # Correct

LTPsteacha curriculum that has beenapproved by the CMMC-AB, ensuring consistency in CMMC training.

C. May market itself as a CMMC-AB Licensed Provider for testing # Incorrect

LTPs provide training, not testing. Testing is handled byLicensed Partner Publishers (LPPs)and exam bodies.

D. Delivers training using some CMMC body of knowledge objectives # Incorrect

LTPs mustfully adhereto theCMMC-AB-approved curriculum, not just "some" objectives.

Why is the Correct Answer "Instructs a curriculum approved by CMMC-AB" (B)?

CMMC-AB Licensed Training Provider (LTP) Program Guidelines

Defines LTPs as entities thatdeliver CMMC-AB-approved training programs.

CMMC Body of Knowledge (BoK)

Specifies that training must follow theCMMC-AB-approved curriculumto ensure standardization.

CMMC-AB Training & Certification Framework

Requires LTPs todeliver structured training that meets CMMC-AB guidelines.

CMMC 2.0 References Supporting This Answer:

Final Answer:#B. Instructs a curriculum approved by CMMC-AB

Question #:123 - [Governance and Source Documents]

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

A. DOD OUSD

B. Authorized holder

C. Information Disclosure Official

D. Presidentially authorized Original Classification Authority

Answer: B

Explanation

DoDI 5200.48 specifies that Authorized Holders of CUI are responsible for applying appropriate CUI markings. An authorized holder is an individual who has lawful government purpose access to the information. This ensures that responsibility for correctly marking information rests with those who create or handle the material, not only with original classification authorities (which apply to classified information, not CUI).

Reference Documents:

- DoDI 5200.48, Controlled Unclassified Information (CUI)

Question #:124 - [Implementation and Scoping]

An organization's sales representative is tasked with entering FCI data into various fields within a spreadsheet on a company-issued laptop. This laptop is an FCI Asset being used to:

A. process and transmit FCI.

B. process and organize FCI.

C. store, process, and transmit FCI.

D. store, process, and organize FCI.

Answer: C

Explanation

Understanding FCI and Asset CategorizationFederal Contract Information (FCI)is any informationnot intended for public releasethat is provided by or generated for thegovernmentunder aDoD contract.

Acompany-issued laptopused by a sales representative to enter FCI into aspreadsheetis considered anFCI assetbecause it:

#Stores FCI– The spreadsheet contains sensitive information.

#Processes FCI– The representative is entering data into the spreadsheet.

#Organizes FCI– The spreadsheet helps structure and manage FCI data.

Processing (Option B and C)is occurring, but since the laptop is primarily being used toorganize data,Option D is the most comprehensive.

Transmission (Option A and C)is not explicitly mentioned, soOption D is the best fit.

Why "Store, Process, and Organize FCI" is Correct?Breakdown of Answer ChoicesOption

Description

Correct?

A. Process and transmit FCI.

#Incorrect–No indication oftransmissionis provided.

B. Process and organize FCI.

#Incorrect–Storage is also a key function of the laptop.

C. Store, process, and transmit FCI.

#Incorrect–Transmission is not confirmed in the scenario.

D. Store, process, and organize FCI.

#Correct – The laptop is used to store, process, and organize FCI in a spreadsheet.

CMMC Asset Categorization Guidelines– DefinesFCI assetsbased onstorage, processing, and organization functions.

Official References from CMMC 2.0 DocumentationFinal Verification and ConclusionThe correct answer isD. Store, process, and organize FCI, as the laptop is used tostore information, enter (process) data, and structure (organize) FCI within a spreadsheet.

Question #:125 - [CMMC Ecosystem]

A CMMC Level 1 Self-Assessment identified an asset in the OSC's facility that does not process, store, or transmit FCI. Which type of asset is this considered?

A. FCI Assets

B. Specialized Assets

C. Out-of-Scope Assets

D. Government-Issued Assets

Answer: C

Explanation

The Cybersecurity Maturity Model Certification (CMMC) 2.0 framework categorizes assets based on their interaction with Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). In a CMMC Level 1 self-assessment, assets are classified based on whether they process, store, or transmit FCI.

FCI Assets– These assets process, store, or transmit FCI and must meet CMMC Level 1 security requirements (17 practices from FAR 52.204-21).

CUI Assets– These assets handle Controlled Unclassified Information (CUI) and are subject to CMMC Level 2 requirements, aligned with NIST SP 800-171.

Specialized Assets– Includes IoT devices, Operational Technology (OT), Government-Furnished Equipment (GFE), and test equipment. These are often categorized separately due to their specific cybersecurity requirements.

Out-of-Scope Assets– Assets that do not process, store, or transmit FCI or CUI. These do not require compliance with CMMC practices.

Government-Issued Assets– These are assets provided by the government for contract-specific purposes, often requiring compliance based on government policies.

The question specifies that the identified assetdoes not process, store, or transmit FCI.

According to CMMC 2.0 guidelines,only assets that handle FCI or CUI are subject to security controls.

Assets that are physically located within an OSC’s facility but do not interact with FCI or CUI fall into the" Out-of-Scope Assets"category.

These assets do not require CMMC-specific cybersecurity controls, as they have no impact on the security of FCI or CUI.

CMMC Scoping Guide (Nov 2021)– Definesout-of-scope assetsas those that are within an OSC’s environment but have no interaction with FCI or CUI.

CMMC 2.0 Level 1 Guide– Only requires security controls on FCI assets, meaning assets that do not process, store, or transmit FCI are out of scope.

CMMC Assessment Process (CAP) Guide– Identifies the classification of assets in an OSC’s environment to determine compliance requirements.

Asset Categories as per CMMC 2.0:Why the Correct Answer is C. Out-of-Scope Assets?Relevant CMMC 2.0 References:Final Justification:Since the assetdoes not process, store, or transmit FCI, it does not fall under "FCI Assets" or "Specialized Assets." It is also not a government-issued asset. Therefore, the correct classification under CMMC 2.0 isOut-of-Scope Assets (C).

Question #:126 - [CMMC Model Overview]

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

A. Level 1.

B. Level 3.

C. Levels 1 and 2.

D. Levels 1,2, and 3.

Answer: D

Explanation

Understanding Access Control (AC) in CMMC Advanced (Level 3)TheCMMC Advanced Level (Level 3)is designed for organizations handlinghigh-value Controlled Unclassified Information (CUI)and aligns with a subset ofNIST SP 800-172for advanced cybersecurity protections.

Access Control (AC) Practices in CMMC Level 3#CMMC Level 1 includesbasic AC practices fromFAR 52.204-21(e.g., restricting access to authorized users).

#CMMC Level 2 includesallAccess Control (AC) practices from NIST SP 800-171(e.g., managing privileged access).

#CMMC Level 3 expands on Levels 1 and 2, incorporatingadditional protections from NIST SP 800-172, such as enhanced monitoring and adversary deception techniques.

CMMC Level 3 builds upon all previous levels, includingAccess Control (AC) practices from Levels 1 and 2.

Options A, B, and C are incorrectbecause Level 3 includesallprevious AC practices fromLevels 1 and 2, plus additional ones.

Why "Levels 1, 2, and 3" is Correct?Breakdown of Answer ChoicesOption

Description

Correct?

A. Level 1

#Incorrect–Level 3 includes AC practices fromLevels 1 and 2, not just Level 1.

B. Level 3

#Incorrect – Level 3 builds onLevels 1 and 2, not just Level 3 practices.

C. Levels 1 and 2

#Incorrect–Level 3 containsadditionalAC practices beyond Levels 1 and 2.

D. Levels 1, 2, and 3

#Correct – Level 3 contains all AC practices from Levels 1 and 2, plus additional ones.

CMMC Model Framework– Outlines howLevel 3 builds upon Level 1 and 2 practices.

NIST SP 800-172– Definesadvanced cybersecurity controlsrequired inCMMC Level 3.

Official References from CMMC 2.0 DocumentationFinal Verification and ConclusionThe correct answer isD. Levels 1, 2, and 3, as CMMC Level 3 includesAccess Control (AC) practices from all previous levels plus additional enhancements.

Question #:127 - [CMMC Assessment Process (CAP)]

When assessing SI.L2-3.14.6: Monitor communications for attack, the CCA interviews the person responsible for the intrusion detection system and examines relevant policies and procedures for monitoring organizational systems. What would be a possible next step the CCA could conduct to gather sufficient evidence?

A. Conduct a penetration test

B. Interview the intrusion detection system's supplier.

C. Upload known malicious code and observe the system response.

D. Review an artifact to check key references for the configuration of the IDS or IPS practice for additional guidance on intrusion detection and prevention systems.

Answer: D

Explanation

Understanding SI.L2-3.14.6: Monitor Communications for AttacksThe practiceSI.L2-3.14.6fromNIST SP 800-171(aligned with CMMC Level 2) requires an organization tomonitor organizational communications for indicators of attack. This typically includes:

#Intrusion Detection Systems (IDS)andIntrusion Prevention Systems (IPS)

#Log analysis and network monitoring

#Incident response planningfor detected threats

As part of aCMMC Level 2 assessment, theCertified CMMC Assessor (CCA)must ensure that theOSC (Organization Seeking Certification)hasproperly implemented and documenteditsmonitoring capabilities.

TheCCA must collect sufficient objective evidenceto determine compliance.

Reviewing anartifact(such as system configurations, IDS/IPS logs, or security policies)helps validatethat intrusion detection is properly implemented.

Configuration settings providedirect evidenceof whethermonitoring for attacksis effectively applied.

Why "Review an artifact to check key references for the configuration of the IDS or IPS" is Correct? Breakdown of Answer ChoicesOption

Description

Correct?

A. Conduct a penetration test

#Incorrect–Penetration testing isnot requiredfor CMMC Level 2 assessments and falls outside an assessor's responsibilities.

B. Interview the intrusion detection system's supplier.

#Incorrect–Thesupplier does not determine compliance; the assessor needs evidence from theOSC’s implementation.

C. Upload known malicious code and observe the system response.

#Incorrect–This would beinvasive testing, which isnot part of a CMMC assessment.

D. Review an artifact to check key references for the configuration of the IDS or IPS practice for additional guidance on intrusion detection and prevention systems.

#Correct – Reviewing system artifacts provides direct evidence of compliance with SI.L2-3.14.6.

NIST SP 800-171 SI.L2-3.14.6– Requires monitoring communications for attack indicators.

CMMC Assessment Process Guide (CAP)– Describesartifact reviewas an essential assessment method.

Official References from CMMC 2.0 and NIST SP 800-171 DocumentationFinal Verification and ConclusionThe correct answer isD. Review an artifact to check key references for the configuration of the IDS or IPS practice for additional guidance on intrusion detection and prevention systems.

This aligns withCMMC 2.0 Level 2 assessment requirementsandSI.L2-3.14.6 compliance verification.

Question #:128 - [CMMC Ecosystem]

A C3PAO has completed a Limited Practice Deficiency Correction Evaluation following an assessment of an OSC. The Lead Assessor has recommended moving deficiencies to a POA&M. but the OSC will remain on an Interim Certification. What is the MINIMUM number of practices that must be scored as MET to initiate this course of action?

A. 80 practices

B. 88 practices

C. 100 practices

D. 110 practices

Answer: C

Explanation

TheLimited Practice Deficiency Correction Evaluationprocess occurs when anOrganization Seeking Certification (OSC)has undergone aCMMC Level 2 Assessmentby aCertified Third-Party Assessment Organization (C3PAO)and hasunresolved deficienciesin some security practices.

According toCMMC 2.0 policy and DFARS 252.204-7021, OSCs can still achieveInterim Certificationif they meet theminimum thresholdof security practices while addressing deficiencies through aPlan of Action & Milestones (POA&M).

TheCMMC 2.0 Interim Rulestates that an OSCmust meet at least 100 out of 110 practicesto qualify for aPOA&M-based remediation.

A maximum of 10 practices can be listed in the POA&Mfor later correction.

Failure to meet at least 100 practices results in failing the assessment outright, requiring a full reassessment after remediation.

The Lead Assessor can recommend POA&M placementonly if the OSC meets at least 100 practices.

Less than 100 practices scored as MET means the OSC does not qualify for a POA&Mand mustretest completely.

DFARS 252.204-7021 and CMMC 2.0 policiesconfirm the100-practice thresholdfor conditional certification.

A. 80 practices (Incorrect)– Falls well below the 100-practice requirement.

B. 88 practices (Incorrect)– Still below the POA&M eligibility threshold.

D. 110 practices (Incorrect)– While meeting 110 practices would be ideal,CMMC allows a POA&M option at 100 practices.

The correct answer isC. 100 practices, as this meets theminimum threshold for POA&M-based Interim Certification.

References:

DFARS 252.204-7021 (CMMC Requirement Clause)

CMMC 2.0 Assessment Process (CAP) Guide

DoD CMMC 2.0 Policy Overview

Question #:129 - [Roles and Responsibilities]

Which are guiding principles in the CMMC Code of Professional Conduct?

A. Objectivity, information integrity, and higher accountability

B. Objectivity, information integrity, and proper use of methods

C. Proper use of methods, higher accountability, and objectivity

D. Proper use of methods, higher accountability, and information integrity

Answer: A

Explanation

The CMMC Code of Professional Conduct applies to all CMMC assessors, practitioners, and ecosystem participants. Its guiding principles are: Objectivity, Information Integrity, and Higher Accountability.

Supporting Extracts from Official Content:

- CMMC Code of Professional Conduct: “Guiding principles… include Objectivity, Information Integrity, and Higher Accountability.”

Why Option A is Correct:

- These three principles are the official guiding values documented in the Code of Professional Conduct.
- Options B, C, and D insert terms (“proper use of methods”) that are not part of the official guiding principles.

References (Official CMMC v2.0 Content):

- CMMC Code of Professional Conduct.

===========

Question #:130 - [CMMC Model Overview]

At which CMMC Level do the Security Assessment (CA) practices begin?

A. Level 1

B. Level 2

C. Level 3

D. Level 4

Answer: B

Explanation

Step 1: Understand the “CA” Domain – Security AssessmentTheCA (Security Assessment)domain includes practices related to:

Planning security assessments,

Performing periodic reviews,

Managing plans of action and milestones (POA&Ms).

These practices derive fromNIST SP 800-171, specifically:

CA.2.157– Develop, document, and periodically update security plans,

CA.2.158– Periodically assess security controls,

CA.2.159– Develop and implement POA&Ms.

Level 1 (Foundational):

Implements only the17 practicesfromFAR 52.204-21

Doesnot include the CA domain

Level 2 (Advanced):

Implements110 practicesfromNIST SP 800-171, including CA.2.157–159

First levelwhereSecurity Assessment (CA)practices are required

Level 3:

Not yet finalized but intended to include selected controls fromNIST SP 800-172

#Step 2: Review CMMC Levels

A. Level 1# No CA domain practices are present at Level 1.

C. Level 3 / D. Level 4# These levels build on CA practices but do not represent thestarting point.

#Why the Other Options Are Incorrect

TheSecurity Assessment (CA)domain practices begin atCMMC Level 2, as part of the implementation ofNIST SP 800-171.

Question #:131 - [CMMC Assessment Process (CAP)]

Which code or clause requires that a contractor is meeting the basic safeguarding requirements for FCI during a Level 1 Self-Assessment?

A. FAR 52.204-21

B. 22CFR 120-130

C. DFARS 252.204-7011

D. DFARS 252.204-7021

Answer: A

Explanation

1. Understanding Basic Safeguarding Requirements for FCI in CMMC Level 1

Federal Contract Information (FCI) is defined as information provided by or generated for the government under a contract that isnot intended for public release.

CMMCLevel 1is designed to ensurebasic safeguardingof FCI, aligning with15 security requirementsfound inFAR 52.204-21 (Basic Safeguarding of Covered Contractor Information Systems).

Contractors handlingonly FCImust meetCMMC Level 1, which alignsdirectlywith the safeguarding requirements set inFAR 52.204-21.

2. FAR 52.204-21 and Its Role in CMMC Level 1 Compliance

FAR 52.204-21establishes the baseline cybersecurity controls that contractors must implement to protectFCI.

The15 basic safeguarding requirementsinclude:

Limiting information accessto authorized users.

Identifying and authenticating usersbefore allowing system access.

Protecting transmitted FCIfrom unauthorized disclosure.

Monitoring and controlling connectionsto external systems.

Applying boundary protectionand cybersecurity measures.

Sanitizing mediabefore disposal.

Updating security configurationsto reduce vulnerabilities.

Providing physical securityprotections.

Controlling physical accessto systems that process FCI.

Enforcing multi-factor authentication (MFA) where applicable.

Patching vulnerabilitiesin software and hardware.

Limiting the use of removable media.

Creating and retaining system audit logs.

Performing risk-based security assessments.

Developing an incident response plan.

These 15 practices form thefoundationof CMMCLevel 1 Self-Assessment, ensuring contractorsmeet minimum cybersecurity expectationsfor handling FCI.

3. Why the Other Options Are Incorrect

B. 22 CFR 120-130:

This refers toInternational Traffic in Arms Regulations (ITAR), which controls the export of defense-related articles and services,notFCI safeguarding requirements.

C. DFARS 252.204-7011:

This clause refers toalternative line item structuresand does not pertain to cybersecurity or safeguarding FCI.

D. DFARS 252.204-7021:

This clause enforcesCMMC requirementsbut doesnot definebasic safeguarding controls. It requires compliance with CMMC but does not specify the foundational requirements (which come fromFAR 52.204-21for Level 1).

4. Official CMMC 2.0 Reference & Study Guide Alignment

TheCMMC 2.0 model documentationconfirms that Level 1 is focused on the15 practices from FAR 52.204-21.

TheDoD’s official CMMC Assessment Guidefor Level 1 explicitly states that meeting FAR 52.204-21 is therequirement for passing a Level 1 Self-Assessment.

TheCMMC 2.0 Scoping Guideclarifies that contractors handling onlyFCIand seekingLevel 1 certificationmust implementonly FAR 52.204-21security controls.

Final Confirmation:The correct answer isA. FAR 52.204-21, as it directly governs the basic safeguarding ofFCIand is the foundational requirement for aLevel 1 Self-Assessmentin CMMC 2.0.

Question #:132 - [CMMC Assessment Process (CAP)]

A Lead Assessor and an OSC's Assessment Official have agreed to have the Assessment results presented during the final Daily Checkpoint of the OSC's CMMC Level 2 Assessment. Which document MUST the Lead Assessor use to present assessment findings to the OSC?

A. CMMC POA&M Brief

B. CMMC Findings Brief

C. CMMC Assessment Tracker Tool

D. CMMC Recommended Findings template

Answer: B

Explanation

According to the CMMC Assessment Process (CAP), the Lead Assessor must use the CMMC Findings Brief to formally present assessment results to the Organization Seeking Certification (OSC). The Findings Brief ensures consistency across assessments and provides the OSC with an official, standardized presentation of results, including observed strengths, weaknesses, and any non-conformities.

Other options are incorrect because:

- POA&M Brief is not part of the official CAP presentation.
- CMMC Assessment Tracker Tool is an internal tool used by assessors, not for presentation to the OSC.

- Recommended Findings template is not a recognized deliverable in CAP.

Reference Documents:

- CMMC Assessment Process (CAP), v1.0

Question #:133 - [CMMC Model Overview]

During an assessment, which phase of the process identifies conflicts of interest?

A. Analyze requirements.

B. Develop assessment plan.

C. Verify readiness to conduct assessment.

D. Generate final recommended assessment results.

Answer: C

Explanation

In the CMMC assessment process, conflicts of interest must be identified early to ensure an impartial and objective evaluation of an organization's compliance with CMMC 2.0 requirements. The appropriate phase for identifying conflicts of interest is during the"Verify Readiness to Conduct Assessment"phase.

Assessment Planning & Conflict of Interest Consideration

Before an assessment begins, theC3PAO (Certified Third-Party Assessment Organization)or theDIBCAC (Defense Industrial Base Cybersecurity Assessment Center) for DOD-led assessmentsmust confirm that there are no conflicts of interest between assessors and the organization being assessed.

A conflict of interest may arise if an assessor haspreviously worked for, consulted with, or provided direct assistance tothe organization under review.

CMMC Assessment Process and PhasesThe CMMC assessment process involves multiple steps, and the verification of readiness is acritical early phaseto ensure that the assessment is unbiased:

Analyze Requirements:This phase focuses on defining the assessment scope, but it does not include conflict of interest verification.

Develop Assessment Plan:This phase focuses on structuring the assessment methodology, not on identifying conflicts.

Verify Readiness to Conduct Assessment (Correct Answer):

At this stage, theC3PAO or assessment team must review potential conflicts of interest.

TheDefense Industrial Base Cybersecurity Assessment Center (DIBCAC)also ensures assessors do not have any prior relationships that could compromise the objectivity of the evaluation.

Generate Final Recommended Assessment Results:This phase occurs at the end of the process, after the assessment is complete, so conflict of interest identification is too late by this stage.

Official CMMC Documentation & References

CMMC Assessment Process (CAP) Guide– The CAP details procedures assessors must follow, including conflict of interest verification.

CMMC 2.0 Scoping and Assessment Guides– Published by the Cyber AB and DoD, these guides reinforce the need for impartiality and independence in assessments.

DoD Instruction 5200.48 (Controlled Unclassified Information Program)– Outlines requirements for ensuring objective cybersecurity assessments.

Step-by-Step Explanation:By ensuring conflicts of interest are identified in the"Verify Readiness to Conduct Assessment"phase, the integrity of the CMMC certification process is maintained, ensuring that assessments are conductedfairly, independently, and in accordance with DoD cybersecurity policies.

Question #:134 - [CMMC Assessment Process (CAP)]

In scoping a CMMC Level 1 Self-Assessment, it is determined that an ESP employee has access to FCI. What is the ESP employee considered?

A. In scope

B. Out of scope

C. OSC point of contact

D. Assessment Team Member

Answer: A

Explanation

Federal Contract Information (FCI)is any informationnot intended for public releasethat is provided or generated under aU.S. Government contracttodevelop or deliver a product or service.

Enhanced Security Personnel (ESP)refers to employees, contractors, or third parties whohave access to FCIwithin anOrganization Seeking Certification (OSC).

UnderCMMC 2.0 Scoping Guidance, anypersonnel, system, or asset with access to FCI is considered in scopefor a CMMC Level 1 assessment.

Since theESP employee has access to FCI, theymustbe included in the assessment scope.

Option B (Out of scope)is incorrect because anyone with access to FCI is automatically considered part of theCMMC Level 1 boundary.

Option C (OSC point of contact)is incorrect because thepoint of contactis typically an administrative or compliance representative, not necessarily someone with FCI access.

Option D (Assessment Team Member)is incorrect because anESP employee is not part of the assessment team but rather a subject of the assessment.

CMMC Level 1 Scoping Guide, Section 2 – Defining Scope for FCI

CMMC Assessment Process (CAP) Guide – Roles and Responsibilities

Federal Acquisition Regulation (FAR) 52.204-21(Basic Safeguarding of FCI)

Understanding Scoping in CMMC Level 1 Self-AssessmentsWhy Option A (In scope) is CorrectOfficial CMMC Documentation ReferencesFinal VerificationSince theESP employee has access to FCI, they are consideredin scopefor the CMMC Level 1 self-assessment, makingOption A the correct answer.

Question #:135 - [Roles and Responsibilities]

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

Question #:136 - [CMMC Assessment Process (CAP)]

Which statement is NOT a measure to determine if collected evidence is sufficient?

A. Evidence covers the sampled organization

B. Evidence is not required if the practice is ISO certified

C. Evidence covers the model scope of the Assessment (Target CMMC Level)

D. Evidence corresponds to the sampled organization in the evidence collection approach

Answer: B

Explanation

The CMMC Assessment Process (CAP) requires that sufficient evidence must:

- Cover the sampled organization,
- Cover the defined model scope of the assessment (Target CMMC Level), and
- Correspond to the evidence collection approach.

Evidence is always required, even if the organization holds other certifications such as ISO. External certifications cannot replace CMMC evidence requirements. Thus, the statement that “Evidence is not required if the practice is ISO certified” is not valid.

Reference Documents:

- CMMC Assessment Process (CAP), v1.0

Question #:137 - [CMMC Model Overview]

During the assessment process, who is the final interpretation authority for recommended findings?

A. C3PAO

B. CMMC-AB

C. OSC sponsor

D. Assessment Team Members

Answer: B

Explanation

Final Interpretation Authority in the CMMC Assessment ProcessDuring aCMMC Level 2 assessment, several entities are involved in the process, including theOrganization Seeking Certification (OSC), Certified Third-Party Assessment Organization (C3PAO), Assessment Team Members, and the CMMC Accreditation Body (CMMC-AB).

Role of the C3PAO and Assessment Team:

TheCertified Third-Party Assessment Organization (C3PAO)is responsible for conducting the assessment and makinginitial recommended findingsbased on NIST SP 800-171 security requirements.

Assessment Team Members(Lead Assessor and support staff) conduct evaluations and submit theirrecommendationsto the C3PAO.

Final Interpretation Authority – CMMC-AB:

TheCMMC Accreditation Body (CMMC-AB)is responsible for ensuring consistency and accuracy in assessments.

If there is any dispute or need for clarification regarding findings, CMMC-AB provides the final interpretation and guidance.

This ensures uniformity in certification decisions across different C3PAOs.

Why CMMC-AB is the Correct Answer:

CMMC-AB has the ultimate authority over thequality assurance processfor assessments.

It reviewsremediation requests, challenges, or disputesfrom the OSC or C3PAO and makes final determinations.

The CMMC-AB maintains oversight to ensure assessmentsalign with CMMC 2.0 policies and DFARS 252.204-7021 requirements.

A. C3PAO– The C3PAO conducts the assessment and submits findings, butit does not have the final interpretation authority. Findings must pass through theCMMC-AB quality assurance process.

C. OSC Sponsor– The OSC (Organization Seeking Certification)cannot interpret findings; they can only respond to identified deficiencies and appeal assessments through CMMC-AB channels.

D. Assessment Team Members– The assessment teamrecommends findingsbut does not make final interpretations. Their role is limited to conducting evaluations, collecting evidence, and submitting reports to the C3PAO.

References:CMMC Assessment Process Guide (CAP v2.0)–Cyber AB

DFARS 252.204-7021(DoD Regulation on CMMC Requirements)

CMMC 2.0 Model Overview(DoD CIO Site)

#Final Answer: B. CMMC-AB

Question #:138 - [CMMC Model Overview]

The evidence needed for each practice and/or process is weight for:

A. adequacy and sufficiency.

B. adequacy and thoroughness.

C. sufficiency and thoroughness.

D. sufficiency and appropriateness.

Answer: A

Explanation

During aCMMC assessment, organizations must provide evidence to demonstrate compliance with requiredpractices and processes. Assessors evaluate this evidence based on two key criteria:

Adequacy– Does the evidence meet the intent of the security requirement?

Sufficiency– Is there enough evidence to reasonably conclude that the practice/process is effectively implemented?

These principles are outlined in theCMMC Assessment Process Guide, which provides a structured approach for evaluating compliance.

Step-by-Step Breakdown:#1. Adequacy – Does the evidence fully meet the requirement?

Adequacyrefers to whether the evidence properly demonstrates that the security practice has been implemented as required.

Example: If an organization claims to enforceMulti-Factor Authentication (MFA), an assessor would checksystem configurations, login policies, and user authentication logsto confirm that MFA is actually in use.

#2. Sufficiency – Is there enough evidence to support the claim?

Sufficiencymeans that there isenough supporting evidenceto prove compliance.

Example: If an organization providesonly one screenshot of an MFA login screen, that alone may not besufficient—additional logs, policies, and user records would help strengthen the case.

(B) Adequacy and Thoroughness#

Thoroughnessis not a defined metric in CMMC evidence evaluation.

The focus is onwhether the evidence meets the requirement (adequacy)and if there isenough of it (sufficiency).

(C) Sufficiency and Thoroughness#

Thoroughnessis not a recognized term in CMMC compliance validation.

Evidence must beadequate and sufficient, not just thorough.

(D) Sufficiency and Appropriateness#

Appropriatenessis not a CMMC-defined criterion.

Thecorrect terms used in CMMC assessmentsareAdequacy(Does it meet the requirement?) andSufficiency(Is there enough proof?).

Why the Other Answer Choices Are Incorrect:

CMMC Assessment Process Guideexplicitly states that evidence must be evaluated based onadequacyandsufficiencyto confirm compliance with security practices.

Final Validation from CMMC Documentation:

Question #:139 - [CMMC Model Overview]

Two network administrators are working together to determine a network configuration in preparation for CMMC. The administrators find that they disagree on a couple of small items. Which solution is the BEST way to ensure compliance with CMMC?

A. Consult with the CEO of the company.

B. Consult the CMMC Assessment Guides and NIST SP 800-171.

C. Go with the network administrator's ideas with the least stringent controls.

D. Go with the network administrator's ideas with the most stringent controls.

Answer: B

Explanation

When preparing forCMMC compliance, organizations must ensure that theirnetwork configurations align with required cybersecurity controls. Ifnetwork administratorsdisagree on certain configurations, the mostobjective and accurateway to resolve the disagreement is by referencingofficial CMMC guidanceandNIST SP 800-171 requirements, which form the foundation of CMMC Level 2.

CMMC Assessment Guides as the Primary Reference

TheCMMC Assessment Guides (Level 1 & Level 2)provide clearinterpretationsof security practices.

Theyexplain how each practice should be implemented and assessedduring certification.

NIST SP 800-171 as the Compliance Baseline

CMMC Level 2is based directly onNIST SP 800-171, which outlines the110 security controlsrequired for protectingControlled Unclassified Information (CUI).

Network configurations must complywith NIST-defined security requirements, including:

Access Control (AC) – Ensuring least privilege principles.

Audit and Accountability (AU) – Logging and monitoring network activity.

System and Communications Protection (SC) – Secure network design and encryption.

Why the Other Answer Choices Are Incorrect:

(A) Consult with the CEO of the company:

ACEO is not necessarily a cybersecurity expertand may not be familiar with CMMC technical requirements.

Technical compliance decisions should be based onCMMC and NISTframeworks, not executive opinions.

(C) Go with the network administrator's ideas with the least stringent controls:

Choosingless stringent controls increases security riskand could lead toCMMC non-compliance.

(D) Go with the network administrator's ideas with the most stringent controls:

While security is important,more stringent controlsmay introduceoperational inefficienciesorunnecessary coststhat are not required for compliance.

The correct approach is to implement what is required by CMMC and NIST SP 800-171, no more and no less.

TheCMMC Assessment GuidesandNIST SP 800-171 Rev. 2areofficial sourcesthat provide the most reliable guidance on compliance.

CMMC Level 2 is entirely based on NIST SP 800-171, making it the definitive source for resolving security disagreements.

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

B. Consult the CMMC Assessment Guides and NIST SP 800-171.

Question #:140 - [CMMC Assessment Process (CAP)]

How are the Final Recommended Assessment Findings BEST presented?

A. Using the CMMC Findings Brief template

B. Using a C3PAO-provided template that is preferred by the OSC

C. Using a C3PAO-branded version of the CMMC Findings Brief template

D. Using the proprietary template created by the Lead Assessor after approval from the C3PAO

Answer: A

Explanation

In the Cybersecurity Maturity Model Certification (CMMC) assessment process, the presentation of the Final Recommended Assessment Findings is a critical step. According to the CMMC Assessment Process guidelines, the Lead Assessor is responsible for compiling and presenting these findings. The prescribed method for this presentation is the utilization of the standardized CMMC Findings Brief template.

Step-by-Step Explanation:

Responsibility of the Lead Assessor:

The Lead Assessor oversees the assessment process and is tasked with compiling the Final Recommended Assessment Findings.

Utilization of the CMMC Findings Brief Template:

To ensure consistency and adherence to CMMC standards, the Lead Assessor must use the official CMMC Findings Brief template when presenting the assessment findings.

Presentation of Findings:

The findings, documented in the CMMC Findings Brief template, are then presented to the Organization Seeking Certification (OSC). This presentation ensures that the OSC receives a clear and standardized report of the assessment outcomes.

References:

CMMC Assessment Process documentation emphasizes the requirement for the Lead Assessor to use the CMMC Findings Brief template for presenting Final Recommended Assessment Findings.

Cyberab

By adhering to this standardized approach, the assessment process maintains uniformity, ensuring that all findings are communicated effectively and in alignment with CMMC guidelines.

Question #:141 - [CMMC Assessment Process (CAP)]

After completing a Level 2 Assessment, a C3PAO is preparing to upload the Assessment Results Package to Enterprise Mission Assurance Support Service. Which document MUST be included as part of the final assessment results package?

A. Final Report

B. Certification rating

C. Summary-level findings

D. All Daily Checkpoint logs

Answer: A

Explanation

Understanding the Assessment Results Package SubmissionAfter completing aCMMC Level 2 Assessment, theCertified Third-Party Assessment Organization (C3PAO)mustsubmit the final assessment results packageto theEnterprise Mission Assurance Support Service (eMASS)system.

TheFinal Reportis themandatory documentthatcontains all assessment details, findings, and scoring.

It serves as theofficial record of the assessmentanddetermines certification eligibility.

Key Required Document: Final Report

A. Final Report # Correct

TheFinal Report is requiredin the submission package todocument assessment results officially.

It includes asummary of findings, scoring, and recommendations.

B. Certification rating # Incorrect

The C3PAO does not issue certification ratings—theDoDandCMMC-ABdetermine certification status after reviewing the Final Report.

C. Summary-level findings # Incorrect

While the Final Reportincludessummary findings, astandalone summary-level findings document is not a required upload.

D. All Daily Checkpoint logs # Incorrect

Checkpoint logsare part of the internal assessment process butare not required in the final eMASS submission.

Why is the Correct Answer "Final Report" (A)?

CMMC Assessment Process (CAP) Document

Specifies that theFinal Report must be submitted to eMASSafter a Level 2 assessment.

CMMC-AB Guidelines for C3PAOs

States that theFinal Report is the key document used to determine certification status.

DFARS 252.204-7021 (CMMC Requirements Clause)

Requires the assessment results to be documented in an official report and submitted via eMASS.

CMMC 2.0 References Supporting This Answer:

Final Answer:#A. Final Report

Question #:142 - [CMMC Ecosystem]

A contractor has implemented IA.L2-3.5.3: Multifactor Authentication practice for their privileged users, however, during the assessment it was discovered that the OSC's standard users do not require MFA to access their endpoints and network resources. What would be the BEST finding?

A. The process is running correctly.

B. It is out of scope as this is a new acquisition.

C. The new acquisition is considered Specialized Assets.

D. Practice is NOT MET since the objective was not implemented.

Answer: D

Explanation

Understanding IA.L2-3.5.3: Multifactor Authentication (MFA) RequirementTheIA.L2-3.5.3practice, derived fromNIST SP 800-171 (Requirement 3.5.3), requires thatmultifactor authentication (MFA) be implemented for both privileged and standard userswhen accessing:

#Organizational endpoints(e.g., laptops, desktops, mobile devices).

#Network resources(e.g., VPNs, internal systems).

#Cloud services containing Controlled Unclassified Information (CUI).

Key Requirement for a "MET" RatingFor IA.L2-3.5.3 to beMet, the organization must:

Require MFA for all privileged users(e.g., system administrators).

Require MFA for standard users accessing endpoints and network resources.

Implement MFA across all relevant systems.

Sincestandard users do not require MFA in the OSC’s current implementation, the practiceis not fully implementedand must be ratedNOT MET.

A. The process is running correctly # Incorrect

MFA isonly applied to privileged users, but it isalso required for standard users. The process isnot fully implemented.

B. It is out of scope as this is a new acquisition # Incorrect

New acquisitionsmust still meet MFA requirementsif they handle CUI or network access.

C. The new acquisition is considered Specialized Assets # Incorrect

Specialized assets (e.g., IoT, legacy systems) may have alternative security controls, but standard users and endpointsmust still comply with MFA.

D. Practice is NOT MET since the objective was not implemented # Correct

MFA must be enabled for both privileged and standard usersaccessing endpoints and network resources. Since standard users are excluded, the practice isNOT MET.

Why is the Correct Answer "D" (Practice is NOT MET since the objective was not implemented)?

CMMC 2.0 Level 2 (Advanced) Requirements

Specifies thatMFA must be applied to all users accessing CUI and network resources.

NIST SP 800-171 (Requirement 3.5.3 – MFA Implementation)

Requires MFA forall user types, including privileged and standard users.

CMMC Assessment Process (CAP) Document

States that a practicemust be fully implemented to be considered MET. Partial implementation meansNOT MET.

CMMC 2.0 References Supporting This Answer:

Question #:143 - [CMMC Ecosystem]

Which training is a CCI authorized to deliver through an approved CMMC LTP?

A. CMMC-AB approved training

B. DoD DFARS and CMMC-AB approved training

C. NARA CUI training and CMMC-AB approved training

D. DoD DFARS, NARA CUI, and CMMC-AB approved training

Answer: A

Explanation

A Certified CMMC Instructor (CCI) is only authorized to deliver CMMC-AB (now The Cyber AB) approved training courses through a Licensed Training Provider (LTP). CCI instructors do not deliver DFARS or NARA CUI training under CMMC authorization—only formally approved CMMC courses.

Supporting Extracts from Official Content:

- CMMC Ecosystem Roles: “CCIs are authorized to deliver CMMC-AB approved training courses through an LTP.”

Why Option A is Correct:

- CCIs teach only CMMC-AB approved training.
- Options B, C, and D include external trainings (DFARS or NARA CUI) that are not within the CCI’s scope.

References (Official CMMC v2.0 Content):

- CMMC Ecosystem documentation – Roles and Responsibilities of LTPs and CCIs.

===========

Question #:144 - [CMMC Model Overview]

Which entity requires that organizations handling FCI or CUI be assessed to determine a required Level of cybersecurity maturity?

A. DoD

B. CISA

C. NIST

D. CMMC-AB

Answer: A

Explanation

TheU.S. Department of Defense (DoD)is the entity thatrequiresorganizations handlingFederal Contract Information (FCI)orControlled Unclassified Information (CUI)to undergo an assessment to determine their required level ofcybersecurity maturityunderCMMC 2.0.

This requirement stems from theDFARS 252.204-7021 clause, which mandates CMMC certification for contractors handling FCI or CUI.

Reference:

DoD CMMC 2.0 Program Overview

DFARS 252.204-7021 (CMMC Requirements)

Step 2: DoD's Cybersecurity Maturity LevelsTheDoD determinestherequired cybersecurity maturity levelfor a contract based on the sensitivity of the information involved:

CMMC Level 1– Required for organizations handlingFCI(Basic Cyber Hygiene).

CMMC Level 2– Required for organizations handlingCUI(Aligned with NIST SP 800-171).

CMMC Level 3– Required for organizations handlinghigh-value CUIand facingAdvanced Persistent Threats (APT)(Aligned with a subset ofNIST SP 800-172).

Reference:

CMMC 2.0 Model Documentation

NIST SP 800-171 & 800-172for security controls

Step 3: Why Other Answer Choices Are IncorrectB. CISA (Incorrect):

TheCybersecurity and Infrastructure Security Agency (CISA)is responsible fornational cybersecuritybut does not mandate CMMC assessments.

C. NIST (Incorrect):

TheNational Institute of Standards and Technology (NIST)provides the security framework (e.g.,NIST SP 800-171) but does not enforce CMMC compliance.

D. CMMC-AB (Incorrect):

TheCyber AB (formerly CMMC-AB)is responsible for accreditingC3PAOsand overseeing theCMMC ecosystem, but it does not determine which organizations require assessments.

Final Confirmation of Correct Answer:The DoD mandates CMMC compliance for organizations handling FCI or CUI.

CMMC requirements are enforced through DFARS clauses in DoD contracts.

Thus, the correct answer is:A. DoD

Question #:145 - [CMMC Model Overview]

While conducting a CMMC Level 2 Assessment, a CCP is reviewing an OSC's personnel security process. They have a policy that describes screening individuals prior to authorizing access to CUI, but it does not mention what organizations should be looking for in an individual. There is no link to a process or procedural document. What should the OSC evaluate when screening individuals prior to accessing CUI?

A. They are trusted and well liked

B. They are a hard and loyal worker

C. Their conduct, integrity, and loyalty

D. Their functionality, reliability, and ability to adapt

Answer: C

Explanation

Under NIST SP 800-171, Personnel Security (PS) family, requirement PS.L2-3.9.1, organizations must screen individuals prior to granting access to CUI. The screening is intended to evaluate conduct, integrity, and loyalty to ensure that individuals can be trusted with sensitive information.

Supporting Extracts from Official Content:

- NIST SP 800-171 Rev. 2, PS.L2-3.9.1: “Screen individuals prior to authorizing access to organizational systems containing CUI… Screening is intended to assess an individual’s conduct, integrity, judgment, loyalty, and reliability.”
- CMMC Level 2 Assessment Guide (Personnel Security practices): confirms that screening covers conduct, integrity, and loyalty.

Why Option C is Correct:

- The key attributes explicitly listed are conduct, integrity, and loyalty.
- Options A and B describe subjective or informal measures, not compliance criteria.
- Option D uses terms not aligned with the official requirement.

References (Official CMMC v2.0 Content):

- NIST SP 800-171 Rev. 2, Personnel Security controls.
- CMMC Assessment Guide, Level 2 – PS.L2-3.9.1.

===========

Question #:146 - [Implementation and Scoping]

Which term describes assessing the ability of a unit equipped with a system to support its mission while withstanding cyber threat activity representative of an actual adversary?

A. Penetration test

B. Black hat testing

C. Red cell assessment

D. Adversarial assessment

Answer: D

Explanation

The term Adversarial Assessment is formally defined in DoD cyber terminology. It describes testing that evaluates a unit or system’s ability to perform its mission while facing simulated cyber threat activity representative of a real-world adversary.

Supporting Extracts from Official Content:

- DoD Cybersecurity Test and Evaluation Guidebook: “Adversarial Assessment: Test conducted to evaluate a unit’s ability to support its mission while withstanding cyber threat activity representative of an actual adversary.”

Why Option D is Correct:

- A penetration test is narrower and focuses on identifying vulnerabilities.
- Black hat testing is not an official DoD or CMMC term.
- Red cell assessment refers more broadly to force-on-force exercises and is not the term used in CMMC /governing DoD definitions.

References (Official CMMC v2.0 Content and Source Documents):

- DoD Cybersecurity Test and Evaluation Guidebook.
- CMMC v2.0 Governance – Source Documents (incorporating DoD definitions).

Question #:147 - [CMMC Model Overview]

Prior to conducting a CMMC Assessment, the contractor must specify the CMMC Assessment scope by categorizing all assets. Which two asset categories are always assessed against CMMC practices?

A. CUI Assets and Specialized Assets

B. Security Protection Assets and CUI Assets

C. Specialized Assets and Contractor Risk Managed Assets

D. Security Protection Assets and Contractor Risk Managed Assets

Answer: B

Explanation

Understanding CMMC Asset Scoping RequirementsBefore conducting aCMMC Level 2 Assessment, anOrganization Seeking Certification (OSC)must define theassessment scopeby categorizing all assets. This ensures that only relevant systems are assessed againstCMMC practices, reducing unnecessary compliance burdens.

According to theCMMC Scoping Guide for Level 2, there are four asset categories:

CUI Assets– Assets that process, store, or transmitControlled Unclassified Information (CUI).

Security Protection Assets (SPA)– Assets that providesecurity functions(e.g., firewalls, intrusion detection systems, identity management systems).

Contractor Risk Managed Assets (CRMA)– Assets thatdo not directly store/process CUIbut interact with CUI environments (e.g., BYOD devices, personal computers used for remote access).

Specialized Assets– Unique systems such asOperational Technology (OT), IoT, and Government Furnished Equipment (GFE), which may requirelimitedCMMC assessment.

Which Asset Categories Are Always Assessed?#1. CUI Assets(ALWAYS ASSESSED)

These are theprimary focusof CMMC Level 2 since they handleCUI.

All110 NIST SP 800-171 controlsapply to these assets.

#2. Security Protection Assets (SPA)(ALWAYS ASSESSED)

Security tools that protectCUI Assetsarealways includedin the assessment.

Examples includefirewalls, antivirus, endpoint detection and response (EDR) tools, and identity management systems.

(A) CUI Assets and Specialized Assets#

CUI Assets are assessed, butSpecialized Assets are only assessed in a limited manner, depending on their role inCUI security.

(C) Specialized Assets and Contractor Risk Managed Assets#

Specialized Assets and CRMAsare typicallynot fully assessedagainst CMMC controls unless they directly impactCUI security.

(D) Security Protection Assets and Contractor Risk Managed Assets#

SPAs are always assessed, butCRMAs are not necessarily assessedunless they directly impact CUI.

TheCMMC Scoping Guide (Level 2)clearly states thatCUI Assets and Security Protection Assetsarealways assessedagainst CMMC practices.

Why the Other Answer Choices Are Incorrect:Final Validation from CMMC Documentation:Thus, the correct answer is:

B. Security Protection Assets and CUI Assets.

Question #:148 - [CMMC Model Overview]

The Level 1 practice description in CMMC is Foundational. What is the Level 2 practice description?

A. Expert

B. Advanced

C. Optimizing

D. Continuously Improved

Answer: B

Explanation

Understanding CMMC 2.0 Levels and Their DescriptionsTheCybersecurity Maturity Model Certification (CMMC) 2.0consists ofthree levels, each representing increasing cybersecurity maturity:

Level 1 – Foundational

Focuses onbasic cyber hygiene

Implements17 practicesaligned withFAR 52.204-21

Primarily protectsFederal Contract Information (FCI)

Level 2 – Advanced(Correct Answer)

Focuses onprotecting Controlled Unclassified Information (CUI)

Implements110 practicesaligned withNIST SP 800-171

Requirestriennial third-party assessments for critical programs

Level 3 – Expert

Focuses onadvanced cybersecurityagainstAPT (Advanced Persistent Threats)

ImplementsNIST SP 800-171 and additional NIST SP 800-172 controls

Requirestriennial government-led assessments

TheCMMC 2.0 framework explicitly describes Level 2 as "Advanced."

Italigns with NIST SP 800-171to ensure robustCUI protection.

A. Expert (Incorrect)– This describesLevel 3, not Level 2.

C. Optimizing (Incorrect)– Not a defined CMMC level description.

D. Continuously Improved (Incorrect)– CMMC does not use this terminology.

The correct answer isB. Advanced, which accurately describesCMMC Level 2.

References:

CMMC 2.0 Model Overview

CMMC 2.0 Scoping Guide

NIST SP 800-171 & NIST SP 800-172

Question #:149 - [CMMC Model Overview]

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

A. NISTSP 800-53.

B. NISTSP 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 Explanation:

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.

References:

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 #:150 - [CMMC Model Overview]

An Assessment Team is reviewing a practice that is documented and being checked monthly. When reviewing the logs, the practice is only being completed quarterly. During the interviews, the team members say they perform the practice monthly but only document quarterly. Is this sufficient to pass the practice?

A. No, the work is not being done as stated.

B. Yes, the practice is being done as documented.

C. No, all three assessment methods must be met to pass.

D. Yes. the interview process is enough to pass a practice.

Answer: A

Explanation

Understanding CMMC Assessment Requirements

CMMC assessments usethree assessment methodsto verify compliance with security practices:

Examine– Reviewing documentation, policies, logs, or records.

Interview– Speaking with personnel to confirm understanding and execution.

Test– Verifying through technical or operational means that the practice is being performed.

Assessment Findings in the Given Scenario

Practice is documented as occurring monthly, but logs show quarterly execution.

Interviews indicate monthly execution, but documentation does not support this claim.

Why the Organization Fails the Practice

Answer A (Incorrect): The work is being performed, but documentation is lacking, so the failure is not purely due to missing execution.

Answer B (Incorrect): The documented frequency does not match the evidence in logs, so the practice is not being done asfully documented.

Answer C (Correct):CMMC requires all three assessment methods (Examine, Interview, Test) to align. Since logs contradict the stated frequency, the practicefailscompliance.

Answer D (Incorrect): Interview responses alone are not enough. The CMMCCAP GuideandNIST SP 800-171Arequire corroboration with logs (Examine) and technical verification (Test).

Conclusion

The correct answer isC: To pass a practice, the organization mustprovide evidence across all three assessment methods.

CMMC Assessment Process (CAP) Guide– Cyber AB

NIST SP 800-171A– Assessing Security Requirements for CUI

DoD CMMC 2.0 Scoping and Assessment Guide

Question #:151 - [CMMC Model Overview]

Who makes the final determination of the assessment method used for each practice?

A. CCP

B. osc

C. Site Manager

D. Lead Assessor

Answer: D

Explanation

Who Determines the Assessment Method for Each Practice?In aCMMC Level 2 Assessment, theLead Assessorhas thefinal authorityin determining theassessment methodused to evaluate each practice.

Key Responsibilities of the Lead Assessor#Ensures theCMMC Assessment Process (CAP) Guideis followed.

#Determines whether a practice is evaluated usinginterviews, demonstrations, or document reviews.

#Directs theCertified CMMC Professionals (CCPs)and other assessors on themethodologyfor gathering evidence.

#Works under aCertified Third-Party Assessment Organization (C3PAO)to ensure proper assessment execution.

CCP (Option A) assists in the assessment but does not make final decisionson methods.

OSC (Option B) is the Organization Seeking Certification, and they do not control assessment methodology.

Site Manager (Option C) may coordinate logistics but has no authority over assessment decisions.

Why "Lead Assessor" is Correct?Breakdown of Answer ChoicesOption

Description

Correct?

A. CCP

#Incorrect–A CCPassistsbut doesnot determine assessment methods.

B. OSC

#Incorrect–The OSC is beingassessedand does not decide assessment methods.

C. Site Manager

#Incorrect–The Site Manager handles logistics butdoes not control assessment methods.

D. Lead Assessor

#Correct – The Lead Assessor has the final say on the assessment method used.

CMMC Assessment Process Guide (CAP)– Defines theLead Assessor’s rolein determining assessment methods.

Official References from CMMC 2.0 DocumentationFinal Verification and ConclusionThe correct answer isD. Lead Assessor, as they havefinal decision-making authority over the assessment methodology.

Question #:152 - [CMMC Model Overview]

An assessment procedure consists of an assessment objective, potential assessment methods, and assessment objects. Which statement is part of an assessment objective?

A. Specifications and mechanisms

B. Examination, interviews, and testing

C. Determination statement related to the practice

D. Exercising assessment objects under specified conditions

Answer: C

Explanation

Understanding CMMC Assessment ProceduresACMMC assessment procedureconsists of:

Assessment Objective– Defines what is being evaluated and the expected outcome.

Assessment Methods– Specifies how the evaluation is conducted (e.g.,examination, interviews, testing).

Assessment Objects– Identifies what is being evaluated, such as policies, systems, or people.

Assessment Objectivesincludedetermination statementsthat describe the expected outcome for each CMMC security practice.

These statements define whether a practice has beenadequately implementedbased ondocumented evidence and assessment findings.

TheCMMC Assessment Process (CAP) GuideandNIST SP 800-171Aspecify that each practice has a determination statement guiding assessment decisions.

A. Specifications and mechanisms#Incorrect

These belong toassessment objects, which refer to the systems, policies, and mechanisms being evaluated.

B. Examination, interviews, and testing#Incorrect

These areassessment methods, which describe how assessorsverifycompliance (e.g., through interviews or testing).

D. Exercising assessment objects under specified conditions#Incorrect

This refers toassessment testing, which is a method, not an assessment objective.

CMMC Assessment Process (CAP) Guide– Describes determination statements as the core of assessment objectives.

NIST SP 800-171A– Defines determination statements as a key element of evaluating security controls.

Why the Correct Answer is "C"?Why Not the Other Options?Relevant CMMC 2.0 References:Final Justification:Since anassessment objectiveincludes adetermination statementthat describes whether a practice is implemented properly, the correct answer isC.

Question #:153 - [CMMC Ecosystem]

When planning an assessment, the Lead Assessor should work with the OSC to select personnel to be interviewed who could:

A. have a security clearance.

B. be a senior person in the company.

C. demonstrate expertise on the CMMC requirements.

D. provide clarity and understanding of their practice activities.

Answer: D

Explanation

Interview Selection in CMMC AssessmentsDuring aCMMC assessment, theLead Assessormust work with theOrganization Seeking Certification (OSC)to select personnel for interviews. The goal is to:

#Verify that personnel understand andperform security-related practices.

#Ensure that individuals canexplain how they implement CMMC requirements.

#Gain insight intoactual cybersecurity operationsrather than just documented policies.

The best interviewees are those whodirectly engage with security practicesand canclearly explain how they perform their duties.

CMMC assessmentsrely on interviewsto validate that security practices areimplemented effectively.

Themost valuable intervieweesare those who canexplainhow security measures are appliedin day-to-day operations.

CMMC Assessment Process (CAP)emphasizes that assessors should speak tothose actively involved in security practicesrather than just senior management or policy owners.

Why "Providing Clarity and Understanding" Is KeyThus,option D is the correct choicebecause the Lead Assessor should prioritizeinterviewing personnel who can clearly explain how CMMC practices are implemented.

A. Have a security clearance.#Incorrect.Security clearance is not a requirementfor CMMC assessments. The focus is onpractical implementation of security controls, not classified work.

B. Be a senior person in the company.#Incorrect. Senior executives may not be involved in theactual implementation of security controls. The best interviewees are those whoperform the work, not just oversee it.

C. Demonstrate expertise on the CMMC requirements.#Incorrect. Whileunderstanding CMMC is important, expertise alonedoes not guarantee practical knowledgeof security controls. The key is thatinterviewees must provide clarity on how they perform security tasks.

Why the Other Answers Are Incorrect

CMMC Assessment Process (CAP) Document– Guides interview selection based on personnel who perform security functions.

NIST SP 800-171 & CMMC 2.0– Emphasize that cybersecurity controls must beactively implemented, not just documented.

CMMC Official ReferencesThus,option D (Provide clarity and understanding of their practice activities) is the correct answeras per official CMMC assessment guidelines.

Question #:154 - [CMMC Assessment Process (CAP)]

Two assessors cannot agree if a certain practice should be rated as MET or NOT MET. Who should they consult to determine the final interpretation?

A. C3PAO

B. CMMC-AB

C. Lead Assessor

D. Quality Assurance Assessor

Answer: C

Explanation

The Lead Assessor has the authority to make the final determination in situations where assessors cannot agree on a rating. CAP specifies that the Lead Assessor ensures consistency, resolves disputes, and provides the authoritative interpretation during the assessment process. Escalation to the CMMC-AB or Quality Assurance would only occur in rare post-assessment review cases, not during an active assessment.

Reference Documents:

- CMMC Assessment Process (CAP), v1.0

Question #:155 - [CMMC Assessment Process (CAP)]

The facilities manager for a company has procured a Wi-Fi enabled, mobile application-controlled thermostat for the server room, citing concerns over the inability to remotely gauge and control the temperature of the room. Because the thermostat is connected to the company's FCI network, should it be assessed as part of the CMMC Level 1 Self-Assessment Scope?

A. No, because it is OT

B. No, because it is an loT device

C. Yes. because it is a restricted IS

D. Yes, because it is government property

Answer: C

Explanation

CMMC Level 1applies toFederal Contract Information (FCI)systems.

Any system or device that is connected to an FCI-handling network is within the assessment scopebecause it canintroduce vulnerabilitiesinto the environment.

TheWi-Fi-enabled thermostat is connected to the FCI network, meaning it haspotential accessto sensitive contract-related data.

PerCMMC Scoping Guidance, this type of device is classified as aRestricted Information System (Restricted IS)—devices that do not store, process, or transmit FCI but areconnected to networks that do.

Restricted IS must be accounted for in the self-assessment scope to ensure they do not compromise security controls.

Reference:

CMMC Level 1 Scoping Guidance

CMMC Assessment Process (CAP) Guide

Step 3: Why Other Answer Choices Are IncorrectA. No, because it is OT (Incorrect):

Operational Technology (OT)includesindustrial control systemsbut does not exempt a device from assessmentif it connects to an FCI network.

B. No, because it is an IoT device (Incorrect):

IoT (Internet of Things) devicesthat areconnected to an FCI network must be assessedto ensure they do not create security vulnerabilities.

D. Yes, because it is government property (Incorrect):

Theownershipof the device (government or company) doesnotdetermine its inclusion in the CMMC assessment scope—its network connectivity does.

Final Confirmation of Correct Answer:The thermostat is part of the CMMC Level 1 Self-Assessment Scope as a Restricted IS.

Thus, the correct answer is:C. Yes, because it is a restricted IS

Question #:156 - [CMMC Model Overview]

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

A. NIST SP 800-53

B. NIST SP 800-171

C. 48 CFR 52.204-21

D. DFARS 252.204-7012

Answer: B

Explanation

CMMC Level 2 requires full implementation of the 110 security requirements specified in NIST SP 800-171 Rev. 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. These practices form the foundation for safeguarding CUI across defense contractor systems.

- NIST SP 800-53 is a broader catalog of security controls for federal systems, not specific to CUI in the defense contractor environment.
- 48 CFR 52.204-21 establishes basic safeguarding requirements for Federal Contract Information (FCI) and corresponds to CMMC Level 1.
- DFARS 252.204-7012 defines safeguarding and incident reporting obligations but does not enumerate the specific security practices required.

Thus, Level 2 practices are aligned to NIST SP 800-171.

Reference Documents:

- CMMC Model v2.0 Overview, December 2021
- NIST SP 800-171 Rev. 2

Question #:157 - [CMMC Model Overview]

The Audit and Accountability (AU) domain has practices in:

A. Level 1.

B. Level 2.

C. Levels 1 and 2.

D. Levels 1 and 3.

Answer: B

Explanation

TheAudit and Accountability (AU) domainis one of the14 familiesof security requirements inNIST SP 800-171 Rev. 2, which is fully adopted byCMMC 2.0 Level 2.

A. Level 1#Incorrect

CMMCLevel 1only includes17 basic FAR 52.204-21 safeguarding requirementsand does not coverAudit and Accountability (AU)practices.

B. Level 2#Correct

TheAU domain is required at Level 2, which aligns withNIST SP 800-171.

CMMC 2.0 Level 2includes110 security controls, among whichAU-related controlsfocus on logging, monitoring, and accountability.

C. Levels 1 and 2#Incorrect

Level 1 does not requireaudit and accountability practices.

D. Levels 1 and 3#Incorrect

CMMC 2.0 only has Levels 1, 2, and 3, andAU is present in Level 2, making Level 3 irrelevant for this answer.

NIST SP 800-171 Rev. 2 (Audit and Accountability - Family 3.3)

TheAU domainconsists of security controls3.3.1 – 3.3.8, focusing on audit log generation, retention, and accountability.

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

AU practices (Audit and Accountability) are only required at Level 2.

Analysis of the Given Options:Official References Supporting the Correct Answer:Conclusion:TheAU domain applies only to CMMC 2.0 Level 2, making the correct answer:

#B. Level 2.

Question #:158 - [CMMC Model Overview]

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

A. 15 practices

B. 17 practices

C. 72 practices

D. 110 practices

Answer: A

Explanation

CMMC (Cybersecurity Maturity Model Certification) 2.0 Level 1 is designed to protectFederal Contract Information (FCI)and consists of17 foundational cybersecurity practices. These practices are directly derived fromFAR 52.204-21(Basic Safeguarding of Covered Contractor Information Systems), which outlines minimum security requirements for contractors handling FCI.

Breakdown of CMMC Level 1 PracticesThe17 practicesin Level 1 focus on basic cybersecurity hygiene and fall under the following6 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 DocumentationThe 17 practices forCMMC Level 1are explicitly listed in theCMMC 2.0 Appendices and Assessment Guide for Level 1, as well as in theFAR 52.204-21 requirements. These practices representbasic safeguarding measuresthat all DoD contractors handlingFCImust 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 ConclusionThe correct answer isB. 17 practicesas verified from theCMMC 2.0 official documentsandFAR 52.204-21 requirements.

Question #:159 - [CMMC Assessment Process (CAP)]

Who is responsible for identifying and verifying Assessment Team Member qualifications?

A. C3PAO

B. CMMC-AB

C. Lead Assessor

D. CMMC Marketplace

Answer: C

Explanation

Understanding the Role of the Lead Assessor in CMMC AssessmentsTheLead Assessoris responsible for managing theAssessment Teamand ensuring that all team members meet the required qualifications as defined by theCMMC Accreditation Body (CMMC-AB)and theCybersecurity Maturity Model Certification (CMMC) Assessment Process (CAP) Guide.

Lead Assessor’s Key Responsibilities (Per CAP Guide)

Verify team member qualificationsto ensure compliance with CMMC-AB guidelines.

Assignappropriate assessment tasksbased on team members’ expertise.

Ensure that theassessment is conducted in accordance with CMMC procedures.

Why Not the Other Options?

A. C3PAO (Certified Third-Party Assessor Organization)#Incorrect

AC3PAOis responsible fororganizing assessmentsand ensuring their execution, but itdoes not verify individual team member qualifications—that responsibility belongs to theLead Assessor.

B. CMMC-AB (CMMC Accreditation Body)#Incorrect

TheCMMC-ABestablishestraining and certification requirements, but itdoes not verify individual assessment team members—that responsibility is given to theLead Assessor.

D. CMMC Marketplace#Incorrect

TheCMMC Marketplacelists authorizedC3PAOs, Registered Practitioners (RPs), and Certified Professionals (CCPs)butdoes not verify assessment team qualifications.

CMMC Assessment Process (CAP) Guide– Defines theLead Assessor’s responsibilityfor verifying assessment team qualifications.

CMMC-AB Certification Guide– Specifies that the Lead Assessor must ensure all assessment team members meet CMMC-AB qualification standards.

Why the Correct Answer is "C. Lead Assessor"?Relevant CMMC 2.0 References:Final Justification:Since theLead Assessor is responsible for verifying assessment team member qualifications, the correct answer isC. Lead Assessor.

Question #:160 - [CMMC Assessment Process (CAP)]

An assessment is being completed at a client site that is not far from the Lead Assessor's home office. The client provides a laptop for the duration of the engagement. During a meeting with the network engineers, the Lead Assessor requests information about the network. They respond that they have a significant number of drawings they can provide via their secure cloud storage service. The Lead Assessor returns to their home office and decides to review the documents. What is the BEST way to retrieve the documents?

A. Log into the secure cloud storage service to save copies of the documents on both the work and client laptops.

B. Log into the client VPN from the client laptop and retrieve the documents from the secure cloud storage service.

C. Log into the client VPN from the assessor's laptop and retrieve the documents from the secure cloud storage service.

D. Use their home office workstation to retrieve the documents from the secure cloud storage service and save them to a USB stick.

Answer: B

Explanation

Best Practices for Handling Sensitive Assessment InformationCMMC assessments involve handlingsensitive and potentially CUI-related documents. Assessors must follow strictsecurity policiesto avoid unauthorized access, data leaks, or non-compliance withCMMC 2.0 and NIST SP 800-171 requirements.

Why Logging into the Client VPN on the Client Laptop is the Best Approach:

Ensures Data Protection:The client laptop is likely configured to meet security controls required for handling assessment-related materials.

Prevents Data Spillage:Keeping all assessment-related activities within the client’s secured environment reduces the risk ofdata leakage or unauthorized storage.

Maintains Compliance with CMMC/NIST Guidelines:Using aproperly configured client laptop and secured connectionensures compliance withNIST SP 800-171 controls on secure remote access(Requirement3.13.12).

A. "Log into the secure cloud storage service to save copies of the documents on both the work and client laptops."

Incorrect#Sensitive data should not be duplicated across multiple systems, especially a non-client-approved laptop. Storing it on an unauthorized systemviolates data handling best practices.

C. "Log into the client VPN from the assessor's laptop and retrieve the documents from the secure cloud storage service."

Incorrect# Theassessor’s laptop may not be authorizedorsecuredto handle client data. CMMC guidelines emphasizeusing approved, secured systemsfor assessment-related information.

D. "Use their home office workstation to retrieve the documents from the secure cloud storage service and save them to a USB stick."

Incorrect#

Transferring sensitive documents via USBintroduces security risks, including unauthorized data storage and potential malware contamination.

Home office workstationsare unlikely to be authorized for handling CMMC-sensitive data.

References:NIST SP 800-171 Rev. 2, Control 3.13.12 ("Use of Secure Remote Access")

CMMC 2.0 Level 2 Assessment Process Guide(Cyber AB)

DoD CUI Handling Guidelines(DoD CIO)

#Final Answer: B. Log into the client VPN from the client laptop and retrieve the documents from the secure cloud storage service.

Question #:161 - [CMMC Ecosystem]

During a Level 1 Self-Assessment, a smart thermostat was identified. It is connected to the Internet on the OSC's WiFi network. What type of asset is this?

A. FCI Asset

B. CUI Asset

C. In-scope Asset

D. Specialized Asset

Answer: D

Explanation

Understanding Asset Categorization in CMMC 2.0InCMMC 2.0, assets are categorized into different types based on their function, connectivity, and whether they process, store, or transmitFederal Contract Information (FCI) or Controlled Unclassified Information (CUI).

TheCMMC 2.0 Scoping GuidedefinesSpecialized Assetsas assetsthat do not fit traditional IT classificationsbut still exist within the organizational environment.

Asmart thermostatis anInternet of Things (IoT) device, which falls underSpecialized Assetsas defined in CMMC.

A. FCI Asset (Incorrect)

FCI Assets process, store, or transmit Federal Contract Information, which asmart thermostat does not.

B. CUI Asset (Incorrect)

CUI Assets handle Controlled Unclassified Information, and athermostat does not process CUI.

C. In-scope Asset (Incorrect)

In-scope Assets include FCI and CUI assets, which asmart thermostat does not qualify as.

The correct answer isD. Specialized Asset, as asmart thermostat is an IoT device, which falls into theSpecialized Assetcategory.

References:

CMMC 2.0 Scoping Guide

DoD Cybersecurity Guidelines on IoT Devices

Question #:162 - [CMMC Ecosystem]

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?

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 containsControlled Unclassified Information (CUI)withspecific categories and dissemination controls.

CUI//SP-PRVCY//FED Onlybreaks down as follows:

CUI# Controlled Unclassified Information designation.

SP-PRVCY#Specifiedcategory forPrivacy Information(SP stands for "Specified").

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

Who Maintains the Official CUI Registry?

TheNational Archives and Records Administration (NARA) oversees the CUI Programand maintains the officialCUI Registry(https://www.archives.gov/cui).

The CUI Registry providesdefinitions, marking guidance, and categoriesfor 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 shouldrefer to the NARA CUI Registryfor official marking interpretations.

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

B. CMMC-AB– TheCMMC Accreditation Bodymanages certification assessments butdoes not define or interpret CUI markings.

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

D. DoD 239.7601 Definitions Page– This refers to generalDoD acquisition definitions, butCUI categories and markings fall under NARA’s authority.

References:NARA CUI Registry(https://www.archives.gov/cui)

DoD CUI Program Guidance(DoD CIO Site)

CMMC 2.0 Level 2 Compliance Requirements(Cyber AB)

#Final Answer: A. NARA

Question #:163 - [CMMC Ecosystem]

An employee is the primary system administrator for an OSC. The employee will be a core part of the assessment, as they perform most of the duties in managing and maintaining the systems. What would the employee be BEST categorized as?

A. Analyzer

B. Inspector

C. Applicable staff

D. Demonstration staff

Answer: C

Explanation

In the context of a Cybersecurity Maturity Model Certification (CMMC) assessment, the roles and responsibilities of individuals involved are clearly delineated to ensure a structured and effective evaluation process. The term "applicable staff" refers to personnel within the Organization Seeking Certification (OSC) who possess specific knowledge or expertise pertinent to the assessment. These individuals are integral to the assessment process as they provide essential information, demonstrate the implementation of security practices, and facilitate the assessment team's understanding of the organization's cybersecurity posture.

In this scenario, the employee serving as the primary system administrator is responsible for managing and maintaining the organization's systems. Given their comprehensive understanding of the system configurations, security controls, and operational procedures, this individual is best categorized as "applicable staff." Their involvement is crucial during the assessment, as they can provide detailed insights, demonstrate compliance measures, and address technical inquiries from the assessment team.

The other options can be delineated as follows:

Analyzer:Typically refers to individuals who analyze data or security incidents, often as part of a security operations center. This role is not specifically defined within the CMMC assessment context.

Inspector:Generally denotes a person who examines or inspects systems and processes, possibly as part of an internal audit or compliance check. This term is not a standard designation within the CMMC assessment framework.

Demonstration staff:While this could imply personnel responsible for demonstrating systems or processes, it is not a recognized role within the CMMC assessment process.

Therefore, the primary system administrator, by virtue of their role and responsibilities, aligns with the "applicable staff" category, playing a pivotal role in facilitating a successful CMMC assessment.

Question #:164 - [CMMC Model Overview]

Which standard and regulation requirements are the CMMC Model 2.0 based on?

A. NIST SP 800-171 and NIST SP 800-172

B. DFARS, FIPS 100, and NIST SP 800-171

C. DFARS, NIST, and Carnegie Mellon University

D. DFARS, FIPS 100, NIST SP 800-171, and Carnegie Mellon University

Answer: A

Explanation

TheCybersecurity Maturity Model Certification (CMMC) 2.0is primarily based on two key National Institute of Standards and Technology (NIST) Special Publications:

NIST SP 800-171– "Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations"

NIST SP 800-172– "Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171"

NIST SP 800-171

This document is thecore foundationof CMMC 2.0 and establishes the security requirements for protectingControlled Unclassified Information (CUI)in non-federal systems.

The 110 security controls fromNIST SP 800-171 Rev. 2are mapped directly toCMMC Level 2.

NIST SP 800-172

This supplement includesenhanced security requirementsfor organizations handlinghigh-value CUIthat faces advanced persistent threats (APTs).

These enhanced requirements apply toCMMC Level 3under the 2.0 model.

B. DFARS, FIPS 100, and NIST SP 800-171#Incorrect

WhileDFARS 252.204-7012mandates compliance withNIST SP 800-171,FIPS 100 does not existas a relevant cybersecurity standard.

C. DFARS, NIST, and Carnegie Mellon University#Incorrect

CMMC is aligned with DFARS and NIST but isnot developed or directly influenced by Carnegie Mellon University.

D. DFARS, FIPS 100, NIST SP 800-171, and Carnegie Mellon University#Incorrect

Again,FIPS 100 is not relevant, andCarnegie Mellon Universityis not a defining entity in the CMMC framework.

CMMC 2.0 Scoping Guide (2023)confirms thatCMMC Level 2 is entirely based on NIST SP 800-171.

CMMC 2.0 Level 3 Draft Documentationexplicitly referencesNIST SP 800-172for enhanced security requirements.

DoD Interim Rule (DFARS 252.204-7021)mandates that organizations meetNIST SP 800-171 for CUI protection.

Reference and Breakdown:Eliminating Incorrect Answer Choices:Official CMMC 2.0 References Supporting the Answer:Final Conclusion:The CMMC 2.0 model is derivedsolely from NIST SP 800-171 and NIST SP 800-172, makingAnswer A the only correct choice.

Question #:165 - [Governance and Source Documents]

Which words summarize categories of data disposal described in the NIST SP 800-88 Revision 1, Guidelines for Media Sanitation?

A. Clear, purge, destroy

B. Clear, redact, destroy

C. Clear, overwrite, purge

D. Clear, overwrite, destroy

Answer: A

Explanation

NIST SP 800-88 Rev. 1 is the authoritative guide for media sanitization. It defines three categories of data disposal: Clear, Purge, and Destroy.

Supporting Extracts from Official Content:

- NIST SP 800-88 Rev. 1: “Media sanitization techniques are divided into three categories: Clear, Purge, and Destroy.”

Why Option A is Correct:

- “Clear, Purge, Destroy” are the exact three categories named.
- Redact and Overwrite are not categories; Overwriting is a technique that may fall under Clear.

References (Official CMMC v2.0 Content and Source Documents):

- NIST SP 800-88 Rev. 1, Guidelines for Media Sanitization.

===========

Question #:166 - [CMMC Assessment Process (CAP)]

In performing scoping, what should the assessor ensure that the scope of the assessment covers?

A. All assets documented in the business plan

B. All assets regardless if they do or do not process, store, or transmit FCI/CUI

C. All entities, regardless of the line of business, associated with the organization

D. All assets processing, storing, or transmitting FCI/CUI and security protection assets

Answer: D

Explanation

Scoping Requirements in CMMC AssessmentsTheCMMC 2.0 Scoping GuideandCMMC Assessment Process (CAP) Documentclearly define what should be included in the scope of an assessment.

The assessment scope must cover:

All assets that process, store, or transmit FCI/CUI

Security Protection Assets (ESP)– these assets help protect FCI/CUI, such as firewalls, endpoint detection systems, and encryption mechanisms.

Thus, thecorrect scope includes both:

#FCI/CUI Assets(Data storage, processing, or transmission assets)

#Security Protection Assets (ESP)(Firewalls, security tools, etc.)

A. All assets documented in the business plan#Incorrect.Business plans may include assets unrelated to FCI /CUI, making this scopetoo broad. Only assets relevant to FCI/CUI should be assessed.

B. All assets regardless if they do or do not process, store, or transmit FCI/CUI#Incorrect. CMMC doesnotrequire organizations to include assets thathave no connection to FCI/CUI.

C. All entities, regardless of the line of business, associated with the organization#Incorrect.Only the assets relevant to FCI/CUI or security protection should be assessed. Unrelated business divisions (like a non-federal commercial division) areout-of-scope.

Why the Other Answers Are Incorrect

CMMC 2.0 Scoping Guide – Level 1 & Level 2

CMMC Assessment Process (CAP) Document

CMMC Official ReferencesThus,option D (All assets processing, storing, or transmitting FCI/CUI and security protection assets) is the correct answeras per official CMMC assessment scoping requirements.

Question #:167 - [CMMC Model Overview]

Which term describes "the protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to. or modification of information"?

A. Adopted security

B. Adaptive security

C. Adequate security

D. Advanced security

Answer: C

Explanation

Understanding the Concept of Security in CMMC 2.0CMMC 2.0 aligns with federal cybersecurity standards, particularlyFISMA (Federal Information Security Modernization Act), NIST SP 800-171, and FAR 52.204-21. One key principle in these frameworks is the implementation of security measures that are appropriate for the risk level associated with the data being protected.

The question describes security measures that are proportionate to therisk of loss, misuse, unauthorized access, or modificationof information. This matches the definition of"Adequate Security."

A. Adopted security# Incorrect

The term"adopted security"is not officially recognized in CMMC, NIST, or FISMA. Organizations adopt security policies, but the concept does not directly align with the question’s definition.

B. Adaptive security# Incorrect

Adaptive securityrefers to adynamic cybersecurity modelwhere security measures continuously evolve based on real-time threats. While important, it does not directly match the definition in the question.

C. Adequate security#Correct

The term"adequate security"is defined inNIST SP 800-171, DFARS 252.204-7012, and FISMAas the level of protection that isproportional to the consequences and likelihood of a security incident.

This aligns perfectly with the definition in the question.

D. Advanced security# Incorrect

Advanced securitytypically refers tohighly sophisticated cybersecurity mechanisms, such as AI-driven threat detection. However, the term does not explicitly relate to the concept of risk-based proportional security.

FISMA (44 U.S.C. § 3552(b)(3))

Definesadequate securityas"protective measures commensurate with the risk and potential impact of unauthorized access, use, disclosure, disruption, modification, or destruction of information."

This directly matches the question's wording.

DFARS 252.204-7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting)

Mandates that contractors apply"adequate security"to protect Controlled Unclassified Information (CUI).

NIST SP 800-171 Rev. 2, Requirement 3.1.1

States that organizations must "limit system access to authorized users and implement adequate security protections to prevent unauthorized disclosure."

CMMC 2.0 Documentation (Level 1 and Level 2 Requirements)

Requires that organizationsapply adequate security measures in accordance with NIST SP 800-171to meet compliance standards.

Analyzing the Given OptionsOfficial References Supporting the Correct AnswerConclusionThe term" adequate security"is the correct answer because it is explicitly defined in federal cybersecurity frameworks asprotection proportional to risk and potential consequences. Thus, the verified answer is:

Question #:168 - [CMMC Model Overview]

A company is about to conduct a press release. According to AC.L1-3.1.22: Control information posted or processed on publicly accessible systems, what is the MOST important factor to consider when addressing CMMC requirements?

A. That the information is correct

B. That the CEO approved the message

C. That the company has to safeguard the release of FCI

D. That so long as the information is only FCI, it can be released

Answer: C

Explanation

AC.L1-3.1.22states:"Control information posted or processed on publicly accessible systems."

This control requires organizations toensure that FCI (Federal Contract Information) is not publicly postedor made accessible in an uncontrolled manner.

FCI must beprotected from unauthorized disclosure, even if it is not classified or CUI.

Reference:

NIST SP 800-171, Requirement 3.1.22

CMMC Level 1 Practice AC.L1-3.1.22

Step 2: Why Safeguarding FCI is Critical in a Press ReleaseIf the company releases apress statementthat includesFCI, it must ensure that the information is not inadvertently exposing sensitive contract-related data.

FCI includesinformation provided by or generated for theDoD under a contractthat isnot intended for public release.

Organizations mustimplement controlsto prevent unintentional exposure.

Step 3: Why Other Answer Choices Are IncorrectA. That the information is correct (Incorrect):

While accuracy is important,CMMC requirements focus on protecting sensitive information, not just ensuring correctness.

B. That the CEO approved the message (Incorrect):

CEO approval does not satisfy CMMC compliance, as it does not address safeguarding FCI.

D. That so long as the information is only FCI, it can be released (Incorrect):

FCI must be protected and cannot be publicly disclosed unless specifically authorizedby the DoD.

Final Confirmation of Correct Answer:The company must safeguard FCI and ensure that no unauthorized disclosures occur in a public press release.

Thus, the correct answer is:C. That the company has to safeguard the release of FCI

Question #:169 - [CMMC Model Overview]

What is the BEST document to find the objectives of the assessment of each practice?

A. CMMC Glossary

B. CMMC Appendices

C. CMMC Assessment Process

D. CMMC Assessment Guide Levels 1 and 2

Answer: D

Explanation

1. Understanding the Role of Assessment Objectives in CMMC 2.0Theassessment objectivesfor each CMMC practice define thespecific criteriathat an assessor uses to evaluate whether a practice is implemented

correctly. These objectives break down each control into measurable components, ensuring a structured and consistent assessment process.

To determine where these objectives are best documented, we need to consider theofficial CMMC documentation sources.

2. Why Answer Choice "D" is Correct – CMMC Assessment Guide Levels 1 and 2TheCMMC Assessment Guide (Levels 1 & 2)is theprimary documentthat provides:

#The detailedassessment objectivesfor each practice

#A breakdown of the expectedevidence and implementation details

#Step-by-stepassessment criteriafor assessors to verify compliance

Each CMMC practice in the Assessment Guide is aligned with the correspondingNIST SP 800-171 or FAR 52.204-21 control, and the guide specifies:

How to assess compliancewith each practice

What evidenceis required for validation

What stepsan assessor should follow

#Reference from Official CMMC Documentation:

CMMC Assessment Guide – Level 2 (Aligned with NIST SP 800-171)explicitly states:

"Each practice is assessed based on defined assessment objectives to determine if the practice is MET or NOT MET."

CMMC Assessment Guide – Level 1 (Aligned with FAR 52.204-21)provides similar objectives tailored for foundational cybersecurity requirements.

Thus,CMMC Assessment Guide Levels 1 & 2 are the BEST sources for assessment objectives.

3. Why Other Answer Choices Are IncorrectOption

Reason for Elimination

A. CMMC Glossary

#The glossary only defines terminology used in CMMC but does not provide assessment objectives.

B. CMMC Appendices

#The appendices contain supplementary details, but they do not comprehensively list assessment objectives for each practice.

C. CMMC Assessment Process (CAP)

#While the CAP document describes the assessmentworkflow and methodology, it does not outline the specific objectives for each practice.

4. ConclusionTo locate thebest reference for assessment objectives, theCMMC Assessment Guide Levels 1 & 2are the most authoritative and detailed sources. They contain step-by-step assessment criteria, ensuring that practices are evaluated correctly.

#Final Answer:

D. CMMC Assessment Guide Levels 1 and 2

Question #:170 - [CMMC Assessment Process (CAP)]

Who will verify the adequacy and sufficiency of evidence to determine whether the practices and related components for each in-scope Host Unit, Supporting Organization/Unit, or enclave have been met?

A. OSC

B. Assessment Team

C. Authorizing official

D. Assessment official

Answer: B

Explanation

Per the CMMC Assessment Process (CAP), the Assessment Team is responsible for determining the adequacy and sufficiency of evidence collected during the assessment. The team validates whether practices and components for each in-scope Host Unit, Supporting Organization, or enclave meet the target CMMC level. The OSC (Organization Seeking Certification) provides evidence, but only the Assessment Team makes the verification and scoring determination.

Reference Documents:

- CMMC Assessment Process (CAP), v1.0

Question #:171 - [CMMC Ecosystem]

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?

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 2InCMMC Level 2, theConfiguration Management (CM) domainis critical for ensuring that systems aresecurely configured, maintained, and monitoredto prevent unauthorized changes. One key aspect of CM is managinguser-installed software, which can introducesecurity risksif not properly controlled.

The correct approach to managinguser-installed softwarealigns withCM.3.068fromNIST SP 800-171, which requires organizations to:

#Establish and enforce configuration settingsto ensure security.

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

Why "Controlled and Monitored" is Correct?The CCP (Certified CMMC Professional) conducting theinterviewshould focus on whether theuser-installed softwareiscontrolled and monitoredto align withCMMC Level 2 requirements. This means verifying:

Approval processesfor user-installed software.

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

Policies that restrict unauthorized installationsto prevent security risks.

Breakdown of Answer ChoicesOption

Description

Correct?

A. Controlled and monitored

#Ensures compliance with CM.3.068, verifying that user-installed software ismanaged securely.

#Correct

B. Removed from the system

Software isnot always removed—only unauthorized or risky software should be.

#Incorrect

C. Scanned for malicious code

While scanning isimportant(covered in SI.3.218), it isnot the primary focusof Configuration Management.

#Incorrect

D. Limited to mission-essential use only

While limiting software is useful,monitoring and controllingis 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 withNIST SP 800-171 security controls.

Official Reference from CMMC 2.0 DocumentationFinal Verification and ConclusionThe correct answer isA. Controlled and monitored, as perCM.3.068inNIST SP 800-171andCMMC 2.0documentation.

Question #:172 - [CMMC Assessment Process (CAP)]

A Lead Assessor has been assigned to a CMMC Assessment During the assessment, one of the assessors approaches with a signed policy. There is one signatory, and that person has since left the company. Subsequently, another person was hired into that position but has not signed the document. Is this document valid?

A. The signatory is the authority to implement and enforce the policy, and since that person is no longer with the company, the policy is not valid.

B. More research on the company policy of creating, implementing, and enforcing policies is needed. If the company has a policy identifying the authority as with the position or person, then the policy is valid.

C. The signatory does not validate or invalidate the policy. For the purpose of this assessment, ensuring that the policy is current and is being implemented by the individuals who are performing the work is sufficient.

D. The authority to implement and enforce lies with the position, not the person. As long as that position's authority and responsibilities have not been removed from implementing that domain, it is still a valid policy.

Answer: C

Explanation

Understanding Policy Validation in CMMC AssessmentsDuring a CMMC assessment, policies must be evaluated based on:

Who has the authority to approve and enforce them

Whether they are current and implemented effectively

The validity of a policydoes not solely depend on the signatorybut rather onhow the organization assigns authority for policy creation, approval, and enforcement.

Some organizations assignauthority to a specific person, meaning anew signatory may be requiredwhen leadership changes.

Others assign authority to aposition/title(e.g., CISO, IT Director), in which casea new signature may not be requiredas long as the role remains responsible for policy enforcement.

The assessment teammust review the organization's policy management processto determine if the policy remains valid despite leadership turnover.

Key Considerations in Policy Validation:Thus,the correct answer is B, as additional research is needed to confirm whether the organization's policy is tied to the individual or the position.

A. The signatory is the authority to implement and enforce the policy, and since that person is no longer with the company, the policy is not valid.#Incorrect. This assumes thatauthority is always tied to a person, which is not always the case. Some organizations delegate authorityto a position, not an individual.

C. The signatory does not validate or invalidate the policy. For the purpose of this assessment, ensuring that the policy is current and is being implemented by the individuals who are performing the work is sufficient. #Incorrect. While implementation is crucial,the authority behind the policy must also be validatedper CMMC documentation requirements.

D. The authority to implement and enforce lies with the position, not the person. As long as that position's authority and responsibilities have not been removed from implementing that domain, it is still a valid policy. #Incorrect. This assumes thatauthority is always assigned to a position, which is not universally true. More research is required to confirm this.

Why the Other Answers Are Incorrect

CMMC Assessment Process (CAP) Document– Outlines the importance of verifying the authority and enforcement of policies.

NIST SP 800-171 (3.12.1 - Security Policies and Procedures)– Requires that policies be maintained and enforced by appropriate personnel.

CMMC Official ReferencesThus,option B (More research on the company policy is needed) is the correct answer, as per official CMMC policy validation guidance.

Question #:173 - [CMMC Ecosystem]

A test or demonstration is being performed for the Assessment Team during an assessment. Which environment MUST the OSC perform this test or demonstration?

A. Client

B. Production

C. Development

D. Demonstration

Answer: B

Explanation

During aCMMC Level 2 assessment, assessors requireobjective evidencethat security controls are implementedin the actual operating environmentwhereControlled Unclassified Information (CUI)is handled.

This means thattests or demonstrations must be conducted in the production environment, where the organization’s real systems and security controls are in use.

Assessment teams need to validate security controls in the actual environment where they are applied, ensuring that security measures are in effect in thereal-world operating conditions.

Option A (Client)is incorrect because "Client" is not a defined assessment environment.

Option C (Development)is incorrect because testing in a development environmentdoes not accurately represent the production security posture.

Option D (Demonstration)is incorrect becausedemonstrations in a separate test environment do not provide valid evidence for CMMC assessments—actual security implementations must be verified in production.

CMMC Assessment Process (CAP) Guide – Section 3.5 (Assessment Methods)

NIST SP 800-171 Assessment Procedures(Verification must occur in the actual system where CUI resides.)

Understanding the Assessment Environment RequirementWhy Option B (Production) is CorrectOfficial CMMC Documentation ReferencesFinal VerificationSinceCMMC assessments require security controls to be validated in the actual production environment, the correct answer isOption B: Production.

Question #:174 - [CMMC Model Overview]

Which assessment method describes the process of reviewing, inspecting, observing, studying, or analyzing assessment objects (i.e., specification, mechanisms, activities)?

A. Test

B. Assess

C. Examine

D. Interview

Answer: C

Explanation

Understanding the "Examine" Assessment Method in CMMC 2.0CMMC 2.0 usesthree assessment methodsto evaluate security compliance:

Examine– Reviewing, inspecting, observing, studying, or analyzing assessment objects (e.g., policies, system documentation).

Interview– Speaking with personnel to verify knowledge and responsibilities.

Test– Performing technical validation to check system configurations.

TheCMMC Assessment Process (CAP)definesExamineas the method used toreview or analyze assessment objects, such as policies, procedures, configurations, and logs.

Relevant CMMC 2.0 Reference:

A. Test # Incorrect

"Test" involvesexecutinga function to validate its security (e.g., verifying access controls through a live system test).

B. Assess # Incorrect

"Assess" is a broad term; CMMC explicitly defines "Examine" as the method for reviewing documentation.

C. Examine # Correct

"Examine" is the official term forreviewing policies, procedures, configurations, or logs.

D. Interview # Incorrect

"Interview" involvesverbal discussions with personnel, not document analysis.

Why is the Correct Answer "Examine" (C)?

CMMC Assessment Process (CAP) Document

Defines "Examine" asanalyzing assessment objects (e.g., policies, procedures, logs, documentation).

NIST SP 800-171A

Specifies "Examine" as a method toreview security controls and configurations.

CMMC 2.0 References Supporting this Answer:

Question #:175 - [CMMC Model Overview]

How many domains does the CMMC Model consist of?

A. 14 domains

B. 43 domains

C. 72 domains

D. 110 domains

Answer: A

Explanation

TheCMMC Model consists of 14 domains, which are based on theNIST SP 800-171 control familieswith additional cybersecurity practices.

Eachdomaincontainspractices and processesthat define cybersecurity requirements for organizations seeking CMMC certification.

Reference:

CMMC 2.0 Model Documentation

NIST SP 800-171 Framework

Step 2: List of 14 CMMC DomainsAccess Control (AC)

Asset Management (AM)(Introduced in CMMC 2.0 for scoping guidance)

Audit and Accountability (AU)

Awareness and Training (AT)

Configuration Management (CM)

Identification and Authentication (IA)

Incident Response (IR)

Maintenance (MA)

Media Protection (MP)

Personnel Security (PS)

Physical Protection (PE)

Risk Management (RM)

Security Assessment (CA)

System and Communications Protection (SC)

Step 3: Why Other Answer Choices Are IncorrectB. 43 domains (Incorrect):

The CMMC model does not have43 domains; this number is incorrect.

C. 72 domains (Incorrect):

There are72 practices in CMMC Level 2, but not72 domains.

D. 110 domains (Incorrect):

110 refers to the number of security controls in NIST SP 800-171, which aligns withCMMC Level 2, but these are controls, not domains.

Final Confirmation of Correct Answer:The CMMC Model consists of 14 domains based on NIST SP 800-171 control families.

Thus, the correct answer is:A. 14 domains

Question #:176 - [CMMC Assessment Process (CAP)]

An assessor is in Phase 3 of the CMMC Assessment Process. The assessor has delivered the final findings, submitted the assessment results package, and provided feedback to the C3PAO and CMMC-AB. What must the assessor still do?

A. Determine level recommendation

B. Archive all assessment artifacts

C. Determine final practice pass/fail results

D. Archive or dispose of any assessment artifacts

Answer: D

Explanation

In Phase 3 (Post-Assessment), the assessor’s responsibility is to archive or dispose of assessment artifacts according to the C3PAO’s policies and retention requirements. By this point, final findings and results have already been delivered, so the only remaining step is ensuring proper handling of assessment materials.

Supporting Extracts from Official Content:

- CAP v2.0, Post-Assessment Activities (§3.17): “The assessor must archive or dispose of any assessment artifacts in accordance with the C3PAO’s retention and destruction policy.”

Why Option D is Correct:

- Determining practice pass/fail results and level recommendations occurs earlier in Phases 2 and 3.

- The final step left for the assessor is the proper archiving or destruction of artifacts.

References (Official CMMC v2.0 Content):

- CMMC Assessment Process (CAP) v2.0, Phase 3: Post-Assessment (§3.17).

===========

Question #:177 - [CMMC Model Overview]

Which domain has a practice requiring an organization to restrict, disable, or prevent the use of nonessential programs?

A. Access Control (AC)

B. Media Protection (MP)

C. Asset Management (AM)

D. Configuration Management (CM)

Answer: D

Explanation

Understanding the Role of Configuration Management (CM) in CMMC 2.0TheConfiguration Management (CM) domainin CMMC 2.0 ensures that systems aresecurely configured and maintainedto prevent unauthorized or unnecessary changes that could introduce vulnerabilities. One key requirement in CM is torestrict, disable, or prevent the use of nonessential programsto reduce security risks.

Relevant CMMC 2.0 Practice:CM.L2-3.4.1 – Establish and enforce security configuration settings for information technology products employed in organizational systems.

This practicerequires organizations to control system configurations, including the removal or restriction ofnonessential programs, functions, ports, and servicestoreduce attack surfaces.

The goal is tominimize exposure to cyber threatsby ensuring only necessary and approved software is running on the system.

A. Access Control (AC) # Incorrect

Access Control (AC) focuses onmanaging user permissions and accessto systems and data, not restricting programs.

B. Media Protection (MP) # Incorrect

Media Protection (MP) deals withprotecting and controlling removable media(e.g., USBs, hard drives) rather than software or system configurations.

C. Asset Management (AM) # Incorrect

Asset Management (AM) is aboutidentifying and tracking IT assets, not configuring or restricting software.

D. Configuration Management (CM) # Correct

CM explicitly coverssecuring system configurationsbyrestricting nonessential programs, ports, services, and functions, making it the correct answer.

Why is the Correct Answer CM (D)?

CMMC 2.0 Practice CM.L2-3.4.1(Security Configuration Management)

Requires organizations toenforce security configuration settingsandremove unnecessary programsto protect systems.

NIST SP 800-171 Requirement 3.4.1

Supportssecure configuration settingsandrestricting unauthorized applicationsto prevent security risks.

CMMC 2.0 Level 2 Requirement

This practice is aLevel 2 (Advanced) requirement, meaningorganizations handling Controlled Unclassified Information (CUI)must comply with it.

CMMC 2.0 References Supporting this Answer:

Question #:178 - [CMMC Ecosystem]

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

A. Ability

B. Eligibility

C. Capability

D. Suitability

Answer: B

Explanation

What Happens in Phase 4 of the CMMC Assessment Process?Phase 4 of theCMMC Assessment Process (CAP)is theFinal Reporting and Decision Phase. During this phase, theLead Assessormust:

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 hasmet the required practices and processes.

Confirm that anydeficiencieshave been corrected or appropriately documented.

Recommendwhether the OSC is eligible for certificationbased on assessment results.

Key Responsibilities of the Lead Assessor in Phase 4:Since theLead Assessor must determine and recommend the OSC's eligibilityto the C3PAO, the correct answer isB. 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 abouteligibilityfor certification.

C. Capability#Incorrect. Capability refers to an organization'stechnical and operational readiness. The Lead Assessor is making a recommendation oneligibility, not just capability.

D. Suitability#Incorrect. Suitability is not a defined term in theCMMC CAP processfor final assessment recommendations. The correct term iseligibility.

Why the Other Answers Are Incorrect

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

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

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

Question #:179 - [CMMC Model Overview]

What type of information is NOT intended for public release and is provided by or generated for the government under a contract to develop or deliver a product or service to the government, but not including information provided by the government to the public (such as on public websites) or simple transactional information, such as necessary to process payments?

A. CDI

B. CTI

C. CUI

D. FCI

Answer: D

Explanation

Understanding Federal Contract Information (FCI)Federal Contract Information (FCI) is defined by48 CFR 52.204-21(Basic Safeguarding of Covered Contractor Information Systems). FCI refers to information that:

Is NOT intended for public release.

Is provided by or generated for the government under a contract.

Is necessary to develop or deliver a product or service to the government.

Excludes publicly available government information(such as information on public websites).

Excludes simple transactional information(e.g., necessary to process payments).

In the context ofCMMC 2.0, organizations thatprocess, store, or transmit FCImust meetCMMC Level 1 (Foundational), which requires implementing17 basic safeguarding practicesoutlined inFAR 52.204-21.

A. CDI (Controlled Defense Information)# Incorrect

This term was used inDFARS 252.204-7012but has been replaced byCUI (Controlled Unclassified Information)in CMMC discussions.

B. CTI (Cyber Threat Intelligence)# Incorrect

This refers to intelligence on cyber threats, tactics, and indicators, not contractual data.

C. CUI (Controlled Unclassified Information)# Incorrect

CUI is sensitive information requiring additional safeguarding but is a separate category from FCI.

D. FCI (Federal Contract Information)#Correct

The definition of FCI explicitly matches the description given in the question.

Why is the Correct Answer FCI (D)?

FAR 52.204-21 (Basic Safeguarding of Covered Contractor Information Systems)

Defines FCI and the required safeguards.

Establishes17 cybersecurity practicesfor FCI protection.

CMMC 2.0 Framework

Level 1 (Foundational)is required for contractors handlingFCI.

Ensures compliance withbasic safeguarding requirementsoutlined inFAR 52.204-21.

NIST SP 800-171 and DFARS 252.204-7012

FCI doesnotrequire compliance withNIST SP 800-171, butCUI does.

CMMC 2.0 References Supporting this Answer:

Question #:180 - [CMMC Ecosystem]

A CCP is part of a CMMC Assessment Team interviewing a subject-matter expert on Access Control (AC) within an OSC. During the interview process, what will the CCP ensure about the information exchanged during the interview?

A. Performed in groups for more efficient use of resources

B. Recorded for inclusion in the Final Recommended Findings report

C. Confidential and non-attributable so interviewees can speak without fear of reprisal

D. Mapped to specific CMMC practices to clearly delineate which practice is being evaluated

Answer: C

Explanation

Understanding the Role of a CCP in CMMC AssessmentsACertified CMMC Professional (CCP)is responsible for assistingCertified CMMC Assessors (CCA)in evaluating anOrganization Seeking Certification (OSC)during a CMMC assessment. One key aspect of this process isconducting interviewswith Subject Matter Experts (SMEs) to verify security practices.

Ensuring that interviewees canspeak freely without fear of retaliationiscriticalto obtainingaccurate and unbiased informationabout the implementation of security controls.

CMMC Assessment Process and the Role of Interviews

TheCMMC Assessment Guide (Level 2)outlines that interviews are conducted to confirm that security practices are effectively implemented.

Interviewees mustfeel comfortable sharing candid responseswithout concern that their statements will lead tonegative consequenceswithin the organization.

Ensuring Confidentiality and Non-Attribution

DoD Assessment Methodologyspecifies that interviews should be conductedconfidentiallytoprotect the identity of interviewees.

TheCMMC Code of Professional Conduct (CoPC)for assessors and professionals reinforces the requirement to maintain theconfidentialityof assessment participants.

Non-attributionensures that responses are used for evaluation purposeswithout linking statements to specific individuals.

Why the Other Answer Choices Are Incorrect:

(A) Performed in groups for more efficient use of resources:

Group interviews may prevent individuals from speaking openly.

Employees might be hesitant to contradict leadership or peers.

(B) Recorded for inclusion in the Final Recommended Findings report:

Interviews arenot directly recorded or attributedin assessment reports.

Instead, findings are documentedwithout identifying specific individuals.

(D) Mapped to specific CMMC practices to clearly delineate which practice is being evaluated:

While responsesinformwhich practices are being assessed, theprimary goalof an interview is to ensure accurate,unbiased information gathering.

Step-by-Step Breakdown:Final Validation from CMMC Documentation:According to theCMMC Assessment Guide and DoD Assessment Methodology, interview confidentiality iscrucialto gatheringaccurateandunbiasedresponses. This makesconfidentiality and non-attributionthe correct answer.

Thus, the correct answer is:

C. Confidential and non-attributable so interviewees can speak without fear of reprisal.

Question #:181 - [CMMC Assessment Process (CAP)]

For a CMMC Level 2 certification, which organization maintains a non-disclosure agreement with the OSC?

A. NIST

B. C3PAO

C. CMMC-AB

D. OUSD A&S

Answer: B

Explanation

The Certified Third-Party Assessment Organization (C3PAO) enters into a contractual relationship with the OSC. As part of that contract, the C3PAO maintains a non-disclosure agreement (NDA) to protect sensitive and proprietary information reviewed during the assessment.

Supporting Extracts from Official Content:

- CAP v2.0, Roles and Responsibilities (§2.8): “The C3PAO maintains a non-disclosure agreement with the OSC to protect all sensitive information disclosed during the assessment.”

Why Option B is Correct:

- Only the C3PAO contracts directly with the OSC and is bound to protect assessment data.

- NIST, The Cyber AB (formerly CMMC-AB), and OUSD A&S do not enter NDAs directly with OSCs.

References (Official CMMC v2.0 Content):

- CMMC Assessment Process (CAP) v2.0, Section on OSC–C3PAO agreements.

===========

Question #:182 - [Governance and Source Documents]

Which words summarize categories of data disposal described in the NIST SP 800-88 Revision 1. Guidelines for Media Sanitation?

A. Clear, purge, destroy

B. Clear redact, destroy

C. Clear, overwrite, purge

D. Clear, overwrite, destroy

Answer: A

Explanation

Understanding NIST SP 800-88 Rev. 1 and Media SanitizationTheNIST Special Publication (SP) 800-88 Revision 1, Guidelines for Media Sanitization, provides guidance onsecure disposalof data from various types of storage media to prevent unauthorized access or recovery.

Clear

Useslogical techniquesto remove data from media, making it difficult to recover usingstandard system functions.

Example:Overwriting all datawith binary zeros or ones on a hard drive.

Applies to:Magnetic media, solid-state drives (SSD), and non-volatile memorywhen the media isreused within the same security environment.

Purge

Usesadvanced techniquesto make data recoveryinfeasible, even with forensic tools.

Example:Degaussinga magnetic hard drive orcryptographic erasure(deleting encryption keys).

Applies to:Media that is leaving organizational control or requires a higher level of assurance than "Clear".

Destroy

Physicallydamages the mediaso that data recovery isimpossible.

Example:Shredding, incinerating, pulverizing, or disintegratingstorage devices.

Applies to:Highly sensitive data that must be permanently eliminated.

B. Clear, Redact, Destroy (Incorrect)– "Redact" is a term used for document sanitization,notdata disposal.

C. Clear, Overwrite, Purge (Incorrect)– "Overwrite" is a method within "Clear," but it isnot a top-level categoryin NIST SP 800-88.

D. Clear, Overwrite, Destroy (Incorrect)– "Overwrite" is a sub-method of "Clear," but "Purge" is missing, making this incorrect.

The correct answer isA. Clear, Purge, Destroy, as these are thethree official categoriesof data disposal inNIST SP 800-88 Revision 1.

References:

NIST SP 800-88 Rev. 1 – Guidelines for Media Sanitization

CMMC 2.0 Security Practices Related to Media Disposal(Aligned with NIST guidance)

Question #:183 - [Governance and Source Documents]

Which resource contains authoritative data classifications of CUI?

A. NARA

B. CMMC-AB

C. DoD Contractors FAQ

D. OSC's privacy policies

Answer: A

Explanation

The National Archives and Records Administration (NARA) serves as the authoritative body overseeing the Controlled Unclassified Information (CUI) program within the United States federal government. NARA maintains the CUI Registry, which is the definitive resource for all categories, subcategories, and associated markings of CUI. This registry provides comprehensive guidance on the identification and handling of CUI, ensuring standardized practices across federal agencies and their contractors.

The other options are delineated as follows:

CMMC-AB:The Cybersecurity Maturity Model Certification Accreditation Body is responsible for overseeing the CMMC program but does not manage CUI classifications.

DoD Contractors FAQ:While it may offer guidance to Department of Defense contractors, it is not an authoritative source for CUI data classifications.

OSC's privacy policies:An Organization Seeking Certification's internal policies pertain to its own data handling practices and are not authoritative for CUI classifications.

Therefore, for authoritative information on CUI data classifications, the NARA's CUI Registry is the appropriate resource.

Question #:184 - [CMMC Model Overview]

In the CMMC Model, how many practices are included in Level 2?

A. 17 practices

B. 72 practices

C. 110 practices

D. 180 practices

Answer: C

Explanation

CMMC Level 2is designed to alignfullywithNIST SP 800-171, which consists of110 security controls (practices).

This meansall 110 practicesfrom NIST SP 800-171 are required for aCMMC Level 2 certification.

How Many Practices Are Included in CMMC Level 2?Breakdown of Practices in CMMC 2.0CMMC Level

Number of Practices

Level 1

17 practices(Basic Cyber Hygiene)

Level 2

110 practices(Aligned with NIST SP 800-171)

Level 3

Not yet finalized but expected to exceed 110

Since CMMC Level 2 mandatesall 110 NIST SP 800-171 practices, the correct answer isC. 110 practices.

A. 17 practices#Incorrect.17 practicesapply only toCMMC Level 1, not Level 2.

B. 72 practices#Incorrect. There is no CMMC level with72 practices.

D. 180 practices#Incorrect. CMMC Level 2only requires 110 practices, not 180.

Why the Other Answers Are Incorrect

CMMC 2.0 Model– Confirms thatLevel 2 includes 110 practicesaligned withNIST SP 800-171.

NIST SP 800-171 Rev. 2– Outlines the110 security controlsrequired for handlingControlled Unclassified Information (CUI).

CMMC Official ReferencesThus,option C (110 practices) is the correct answer, as per official CMMC guidance.

Question #:185 - [CMMC Ecosystem]

When are data and documents with legacy markings from or for the DoD required to be re-marked or redacted?

A. When under the control of the DoD

B. When the document is considered secret

C. When a document is being shared outside of the organization

D. When a derivative document's original information is not CUI

Answer: C

Explanation

Background on Legacy Markings and CUI

Legacy markings refer to classification labels used before the implementation of theControlled Unclassified Information (CUI) ProgramunderDoD Instruction 5200.48.

Documents with legacy markings (such as “For Official Use Only” (FOUO) or “Sensitive But Unclassified” (SBU)) must be reviewed for re-marking or redaction to align withCUI requirements.

When Must Legacy Markings Be Updated?

If the document is retained internally (Answer A - Incorrect): Documents under DoD control do not require immediate re-marking unless they are being shared externally.

If the document is classified as Secret (Answer B - Incorrect): This question is aboutCUI, not classified information. Secret-level documents follow different marking rules underDoD Manual 5200.01.

If a document is being shared externally (Answer C - Correct):

According toDoD Instruction 5200.48, Section 3.6(a), organizations mustreview legacy markings before sharing documents outside the organization.

The document must bere-markedin compliance with the CUI Program before dissemination.

If the original document does not contain CUI (Answer D - Incorrect): The original source document's status does not affect the requirement to re-mark a derivative document if it contains CUI.

Conclusion

The correct answer isC: Documents with legacy markings must bere-marked or redacted when being shared outside the organizationto comply with DoD CUI guidelines.

DoD Instruction 5200.48(Controlled Unclassified Information)

CUI Marking Handbook by NARA(National Archives and Records Administration)

CMMC 2.0 Scoping Guide for CUI Environments

Question #:186 - [Implementation and Scoping]

Which example represents a Specialized Asset?

A. SOCs

B. Hosted VPN services

C. Consultants who provide cybersecurity services

D. All property owned or leased by the government

Answer: D

Explanation

Understanding Specialized Assets in CMMCASpecialized Assetis defined asa system, device, or infrastructure component that is not a traditional IT system but still plays a role in cybersecurity or business operations.

Types of Specialized Assets (as per CMMC guidance):#Operational Technology (OT)– Industrial control systems, SCADA systems.

#Security Operations Centers (SOCs)– Dedicated cybersecurity monitoring and response centers.

#IoT Devices– Smart sensors, embedded systems.

#Restricted IT Systems– Systems with highly controlled access.

A. SOCs # Correct

Security Operations Centers (SOCs) are specialized cybersecurity environmentsused forthreat monitoring, detection, and response.

They oftenoperate outside standard IT infrastructureand are classified asspecialized assetsunder CMMC.

B. Hosted VPN services # Incorrect

VPN services are standard IT infrastructureanddo not qualify as specialized assets.

C. Consultants who provide cybersecurity services # Incorrect

Consultants are personnel, not specialized assets. Specialized assets refer tosystems, devices, or infrastructure.

D. All property owned or leased by the government # Incorrect

Government property is not automatically considered a specialized assetunder CMMC. Specialized assets refer tospecific IT or cybersecurity-related infrastructure.

Why is the Correct Answer "SOCs" (A)?

CMMC 2.0 Assessment Process (CAP) Document

DefinesSpecialized Assetsand includesSOCsin its examples.

CMMC-AB Guidelines

Listssecurity infrastructure like SOCsasSpecialized Assetsdue to their unique cybersecurity function.

NIST SP 800-171 & CMMC 2.0 Security Domains

Recognizesdedicated security monitoring environmentsas part of an organization's cybersecurity posture.

CMMC 2.0 References Supporting This Answer:

Final Answer:#A. SOCs (Security Operations Centers)

Question #:187 - [CMMC Model Overview]

What service is the MOST comprehensive that the RPO provides?

A. Training services

B. Education services

C. Consulting services

D. Assessment services

Answer: C

Explanation

Understanding the Role of a Registered Provider Organization (RPO)ARegistered Provider Organization (RPO)is an entity recognized by theCMMC Accreditation Body (CMMC-AB)to provideconsulting servicesto organizations seekingCMMC certification.

Key Functions of an RPO#Consulting servicesto help companies prepare for CMMC assessments.

#Guidance on security controlsrequired for compliance.

#Assistance with documentation, policy development, and gap analysis.

#Preparation for third-party CMMC assessmentsbutdoes not conduct official CMMC assessments(this is the role of a C3PAO).

Consulting servicesare thebroadest and most comprehensivefunction of an RPO.

RPOs do not conduct assessments(eliminating option D).

Training and educationmay be part of consulting but arenot the primary function(eliminating A and B).

Consulting includes training, guidance, documentation assistance, and security readiness, making it themost comprehensive service offered.

Why "Consulting Services" is the Correct Answer?Breakdown of Answer ChoicesOption

Description

Correct?

A. Training services

#Incorrect–RPOs may provide training, but this isnot their primary function.

B. Education services

#Incorrect–Similar to training, butnot the most comprehensive service.

C. Consulting services

#Correct – The core function of an RPO is consulting, which includes various readiness services.

D. Assessment services

#Incorrect–Only aC3PAO (Certified Third-Party Assessment Organization)can conductofficial CMMC assessments.

TheCMMC-AB RPO Programdefines an RPO as aconsulting organization that assists companies in preparing for CMMC certificationbutdoes not perform assessments.

Official References from CMMC 2.0 DocumentationFinal Verification and ConclusionThe correct answer isC. Consulting services, asRPOs primarily provide advisory and readiness supportto organizations preparing forCMMC compliance.

Question #:188 - [CMMC Model Overview]

Which term describes the prevention of damage to. protection of, and restoration of computers and electronic communications systems/services, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation?

A. Cybersecurity

B. Data security

C. Network security

D. Information security

Answer: A

Explanation

The term that describes"the prevention of damage to, protection of, and restoration of computers and electronic communication systems/services, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation"isCybersecurity.

Step-by-Step Breakdown:#1. Cybersecurity Defined

Cybersecurityfocuses onprotecting networks, systems, and datafrom cyber threats.

It includes measures to ensure:

Availability(data is accessible when needed).

Integrity(data is accurate and unaltered).

Authentication(verifying users' identities).

Confidentiality(ensuring only authorized access).

Non-repudiation(preventing denial of actions).

The definition in the questionaligns directly with cybersecurity principles, making it the best answer.

#2. Why the Other Answer Choices Are Incorrect:

(B) Data Security#

Data securityfocusesspecificallyon protectingstored information(e.g., encryption, access controls), but cybersecurity is broader—it includesnetworks, systems, and communication services.

(C) Network Security#

Network securityis asubset of cybersecuritythat focuses on protectingnetwork infrastructure(e.g., firewalls, intrusion detection systems).

The definition in the question includesmore than just networks, so cybersecurity is the better choice.

(D) Information Security#

Information security (InfoSec)is related but broader than cybersecurity.

InfoSeccoversphysical and organizational security(e.g., policies, procedures) in addition todigital protections.

CMMC and NIST SP 800-171 define cybersecurityas the protection ofsystems, networks, and data from cyber threats.

DoD Cybersecurity Definitions(aligned with NIST) confirm that cybersecurity is the term thatbest fits the definition in the question.

Final Validation from CMMC Documentation:

Question #:189 - [CMMC Model Overview]

Which term describes the process of granting or denying specific requests to obtain and use information, related information processing services, and enter specific physical facilities?

A. Access control

B. Physical access control

C. Mandatory access control

D. Discretionary access control

Answer: A

Explanation

Understanding Access Control in CMMCAccess control refers to the process ofgranting or denyingspecific requests to:

Obtain and use information

Access information processing services

Enter specific physical locations

TheAccess Control (AC) domain in CMMCis based onNIST SP 800-171 (3.1 Access Control family)and includes requirements to:

#Implement policies for granting and revoking access.

#Restrict access to authorized personnel only.

#Protect physical and digital assets from unauthorized access.

Since the questionbroadly asks about the process of granting or denying access to information, services, and physical locations, the correct answer isA. Access Control.

B. Physical access control#Incorrect.Physical access controlis asubsetof access control that only applies tophysical locations(e.g., keycards, security guards, biometrics). The question includesinformation and services, makinggeneral access controlthe correct choice.

C. Mandatory access control (MAC)#Incorrect.MAC is a specific type of access controlwhere access is strictly enforced based onsecurity classifications(e.g., Top Secret, Secret, Confidential). The questiondoes not specify MAC, so this is incorrect.

D. Discretionary access control (DAC)#Incorrect.DAC is another specific type of access control, whereownersof data decide who can access it. The question asksgenerallyabout granting/denying access, makingaccess control (A)the best answer.

Why the Other Answers Are Incorrect

CMMC 2.0 Model - AC.L2-3.1.1 to AC.L2-3.1.22– Covers access control requirements, includingcontrolling access to information, services, and physical spaces.

NIST SP 800-171 (3.1 - Access Control Family)– Defines the general principles of access control.

CMMC Official ReferencesThus,option A (Access Control) is the correct answer, as it best aligns withCMMC access control requirements.

Question #:190 - [CMMC Assessment Process (CAP)]

For CMMC Assessments, during Phase 1 of the CMMC Assessment Process, which are responsible for identifying potential conflicts of information?

A. C3PAO and OSC

B. OSC and CMMC-AB

C. CMMC-AB and C3PAO

D. Lead Assessor and Assessment Team Members

Answer: D

Explanation

In Phase 1 (Planning) of the CMMC Assessment Process, the Lead Assessor is responsible for managing the team and identifying conflicts of interest. Assessment team members must also disclose potential conflicts.

Supporting Extracts from Official Content:

- CAP v2.0, Planning (§2.5–2.8): “The Lead Assessor and Assessment Team Members must identify and disclose any conflicts of interest prior to conducting the assessment.”

Why Option D is Correct:

- Only the Lead Assessor and assessment team are responsible for identifying conflicts of interest during Phase 1.
- Options A, B, and C incorrectly assign this role to organizations that do not hold the responsibility.

References (Official CMMC v2.0 Content):

- CMMC Assessment Process (CAP) v2.0, Phase 1 Planning responsibilities.

===========

Question #:191 - [Roles and Responsibilities]

Which statement BEST describes the key references a Lead Assessor should refer to and use the:

A. DoD adequate security checklist for covered defense information.

B. CMMC Model Overview as it provides assessment methods and objects.

C. safeguarding requirements from FAR Clause 52.204-21 for a Level 2 Assessment.

D. published CMMC Assessment Guide practice descriptions for the desired certification level.

Answer: D

Explanation

Key References for a Lead Assessor in a CMMC AssessmentALead Assessorconducting aCMMC assessmentmust rely onofficial CMMC guidance documentsto evaluate whether anOrganization Seeking Certification (OSC)meets the required cybersecurity practices.

TheCMMC Assessment Guideprovidesdetailed descriptionsof eachpractice and processat the specificCMMC level being assessed.

It defines:#Theassessment objectivesfor each practice.#Therequired evidencefor compliance.#Thescoring criteriato determine if a practice isMET or NOT MET.

Most Relevant Reference: CMMC Assessment Guide

A. DoD adequate security checklist for covered defense information # Incorrect

TheDoD adequate security checklistis related toDFARS 252.204-7012 compliance, butCMMC assessmentsfollow theCMMC Assessment Guide.

B. CMMC Model Overview as it provides assessment methods and objects # Incorrect

TheCMMC Model Overviewprovideshigh-level guidance, butdoes not contain specific assessment criteria.

C. Safeguarding requirements from FAR Clause 52.204-21 for a Level 2 Assessment # Incorrect

FAR 52.204-21is relevant toCMMC Level 1 (FCI protection), butCMMC Level 2 follows NIST SP 800-171and requiresCMMC Assessment Guidesfor validation.

D. Published CMMC Assessment Guide practice descriptions for the desired certification level # Correct

TheCMMC Assessment Guideis theofficial documentused to determine if anOSC meets the required security practices for certification.

Why is the Correct Answer "D. Published CMMC Assessment Guide practice descriptions for the desired certification level"?

CMMC Assessment Process (CAP) Document

Specifies thatLead Assessors must use the CMMC Assessment Guidefor official scoring.

CMMC Assessment Guide for Level 1 & Level 2

Providesdetailed descriptions, assessment methods, and scoring criteriafor each practice.

CMMC-AB Guidance for Certified Third-Party Assessment Organizations (C3PAOs)

Confirms thatCMMC assessments must follow the Assessment Guide, not general DoD security policies.

CMMC 2.0 References Supporting This Answer:

Final Answer:#D. Published CMMC Assessment Guide practice descriptions for the desired certification level.

Question #:192 - [CMMC Assessment Process (CAP)]

Which standard of assessment do all C3PAO organizations execute an assessment methodology based on?

A. ISO 27001

B. NISTSP800-53A

C. CMMC Assessment Process

D. Government Accountability Office Yellow Book

Answer: C

Explanation

Understanding the C3PAO Assessment MethodologyACertified Third-Party Assessment Organization (C3PAO)is an entity authorized by theCMMC Accreditation Body (CMMC-AB)to conduct officialCMMC Level 2 assessmentsfor organizations seeking certification.

C3PAOs must follow theCMMC Assessment Process (CAP), which outlines:#Theassessment methodologyfor evaluating compliance.#Evidence collectionprocedures (interviews, artifacts, testing).#Assessment scoring and reportingrequirements.#Guidance for assessorson executing standardized assessments.

ISO 27001 (Option A)is an international standard forinformation security managementbut isnot the basis for CMMC assessments.

NIST SP 800-53A (Option B)providessecurity control assessments for federal systems, but CMMC assessments arebased on NIST SP 800-171.

GAO Yellow Book (Option D)is agovernment auditing standardused forfinancial and performance audits, not cybersecurity assessments.

CMMC Assessment Process (CAP) (Option C) is the correct answerbecause it defines how C3PAOs conduct CMMC assessments.

CMMC Assessment Process Guide (CAP)– GovernsC3PAO assessment execution.

CMMC 2.0 Model Documentation– RequiresC3PAOs to follow CAP proceduresfor assessments.

Key Requirement: CMMC Assessment Process (CAP)Why "CMMC Assessment Process" is Correct?Official References from CMMC 2.0 DocumentationFinal Verification and ConclusionThe correct answer isC. CMMC Assessment Process, as it is theofficial methodology all C3PAOs must follow when conducting CMMC assessments.

Question #:193 - [CMMC Model Overview]

An Assessment Team is conducting interviews with team members about their roles and responsibilities. The team member responsible for maintaining the antivirus program knows that it was deployed but has very little knowledge on how it works. Is this adequate for the practice?

A. Yes, the antivirus program is available, so it is sufficient.

B. Yes, antivirus programs are automated to run independently.

C. No, the team member must know how the antivirus program is deployed and maintained.

D. No, the team member's interview answers about deployment and maintenance are insufficient.

Answer: C

Explanation

For a practice to beadequately implementedin aCMMC Level 2 assessment, theresponsible personnel must demonstrate knowledge of deployment, maintenance, and operationof security tools such asantivirus programs. Simply having the tool in place isnot sufficient—there must be evidence that it isproperly configured, updated, and monitoredto protect against threats.

Step-by-Step Breakdown:#1. Relevant CMMC and NIST SP 800-171 Requirements

CMMC Level 2 aligns with NIST SP 800-171, which includes:

Requirement 3.14.5 (System and Information Integrity - SI-3):

"Employautomatedmechanisms toidentify, report, and correctsystem flaws in a timely manner."

Requirement 3.14.6 (SI-3(2)):

"Employautomated toolsto detect and prevent malware execution."

These requirements imply that theperson responsible for antivirus must understand how it is deployed and maintainedto ensure compliance.

#2. Why the Team Member's Knowledge is Insufficient

Antivirus tools requireregular updates,configuration adjustments, andmonitoringto function properly.

The responsible team member must:

Knowhow the antivirus was deployedacross systems.

Be able toconfirm updates, logs, and alerts are monitored.

Understand how torespond to malware detectionsand failures.

If the team member lacks this knowledge, assessors maydetermine the practice is not fully implemented.

#3. Why the Other Answer Choices Are Incorrect:

(A) Yes, the antivirus program is available, so it is sufficient.#

Incorrect:Just having antivirus softwareinstalleddoes not prove compliance. It must bemanaged and maintained.

(B) Yes, antivirus programs are automated to run independently.#

Incorrect:While automation helps, security toolsrequire oversight, updates, and configuration.

(D) No, the team member's interview answers about deployment and maintenance are insufficient.#

Partially correct but incomplete:Themain issueis that the team membermust have sufficient knowledge, not just that their answers are weak.

Final Validation from CMMC Documentation:TheCMMC Assessment Guide for SI-3 and SI-3(2)states that personnel mustunderstand the function, deployment, and maintenance of security toolsto ensure proper implementation.

Thus, the correct answer is:

Question #:194 - [CMMC Model Overview]

An organization that manufactures night vision cameras is looking for help to address the gaps identified in physical access control systems. Which certified individual should they approach for implementation support?

A. CCA of the C3PAO performing the assessment

B. RP of an organization not part of the assessment

C. Practitioner of the organization performing the assessment LTP

D. DoD Contract Official of the organization performing the assessment

Answer: B

Explanation

Anorganization seeking helpto address security gaps—such asphysical access control deficiencies—needs acertified professional who can provide implementation supportwithoutbeing involved in the actual CMMC assessment.

A Registered Practitioner (RP)is a CMMC-certified individualwho provides consulting and implementation supportto organizations butdoes not perform assessments.

RPs work independently from C3PAOsand canassist in fixing gapsin security controlsbeforeorafteran assessment.

Since RPs are not assessors, they can provide direct remediation supportwithout any conflict of interest.

The OSC needs assistance in implementing security controls(not assessment).

An RP is trained and authorized to provide remediation and advisory services.

Conflict of interest rules prevent the assessing C3PAO from providing implementation support.

A. CCA of the C3PAO performing the assessment (Incorrect)

ACertified CMMC Assessor (CCA)is responsible for conducting the assessmentonly.

TheC3PAO performing the assessment cannot also provide remediationdue to aconflict of interest.

C. Practitioner of the Organization Performing the Assessment LTP (Incorrect)

The assessmentLead Technical Practitioner (LTP)cannot provide remediation support for an OSC they are assessing.

D. DoD Contract Official of the Organization Performing the Assessment (Incorrect)

DoD Contract Officialsoversee contract compliance butdo not provide cybersecurity implementation support.

The correct answer isB. RP of an organization not part of the assessment, asonly independent RPs can assist with remediation and implementation support.

References:

CMMC 2.0 Registered Practitioner (RP) Program

CMMC Code of Professional Conduct (CoPC) Conflict of Interest Policy

CMMC 2.0 Assessment Process (CAP) Guide

Question #:195 - [CMMC Model Overview]

Which authority leads the CMMC direction, standards, best practices, and knowledge framework for how to map the controls and processes across different Levels that range from basic cyber hygiene to advanced cyber practices?

A. NIST

B. DoD CIO office

C. Federal CIO office

D. Defense Federal Acquisition Regulation Council

Answer: B

Explanation

Understanding the Role of the DoD CIO Office in CMMCTheDepartment of Defense (DoD) Chief Information Officer (CIO) officeis theprimary authorityresponsible for leading the direction, standards, and best practices of theCybersecurity Maturity Model Certification (CMMC)framework.

The DoD CIO Oversees CMMC Policy and Implementation

TheDoD CIO Office is responsible for the governance and strategic direction of CMMC.

It ensures thatCMMC aligns with DoD cybersecurity policies, such asDoD Instruction 5200.48 (Controlled Unclassified Information)andNIST SP 800-171.

CMMC Development and Evolution

TheDoD CIO played a critical role in launching CMMCto improve cybersecurity across theDefense Industrial Base (DIB).

The CIO office leadspolicy development and updates to the CMMC framework, including the transition fromCMMC 1.0 to CMMC 2.0.

Alignment of CMMC with Federal Cybersecurity Strategy

The DoD CIO ensures that CMMCintegrates with federal cybersecurity policiesandNIST frameworks.

It provides oversight formapping CMMC Levels (1-2-3) to existing cybersecurity standards and controls.

A. NIST (Incorrect)

TheNational Institute of Standards and Technology (NIST)provides thetechnical framework (NIST SP 800-171, SP 800-172), butNIST does not lead the CMMC program.

C. Federal CIO Office (Incorrect)

TheFederal CIO focuses on broader government IT policiesandnot specifically on DoD cybersecurity requirementslike CMMC.

D. Defense Federal Acquisition Regulation Council (Incorrect)

TheDFARS Counciloverseescontracting regulationsrelated to CMMC (e.g.,DFARS 252.204-7012, 7019, 7020, 7021), but it doesnot lead CMMC standards and best practices.

The correct answer isB. DoD CIO Office, as it isthe lead authority guiding the CMMC framework, standards, and implementation across the Defense Industrial Base (DIB).

References:

DoD CIO Website on CMMC

CMMC 2.0 Overview by DoD

DoD Instruction 5200.48 (CUI Program)

DFARS 252.204-7012 & CMMC 2.0 Policy Documents

Question #:196 - [CMMC Model Overview]

Who will verify the adequacy and sufficiency of evidence to determine whether the practices and related components for each in-scope Host Unit. Supporting Organization/Unit, or enclave has been met?

A. OSC

B. Assessment Team

C. Authorizing official

D. Assessment official

Answer: B

Explanation

Who Verifies the Adequacy and Sufficiency of Evidence?In the CMMC assessment process, it is theAssessment Teamthat is responsible for verifying whether thepractices and related componentshave been met for each in-scopeHost Unit, Supporting Organization/Unit, or enclave.

TheCMMC Assessment Teamis composed of certified assessors and led by aCertified CMMC Assessor (CCA). Their primary role is to:

Review evidenceprovided by theOrganization Seeking Certification (OSC).

Determine compliancewith required CMMC practices and processes.

Evaluate the sufficiencyof evidence to confirm that all required practices have been properly implemented.

Document and report findingsto the CMMC Accreditation Body (CMMC-AB).

Breakdown of Answer ChoicesOption

Description

Correct?

A. OSC (Organization Seeking Certification)

The OSC provides documentation and evidence but doesnotverify its adequacy.

#Incorrect

B. Assessment Team

#Responsible for verifying the adequacy and sufficiency of evidence.

#Correct

C. Authorizing Official

Typically refers to an official responsible for system accreditation underNIST RMF, not CMMC.

#Incorrect

D. Assessment Official

Not a defined role in the CMMC framework.

#Incorrect

TheCMMC Assessment Process Guide(CAP) outlines theAssessment Team'sresponsibility in verifying evidence.

TheCMMC Assessment Teamevaluates whether theorganization's cybersecurity practices meet CMMC requirements.

Official Reference from CMMC 2.0 DocumentationFinal Verification and ConclusionThe correct answer isB. Assessment Team, as per CMMC 2.0 documentation and official assessment processes.

Question #:197 - [CMMC Assessment Process (CAP)]

The Assessment Team has completed the assessment and determined the preliminary practice ratings. The preliminary practice ratings must be shared with the OSC prior to being finalized for submission. Based on this information, the assessor should present the preliminary practice ratings:

A. During the final Daily Checkpoint

B. After discussing with the CMMC-AB

C. Via email after the final Daily Checkpoint

D. Over the phone after the final Daily Checkpoint

Answer: A

Explanation

According to the CMMC Assessment Process (CAP) v2.0, assessors are required to conduct Daily Checkpoint Meetings at the end of each day to summarize progress with the OSC (Organization Seeking Certification). The final Daily Checkpoint is where preliminary practice ratings are shared, before the quality assurance review and Out-Brief. The Out-Brief is reserved for the presentation of final results. Additionally, Department of Defense regulations (32 CFR §170.17(c)(2)) provide a 10-business-day re-evaluation window for requirements marked NOT MET before the final report is delivered, which necessitates that the OSC see preliminary ratings during the assessment process itself.

Supporting Extracts from Official Content:

- CAP v2.0, §2.23: “The assessment team shall host a Daily Checkpoint Meeting with the OSC at the end of each assessment day to summarize progress.”

- CAP v2.0, §3.7: “The C3PAO shall conduct the quality assurance review… prior to the conduct of the Out-Brief Meeting.”

- CAP v2.0, §3.10: “The purpose of the Out-Brief Meeting is to convey the results of the assessment to the OSC.”

- 32 CFR §170.17(c)(2): “A security requirement assessed as NOT MET may be re-evaluated… for 10 business days… if the CMMC Assessment Findings Report has not been delivered.”

Why Option A is Correct:

- The CAP specifies that Daily Checkpoint Meetings are the formal, structured mechanism for assessors to communicate progress and preliminary findings to the OSC.
- The final Daily Checkpoint provides the OSC with visibility into the preliminary practice ratings before they are finalized, ensuring transparency and alignment.
- The Out-Brief is explicitly for conveying the final assessment results after the C3PAO has completed QA.
- Federal regulation (32 CFR §170.17(c)(2)) requires the OSC to have access to preliminary results so they can provide additional evidence for re-evaluation before the report is locked, further confirming that this exchange must occur at the final Daily Checkpoint.

References (Official CMMC v2.0 Content):

- CMMC Assessment Process (CAP) v2.0: Sections 2.23 (Daily Checkpoints), 3.7–3.10 (QA and Out-Brief).
- 32 CFR §170.17(c)(2): Security Requirement Re-evaluation Window.
- DoD CMMC Assessment Guide – Level 2 (v2.13): Guidance on MET/NOT MET determinations and findings.

Question #:198 - [CMMC Ecosystem]

A C3PAO is conducting High Level Scoping for an OSC that requested an assessment Which term describes the people, processes, and technology that will be applied to the contract who are requesting a CMMC Level assessment?

A. Host Unit

B. Branch Office

C. Coordinating Unit

D. Supporting Organization/Units

Answer: A

Explanation

Understanding High-Level Scoping in a CMMC AssessmentDuringHigh-Level Scoping, aCertified Third-Party Assessment Organization (C3PAO)determines thepeople, processes, and technologythat are within scope for theCMMC Level 1 or Level 2 assessment.

Supporting Organization/Unitsrefer to thespecific groups, departments, or teamsthat handleControlled Unclassified Information (CUI)orFederal Contract Information (FCI)and are responsible for applyingCMMC security practices.

These units aredirectly involved in the contract's executionand are included in the CMMC assessment scope.

Key Term: Supporting Organization/Units

A. Host Unit # Incorrect

This term is not used inCMMC assessment scoping.

B. Branch Office # Incorrect

Abranch officemay or may not be in scope; scoping is based onwhether the unit handles CUI or FCI, not its physical location.

C. Coordinating Unit # Incorrect

No official CMMC term refers to a "Coordinating Unit."

D. Supporting Organization/Units # Correct

This termcorrectly describes the entities that apply security controls for the contract and are within the CMMC assessment scope.

Why is the Correct Answer "D. Supporting Organization/Units"?

CMMC Scoping Guidance for Level 1 & Level 2 Assessments

DefinesSupporting Organization/Unitsasin-scope entities responsible for implementing cybersecurity controls.

CMMC Assessment Process (CAP) Document

Specifies that theC3PAO must identify and document the units responsible for security compliance.

DoD CMMC 2.0 Guidance on Scoping

Requires theassessment team to define the people, processes, and technology that fall within the scopeof the assessment.

CMMC 2.0 References Supporting This Answer:

Question #:199 - [Governance and Source Documents]

Which statement BEST describes the requirements for a C3PA0?

A. An authorized C3PAO must meet some DoD and all ISO/IEC 17020 requirements.

B. An accredited C3PAO must meet all DoD and some ISO/IEC 17020 requirements.

C. AC3PAO must be accredited by DoD before being able to conduct assessments.

D. A C3PAO must be authorized by CMMC-AB before being able to conduct assessments.

Answer: D

Explanation

Understanding C3PAO RequirementsACertified Third-Party Assessment Organization (C3PAO)is an entityauthorized by the CMMC Accreditation Body (CMMC-AB)to conductCMMC Level 2 Assessmentsfor organizations handlingControlled Unclassified Information (CUI).

Key Requirements for a C3PAO to Conduct Assessments:#Must be authorized by CMMC-AB before conducting assessments.

#Must meet CMMC-AB and DoD cybersecurity and process requirements.

#Must comply with ISO/IEC 17020 standards for inspection bodies.

#Must undergo a rigorous vetting process, including cybersecurity verification.

A. An authorized C3PAO must meet some DoD and all ISO/IEC 17020 requirements # Incorrect

C3PAOs must comply with CMMC-AB authorization requirementsbefore performing assessments.

While they must align withISO/IEC 17020, they donotnecessarily meet all requirements upfront.

B. An accredited C3PAO must meet all DoD and some ISO/IEC 17020 requirements # Incorrect

C3PAOs are not accredited by DoD; they areauthorized by CMMC-ABto perform assessments.

Accreditation follows full compliance with CMMC-AB and ISO/IEC 17020 requirements.

C. A C3PAO must be accredited by DoD before being able to conduct assessments # Incorrect

The DoD does not directly accredit C3PAOs—CMMC-AB is responsible forauthorization and oversight.

D. A C3PAO must be authorized by CMMC-AB before being able to conduct assessments # Correct

CMMC-AB grants authorization to C3PAOs, allowing them to perform assessmentsonly after meeting specific requirements.

Why is the Correct Answer "D" (A C3PAO must be authorized by CMMC-AB before being able to conduct assessments)?

CMMC-AB Certified Third-Party Assessment Organization (C3PAO) Guidelines

States thatC3PAOs must receive CMMC-AB authorization before conducting assessments.

CMMC 2.0 Assessment Process (CAP) Document

Specifies that onlyC3PAOs authorized by CMMC-AB can conduct official CMMC assessments.

ISO/IEC 17020 Compliance for C3PAOs

Defines theinspection body requirements for C3PAOs, which must be met for accreditation.

CMMC 2.0 References Supporting This Answer:

Question #:200 - [CMMC Assessment Process (CAP)]

While determining the scope for a company's CMMC Level 1 Self-Assessment, the contract administrator includes the hosting providers that manage their IT infrastructure. Which asset type BEST describes the third-party organization?

A. ESPs

B. People

C. Facilities

D. Technology

Answer: A

Explanation

When a company usesthird-party IT providersto manage their infrastructure, these organizations are classified asExternal Service Providers (ESPs)underCMMC scoping guidelines.

Step-by-Step Breakdown:#1. What is an ESP?

External Service Providers (ESPs)arethird-party organizationsthat:

ProvideIT services, cloud hosting, and managed security solutions.

Process, store, or transmit FCI or CUIon behalf of a contractor.

Mustmeet the same security requirementsas the OSC if they handle FCI or CUI.

If a company relies ona hosting provider to manage IT infrastructure, that provider is anESPunderCMMC scoping guidelines.

#2. Why the Other Answer Choices Are Incorrect:

(B) People#

Incorrect:ESPs areorganizations, not individual people.

(C) Facilities#

Incorrect:Facilities refer tophysical locationslike office buildings or data centers, not third-partyservice providers.

(D) Technology#

Incorrect:While ESPs provide technology services, the correct term forthird-party IT providersunder CMMC isESPs, not just "Technology."

TheCMMC Level 1 Scoping GuidedefinesExternal Service Providers (ESPs)asthird-party organizations that manage IT infrastructure and security services.

Final Validation from CMMC Documentation:Thus, the correct answer is:

#A. ESPs (External Service Providers).

Question #:201 - [CMMC Ecosystem]

An assessor has been working with an OSC's point of contact to plan and prepare for their upcoming assessment. What is one of the MOST important things to remember when analyzing requirements for an assessment?

A. Scoping an assessment is easy and worry-free.

B. The initial plan cannot be changed once agreed upon.

C. There is a determined amount of time that the OSC's point of contact has to submit evidence and rough order-of-magnitude.

D. Assessors need to continuously review and update the requirements and plan for the assessment as information is gathered.

Answer: D

Explanation

Planning and preparing for aCMMC assessmentinvolves collaboration between theassessorand theOrganization Seeking Certification (OSC)to determine scope, required evidence, and logistics. This planning process isdynamicand must adapt as new information emerges.

Assessment Scope and Requirements May Change

As assessors gather evidence and analyze the environment,new details about assets, networks, and security controlsmay require adjustments to the assessment plan.

TheCMMC Assessment Process (CAP) Guideemphasizes that assessmentrequirements and scope should be continuously reviewed and updatedto reflect real-time findings.

Assessors Follow an Adaptive Approach

DuringCMMC assessments, organizations may discover additionalFCI or CUI assets, which can change the required security practices to be evaluated.

Assessors shouldrevise the assessment approach accordinglyrather than strictly following an initial, unchangeable plan.

A. Scoping an assessment is easy and worry-free#Incorrect

Scoping is acritical and complex processthat requires careful evaluation of the OSC’s information systems and assets.

CMMC Scoping Guidestates thatidentifying in-scope assets is crucial and requires significant effort.

B. The initial plan cannot be changed once agreed upon#Incorrect

Theinitial assessment plan is a starting point, butit must be flexiblebased on real-time findings.

CMMC CAP Guideemphasizescontinuous refinementduring the assessment process.

C. There is a determined amount of time that the OSC's point of contact has to submit evidence and rough order-of-magnitude#Incorrect

While there aretimelines, the key focus is ensuring thatall necessary evidence is gathered accuratelyrather than rushing to meet a strict deadline.

CMMC Assessment Process (CAP) Guide– States that assessment requirements and planning should be updated as additional information is gathered.

CMMC Scoping Guide (Nov 2021)– Explains that assessors must continually refinein-scope assets and requirementsthroughout the process.

Why the Correct Answer is "D"?Why Not the Other Options?Relevant CMMC 2.0 References:Final Justification:Assessment planning is a dynamic process.Assessors must continuously review and update the requirements and planas new information emerges, makingDthe correct answer.

Question #:202 - [CMMC Ecosystem]

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?

A. CCP

B. C3PAO

C. Lead Assessor

D. Advisory Board

Answer: C

Explanation

During aCMMC readiness review, anOrganization Seeking Certification (OSC)may argue that a specificenclave (network segment or system) is out of scopefor assessment. TheLead Assessor is responsible for verifying and approving this request.

Certified CMMC Professional (CCP)

A CCP supports OSCs inpreparing for assessmentsbutdoes not make final scope determinations.

Certified Third-Party Assessment Organization (C3PAO)

The C3PAOoversees the assessmentbut doesnot personally verify scope exclusions—that falls under theLead Assessor’s role.

Lead Assessor (Correct Answer)

TheLead Assessor has the authorityto determine if anenclave is out of scopebased on OSC-provided evidence.

The Lead Assessor followsCMMC Assessment Process (CAP) guidelinesto ensure proper scoping.

Advisory Board

TheCMMC-AB (Advisory Board) does not make scope determinations. It focuses onprogram oversightandcertification processes.

CMMC Assessment Process (CAP) v1.0

TheLead Assessor is responsible for confirming the assessment scopeand determining enclave applicability.

CMMC Scoping Guidance for Level 2 Assessments

Requires theLead Assessor to review and approve any enclave exclusionsbefore finalizing the assessment scope.

Roles and Responsibilities in CMMC Assessments:Official References Supporting the Correct Answer: Conclusion:TheLead Assessoris the correct answer because they have the authority to verify scope determinations during the assessment.

#Correct Answer: C. Lead Assessor

Question #:203 - [Governance and Source Documents]

Which regulation allows for whistleblowers to sue on behalf of the federal government?

A. NISTSP 800-53

B. NISTSP 800-171

C. False Claims Act

D. Code of Professional Conduct

Answer: C

Explanation

Understanding the False Claims Act (FCA) and Whistleblower ProtectionsTheFalse Claims Act (FCA)(31 U. S.C. §§ 3729–3733) is aU.S. federal lawthat allowswhistleblowers (also known as "relators")to sue on behalf of the federal government if they believe a company issubmitting fraudulent claimsfor government funds.

The FCA includes a"qui tam" provision, which:

#Allows private individuals to file lawsuits on behalf of the U.S. government.

#Provides financial rewards to whistleblowersif the lawsuit results in recovered funds.

#Protects whistleblowers from employer retaliation.

In the context ofCMMC and cybersecurity compliance, theFCA has been used to hold companies accountableformisrepresenting their cybersecurity compliancewhen working with federal contracts.

For example:

If a companyfalsely claimscompliance withCMMC, NIST SP 800-171, or DFARS 252.204-7012butfails to meet security requirements, it could beliable under the FCA.

TheDepartment of Justice (DOJ)has pursued cases under theCyber-Fraud Initiative, using theFCA against defense contractorsfor cybersecurity noncompliance.

Thus, the correct answer isC. False Claims Actbecause it specifically allows whistleblowers tosue on behalf of the federal government.

A. NIST SP 800-53#Incorrect.NIST SP 800-53provides security controls for federal agencies butdoes notcontain whistleblower provisions.

B. NIST SP 800-171#Incorrect.NIST SP 800-171outlines security requirements for protectingCUI, but itdoes not have legal mechanismsfor whistleblower lawsuits.

D. Code of Professional Conduct#Incorrect. TheCMMC Code of Professional Conductapplies toC3PAOs and assessorsbut doesnot provide a legal basis for whistleblower lawsuits.

Why the Other Answers Are Incorrect

False Claims Act (31 U.S.C. §§ 3729–3733)– Establishes whistleblower protections and qui tam lawsuits.

DOJ Cyber-Fraud Initiative– Uses the FCA to enforce cybersecurity compliance in government contracts.

DFARS 252.204-7012 & CMMC– Require accurate reporting of cybersecurity compliance, which can lead to FCA violations if misrepresented.

CMMC Official ReferencesThus,option C (False Claims Act) is the correct answeras per official legal guidance.

Question #:204 - [CMMC Model Overview]

Which CMMC Levels focus on protecting CUI from exfiltration?

A. Levels 1 and 2

B. Levels 1 and 3

C. Levels 2 and 3

D. Levels 1, 2, and 3

Answer: C

Explanation

- Level 1 only addresses the protection of Federal Contract Information (FCI) and does not include requirements for safeguarding Controlled Unclassified Information (CUI).
- Level 2 is explicitly designed to protect Controlled Unclassified Information (CUI). It requires implementation of all 110 security requirements from NIST SP 800-171 Rev. 2, which directly support the safeguarding of CUI and help prevent its unauthorized disclosure or exfiltration.
- Level 3 builds on Level 2 by including a subset of requirements from NIST SP 800-172. These additional practices are designed to enhance the protection of CUI against advanced persistent threats (APTs), further strengthening defenses against exfiltration.

Therefore, the levels that focus on protecting CUI from exfiltration are Levels 2 and 3.

Reference Documents:

- CMMC Model v2.0 Overview (DoD, December 2021)
- NIST SP 800-171 Rev. 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
- NIST SP 800-172, Enhanced Security Requirements for Protecting Controlled Unclassified Information

Question #:205 - [CMMC Ecosystem]

An OSC lead has provided company information, identified that they are seeking CMMC Level 2, stated that they handle FCI. identified stakeholders, and provided assessment logistics. The OSC has provided the company's cyber hygiene practices that are posted on every workstation, visitor logs, and screenshots of the configuration of their FedRAMP-approved applications. The OSC has not won any DoD government contracts yet but is working on two proposals Based on this information, which statement BEST describes the CMMC Level 2 Assessment requirements?

A. Ready because there is no need to certify this company until after they win a DoD contract.

B. Not ready because the OSC is not on contract because they do not know the scope of FCI protection required by the contract.

C. Not ready because the OSC still lacks artifacts that prove they have implemented all the CMMC Level 2 Assessment requirements.

D. Ready because all DoD contractors are required to achieve CMMC Level 2; therefore, they are being proactive in seeking certification.

Answer: C

Explanation

CMMC Level 2 Readiness and Certification RequirementsCMMCLevel 2is required forOrganizations Seeking Certification (OSCs) that handle Controlled Unclassified Information (CUI)and aligns withNIST SP 800-171's 110 security controls.

Key Readiness Indicators for a Level 2 Assessment:

The OSC must have implemented all 110 security practices from NIST SP 800-171.

Documented and validated cybersecurity policies and procedures must exist.

The OSC must be prepared to provide objective evidence (artifacts) proving compliance.

Why the OSC in the Question is Not Ready:

They have not won a DoD contract yet# This means they do not yet have a contractually definedCUI environment, which is the foundation for defining their security scope.

They have only provided FCI-related artifacts(e.g., visitor logs, workstation policies, FedRAMP configurations).

Lack of full documentation of CMMC Level 2 controls# The assessment requiresevidence for all 110 security practices(e.g., system security plans, incident response records, security awareness training documentation).

A. "Ready because there is no need to certify this company until after they win a DoD contract."

Incorrect# Some organizationsseek certification proactivelybefore winning contracts. However, readiness depends on implementingall 110 required controls, not contract status alone.

B. "Not ready because the OSC is not on contract because they do not know the scope of FCI protection required by the contract."

Incorrect# CMMC Level 2focuses on CUI, not just FCI. While FCI protection is important, the assessment's focus is onCUI security requirements, which arenot fully addressed by the provided artifacts.

D. "Ready because all DoD contractors are required to achieve CMMC Level 2; therefore, they are being proactive in seeking certification."

Incorrect# While it is commendable that the OSC is being proactive,readiness is based on full compliance with NIST SP 800-171, not just intent.

References:NIST SP 800-171 Rev. 2(NIST Official Site)

CMMC 2.0 Level 2 Assessment Guide(Cyber AB)

DFARS 252.204-7012 & CMMC 2.0 Requirements(DoD CIO)

#Final Answer: C. Not ready because the OSC still lacks artifacts that prove they have implemented all the CMMC Level 2 Assessment requirements.

Question #:206 - [CMMC Model Overview]

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

A. Level 1

B. Level 3

C. Levels 1 and 2

D. Levels 1, 2, and 3

Answer: D

Explanation

The CMMC Model v2.0 is cumulative. The Advanced Level (Level 3) requires full implementation of NIST SP 800-171 (aligned to Level 2) and adds a subset of additional practices from NIST SP 800-172. Because levels build on one another, the Access Control (AC) practices at Level 3 inherently include those from Level 1 (basic FCI protections), Level 2 (CUI protections), and additional Level 3 requirements.

Supporting Extracts from Official Content:

- CMMC Model v2.0 Overview: "The model is cumulative; practices at a higher level include the practices of all lower levels."
- Level 3 description: "Advanced… Expert Level requires implementation of NIST SP 800-171 plus a subset of NIST SP 800-172."

Why Option D is Correct:

- The Advanced Level includes all AC practices from Level 1 and Level 2, as well as the additional ones unique to Level 3.

- Therefore, it contains Access Control practices from Levels 1, 2, and 3.

References (Official CMMC v2.0 Content):

- CMMC Model v2.0, Overview of Levels (Cumulative nature of practices).

- NIST SP 800-171 and NIST SP 800-172 (control sources for Levels 2 and 3).

===========

About Exams4sure.com

Exams4sure.com was founded in 2007. We provide latest & high quality IT / Business Certification Training Exam Questions, Study Guides, Practice Tests.

We help you pass any IT / Business Certification Exams with 100% Pass Guaranteed or Full Refund. Especially Cisco, CompTIA, Citrix, EMC, HP, Oracle, VMware, Juniper, Check Point, LPI, Nortel, EXIN and so on.

View list of all certification exams: All vendors

We prepare state-of-the art practice tests for certification exams. You can reach us at any of the email addresses listed below.

- Sales: sales@exams4sure.com
- Feedback: feedback@exams4sure.com
- Support: support@exams4sure.com

Any problems about IT certification or our products, You can write us back and we will get back to you within 24 hours.