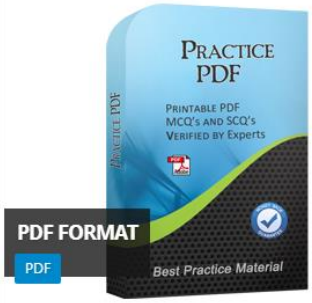
ActualVCE

- 24/7 customer support, Secure shopping site
- Free One year updates to match real exam scenarios
- If you failed your exam after buying our products we will refund the full amount back to you.

Download Demo

- Online Tool, Convenient, easy to study.
- Instant Online Access
- Supports All Web Browsers
- Practice Online Anytime
- Test History and Performance Review
- Supports Windows / Mac / Android / iOS, etc.

- Installable Software Application
- Simulates Real Exam Environment
- Builds Exam Confidence
- Supports MS Operating System
- Two Modes For Practice
- Practice Offline Anytime



- Printable PDF Format
- Prepared by IT Experts
- Instant Access to Download
- Study Anywhere, Anytime
- 365 Days Free Updates
- Free PDF Demo Available

Security & Privacy

ActualVCE respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

365 Days Free Updates

Free update is available within 365 days after your purchase. After 365 days, you will get 50% discounts for updating.

Instant Download

After Payment, our system will send you the products you purchase in mailbox in a minute after payment. If not received within 2 hours, please contact ActualVCE.

Try Before Buy

ActualVCE offers free demo of each product. You can check out the interface, question quality and usability of our practice exams before you decide to buy.

http://www.actualvce.com/

Believable Exam Dumps Questions grant you ensured success by your first attempt - ActualVCE

Exam : **CMMC-CCP**

Title : Certified CMMC Professional (CCP) Exam

Vendor : Cyber AB

Version : DEMO

NO.1 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.
Why "C3PAO" is Correct?
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.
Breakdown of Answer Choices
Option
Description
Correct?
A). C3PAO
#Correct - C3PAOs finalize and submit assessment results.
B). CMMC-AB
#Incorrect-The CMMC-AB accredits C3PAOs but 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.
Official References from CMMC 2.0 Documentation
CMMC Assessment Process Guide (CAP)- DefinesC3PAO authorityover final assessment results.
Final Verification and Conclusion
The correct answer isA. C3PAO, as theC3PAO has final decision-making authority over CMMC assessment results.

NO.2 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:

Control Reference: CA.L2-3.12.1

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.

Assessment Criteria & Justification for the Correct Answer:

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.

Official CMMC 2.0 References Supporting the 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." 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.

NO.3 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 Assessments

TheCMMC 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.)

Why the Other Answers Are Incorrect

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.

CMMC Official References

CMMC 2.0 Scoping Guide - Level 1 & Level 2

CMMC Assessment Process (CAP) Document

Thus,option D (All assets processing, storing, or transmitting FCI/CUI and security protection assets) is the correct answeras per official CMMC assessment scoping requirements.

NO.4 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 2.0

According 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.

Why Option C (Examine) is Correct

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.

Official CMMC Documentation References

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

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

Final Verification

Since the activity involves reviewing documents and records to verify access control measures, it falls under theExaminemethod, makingOption C the correct answer.

NO.5 A member of the Assessment Team has been assigned the responsibility of maintaining and protecting information from the OSC. The Assessment Results Package, PCI, CUI, and any notes must be retained and protected from disclosure. To protect the OSC's information, which principle should be used, and for how long?

A. Cryptography and hashing for 1 year

B. Confidentiality and non-disclosure for 3 years

C. Availability, confidentiality, and integrity for 1 year

D. Authentication, authorization, and accounting for 3 years

Answer: B

Explanation:

The core protection principle for OSC-provided assessment information (including PCI/CUI, assessment workpapers/notes, and the assessment results package) is confidentiality / non-disclosure . The CMMC rules require assessors not to disclose OSC information outside the assessment participants, except as required by law. For example, CMMC assessor requirements include not sharing information about an OSC obtained during pre-assessment and assessment

activities with anyone not involved in that specific assessment .
For retention, the authoritative requirement in the CMMC Program rule (32 CFR Part 170) is that assessment-related records are maintained for six (6) years , unless disposition is otherwise authorized by the CMMC PMO. This record set includes assessment materials and working papers generated during Level 2 certification assessments, and it also includes contractual agreements.
Important correction to the multiple-choice options: none of the answers list the official six-year retention period. The best available option is therefore B because it correctly captures the required confidentiality
/non-disclosure principle-but the " 3 years " duration in the option does not match the official CMMC v2.0 retention requirement (which is 6 years).

NO.6 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:
According to the CMMC Assessment Process (CAP), specifically during the Phase 3: Conduct Assessment (Evidence Collection and Verification), the Assessment Team must evaluate all collected artifacts, interview notes, and test results against two primary dimensions: Adequacy and Sufficiency.
Adequacy (The "Right" Evidence): This criterion focuses on the quality, relevance, and validity of the evidence. It addresses whether the evidence actually maps to the specific CMMC practice being assessed and whether it is authoritative (e.g., signed, current, and from a trusted source). If an assessor asks, "Is this therightpiece of information to prove this practice is met?" they are testing for Adequacy.
Sufficiency (The "Enough" Evidence): This criterion focuses on the quantity and scope of the evidence. It addresses whether the Assessment Team has collected enough data points (across the required number of assets and using the required methods of Examine, Interview, and Test) to reach a confident conclusion. If an assessor asks, "Do I haveenoughexamples of this practice in action across the entire enclave?" they are testing for Sufficiency.
Why other options are incorrect:
B and D (Objectivity/Subjectivity): While assessors must remain objective, these are not the formal "criteria" used to categorize the evidence collection quality within the CAP framework.
C (Sufficiency): As noted above, Sufficiency is about theamountof evidence, not whether it is thecorrect type (the "right" evidence).
Reference Documents:
CMMC Assessment Process (CAP) v1.0: Section 3.4, "Collect and Verify Evidence," which explicitly defines the requirement for evidence to be both adequate and sufficient.
CMMC Level 2 Assessment Guide: Guidance on the application of the Examine, Interview, and Test (E-I-T) methods to ensure evidence quality.
NIST SP 800-171A: The foundation for CMMC assessment procedures, which emphasizes the need for relevant (adequate) evidence to support findings.

NO.7 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." Final Validation from CMMC Documentation:

TheCMMC Level 1 Scoping GuidedefinesExternal Service Providers (ESPs)asthird-party organizations that manage IT infrastructure and security services.

Thus, the correct answer is:

#A. ESPs (External Service Providers).

NO.8 Within what amount of time MUST convictions, guilty pleas, or no contest pleas to crimes of fraud, larceny, embezzlement, misappropriation of funds, misrepresentation, perjury, false swearing, conspiracy to conceal, or a similar offense in any legal proceeding, civil or criminal, whether or not connected with activities that relate to carrying out a Lead Assessor role, be reported to the CMMC Accreditation Body?

A. 90 days.

B. 30 days.

C. 3 days.

D. 7 days.

Answer: B

Explanation:

The correct answer is B , 30 days. The official CMMC Program rule at 32 CFR Part 170 , Subpart C, requires CMMC ecosystem members to report certain criminal matters to the Accreditation Body

within 30 days . The rule specifically includes convictions, guilty pleas, and no contest pleas involving crimes such as fraud, larceny, embezzlement, misappropriation of funds, misrepresentation, perjury, false swearing, conspiracy to conceal, or similar offenses in civil or criminal legal proceedings. This requirement applies whether or not the offense is directly connected to the individual's CMMC ecosystem role.
This requirement is important because CMMC ecosystem roles, including Lead Assessors, depend on trustworthiness, professional integrity, impartiality, and reliability. A Lead Assessor participates in activities that may affect whether an OSC receives a CMMC certification, so criminal conduct involving dishonesty or misuse of funds is highly relevant to the integrity of the ecosystem. Option A , 90 days, is incorrect because the reporting window is shorter. Option C , 3 days, and option D , 7 days, are also incorrect because they do not match the official 30-day reporting requirement.
Although older training materials may use the term
"CMMC-AB," the current terminology commonly refers to the Accreditation Body or The Cyber AB.
The required reporting period remains 30 days .

NO.9 A CCP is consulting with an OSC. In the course of an interview, the OSC representative asks the CCP what basic safeguarding requirements must be met with respect to CMMC Level 1. The CCP tells the representative that this publication contains all the requirements from:

A. NIST SP 800-171.

B. DFARS Clause 252.202-7014.

C. DFARS Clause 252.204-7012.

D. FAR Clause 52.204-21.

Answer: D

Explanation:
The correct answer is D because CMMC Level 1 is based on the basic safeguarding requirements in FAR Clause 52.204-21 , not on the full NIST SP 800-171 or DFARS 252.204-7012 requirements. The official CMMC Model Overview states that Level 1 focuses on protecting Federal Contract Information (FCI) and consists of security requirements that correspond to the basic safeguarding requirements specified in 48 CFR
52.204-21 , commonly referred to as the FAR Clause. It also states that Level 2 is the level that incorporates the 110 security requirements from NIST SP 800-171 Rev. 2 for protection of Controlled Unclassified Information (CUI) .
FAR 52.204-21 applies to covered contractor information systems that process, store, or transmit Federal Contract Information. The clause requires contractors to apply basic safeguarding requirements and procedures, including limiting system access to authorized users, controlling external connections, protecting information on publicly accessible systems, identifying and authenticating users, and sanitizing or destroying media containing FCI before disposal or reuse.
Option A is incorrect because NIST SP 800-171 is associated with CMMC Level 2, not Level 1. Option B is incorrect because the cited DFARS clause number is not the CMMC Level 1 source. Option C is incorrect because DFARS 252.204-7012 is tied to safeguarding covered defense information and implementing NIST SP 800-171 for CUI, not the Level 1 basic safeguarding baseline.

NO.10 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.

Why "Lead Assessor" is Correct?

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.

Breakdown of Answer Choices

Option

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.

Official References from CMMC 2.0 Documentation

CMMC Assessment Process Guide (CAP)- Defines theLead Assessor's rolein determining assessment methods.

Final Verification and Conclusion

The correct answer isD. Lead Assessor, as they havefinal decision-making authority over the assessment methodology.

NO.11 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.

NO.12 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 CMMC
NIST 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 Choices
NIST 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 800-171
The 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.
Official Reference from CMMC 2.0 Documentation
CMMC 2.0 Level 2alignsdirectlywith NIST SP800-171 Rev. 2.
DoD contractors that handle CUImustcomply withall 110 controlsfrom NIST SP800-171.
Final Verification and Conclusion
The correct answer isD. NIST SP 800-171, as this documentexplicitly definesthe cybersecurity requirements for protectingCUI in nonfederal systems and organizations.

NO.13 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 CMMC
Access 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.

Why the Other Answers Are Incorrect
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.
CMMC Official References
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.
Thus,option A (Access Control) is the correct answer, as it best aligns withCMMC access control requirements.

NO.14 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 Activities
Objectivityin 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.
Why is the Correct Answer "C. Avoiding the appearance of or actual, conflicts of interest"?
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.
CMMC 2.0 References Supporting This Answer:
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.

NO.15 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:

NO.16 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.
Breaking Down the Scenario:
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.
Analysis of the Given Options:
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.
Official References Supporting the Correct Answer:
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.

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

NO.17 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:
According to the CMMC Assessment Process (CAP) and the C3PAO Authorization Requirements, every assessment conducted by a Certified Third-Party Assessment Organization (C3PAO) must undergo a formal Quality Management System (QMS) review before the results are finalized and uploaded to the eMASS (Enterprise Mission Assurance Support Service) or the SPRS (Supplier Performance Risk System).
The Quality Review Requirement: The CAP explicitly states that the C3PAO is responsible for the accuracy and integrity of the assessment findings. Before the Assessment Team Lead can formally submit the package, a person or team within the C3PAO (who was ideally not part of the active assessment team to ensure objectivity) must conduct an internal review. This review ensures that the evidence collected supports the
"Met" or "Not Met" determinations and that all CMMC methodology requirements were followed.
Why other options are incorrect:
Option A: While there may be administrative costs associated with maintaining C3PAO status, paying a specific "per-submission fee" is not a mandatory procedural stepwithin the assessment lifecyclethat governs the validity of the results.
Option C: The Cyber AB (CMMC-AB) provides the platform and oversight, but a "forthcoming notification" is not a formal requirement in the CAP; the act of submission itself serves as the notification.
Option D: While a final briefing is a "best practice" and usually occurs during the "Post-Assessment" phase, the internal quality review (Option B) is the regulatory mandate that must be completed to ensure the C3PAO's certification of the results is valid and defensible.
Reference Documents:
CMMC Assessment Process (CAP) v1.0: Section on "Phase 4: Reporting Results," specifically the sub-section on C3PAO Quality Assurance Review.
C3PAO Quality Management System (QMS) Requirements: Outlines the necessity for internal validation of assessment packages to maintain accreditation.

NO.18 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 Sanitization
TheNIST 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.
Three Categories of Data Disposal in NIST SP 800-88 Rev. 1
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.
Why "A. Clear, Purge, Destroy" is Correct?
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.
Conclusion
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)

NO.19 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) Key Responsibilities of the Lead Assessor in Phase 4:
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.
Since theLead Assessor must determine and recommend the OSC's eligibilityto the C3PAO, the correct answer isB. Eligibility.
Why the Other Answers Are Incorrect
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.
CMMC Official References
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.
Thus,option B (Eligibility) is the correct answer, as per official CMMC guidance.

NO.20 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.
Step-by-Step Breakdown:
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.
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.

NO.21 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.
Final Validation from CMMC Documentation:
TheCMMC Assessment Guide (Level 2)explicitly states that assessment procedures are derived fromNIST SP
800-171A.
Thus, the correct answer is:

NO.22 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 Assessment
During 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 Why "D. Final and recorded Daily Checkpoint log" is Correct?
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.
Why Other Answers Are Incorrect?
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.
Conclusion
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

NO.23 Which term describes a group of individuals that conduct operational network vulnerability evaluations and provide mitigation techniques to customers?

A. Red team

B. Blue team

C. White hat hackers

D. Penetration test team

Answer: D

Explanation:
The best match is Penetration test team because penetration testing is an authorized, structured security evaluation intended to find vulnerabilities in systems or networks and produce results that enable remediation/mitigation .
Authoritatively, NIST SP 800-115 (Technical Guide to Information Security Testing and Assessment) is a primary federal reference for technical security testing. It describes the purpose of technical testing as helping organizations plan and conduct tests , analyze findings , and develop mitigation strategies - which aligns directly with "vulnerability evaluations" and "providing mitigation techniques." The DoD also points its Components to NIST SP 800-115 as guidance for penetration testing activities.
By contrast, a Red Team is typically framed as an "ethical adversary" that emulates attackers to test detection
/response and overall readiness; it is often broader, scenario-driven, and focused on demonstrating what a capable adversary can accomplish rather than performing a scoped vulnerability evaluation with remediation- oriented outputs. A Blue Team is primarily defensive operations (monitoring, detection, response), not the group defined by conducting vulnerability evaluations for customers. " White hat hackers " is a general label for ethical hackers, but it is less specific than the established service construct of a penetration test team .
Because the question emphasizes operational network vulnerability evaluations plus mitigation techniques
, the most precise and standard term is D: Penetration test team , supported by NIST's testing-and-mitigation framing.