CyberAB.CMMC-CCP.v2026-11-10.q95

Exam Code:	CMMC-CCP
Exam Name:	Certified CMMC Professional (CCP) Exam
Certification Provider:	Cyber AB
Free Question Number:	95
Version:	v2026-11-10
# of views:	106
# of Questions views:	1000
https://www.freecram.net/torrent/CyberAB.CMMC-CCP.v2026-11-10.q95.html	

NEW QUESTION: 1
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 FIPS-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: (SHOW ANSWER)
Understanding SC.L2-3.13.14 - Control and Monitor the Use of VoIP Technologies 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.
Why Option D is Correct
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.

Official CMMC Documentation References
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
Final Verification
IfVoIP is not used within the OSC's system boundary, the control does not require assessment, making Option D the correct answer.

NEW QUESTION: 2
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: (SHOW ANSWER)
Understanding the Best Source for CMMC Practice Descriptions
TheCMMC 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.

NEW QUESTION: 3
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: (SHOW ANSWER)
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.
Analysis of the Given Options:
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.
Official References Supporting the Correct 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.
Conclusion:
TheAU domain applies only to CMMC 2.0 Level 2, making the correct answer:
#B. Level 2.

NEW QUESTION: 4
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: (SHOW ANSWER)
Understanding Evidence Sufficiency in CMMC Level 2 Assessments
During 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.
Why Option B (Sufficiency) is Correct
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.
Official CMMC Documentation References
CMMC Assessment Process (CAP) Guide - Section 3.6 (Determining Sufficiency of Evidence)
CMMC Level 2 Assessment Guide - Evidence Collection and Evaluation Final Verification Since theLead Assessor is ensuring enough evidence is available to verify compliance, the correct answer isOption B: Sufficiency.

NEW QUESTION: 5
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: (SHOW ANSWER)

According to the CMMC Assessment Process (CAP), specifically within the Phase 4: Reporting Results requirements, a C3PAO must ensure that every assessment package undergoes a rigorous quality review before it is finalized and submitted to the Department of Defense (DoD).
The Role of the CQAP: The CMMC Quality Assurance Professional (CQAP) is a designated role within a C3PAO responsible for verifying that the assessment was conducted in accordance with the CAP and that the evidence collected (the "Artifacts") supports the findings (Met/Not Met).
Mandatory Inclusion: When generating the Final Recommended Assessment Results, the package is not considered complete or valid without the formal review documentation from the CQAP. This documentation serves as the "stamp of approval" that the internal Quality Management System (QMS) of the C3PAO has validated the assessment team's work.
Why other options are incorrect:
Option A: While the Assessment Plan is a required document during the planning phase, it is an input to the process, not a mandatory component of theFinal Resultsgeneration in the same way quality validation is.
Option B: Daily Checkpoints are administrative tools used during the "Conduct Assessment" phase to keep the OSC informed. While they are part of the assessment record, they are not a mandatory technical component of the final results package.
Option C: The contract is a legal/business requirement handled during the "Plan and Prepare" phase; it is not included in the technical assessment results uploaded to the DoD.
Reference Documents:
CMMC Assessment Process (CAP) v1.0: Section 4.2 (Finalize Assessment Report) and Section 4.3 (C3PAO Quality Review).
C3PAO Authorization Requirements: Specifies the requirement for a Quality Assurance (QA) function to review all assessment outputs to ensure consistency and integrity across the ecosystem.

NEW QUESTION: 6
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: (SHOW ANSWER)
Understanding IA.L2-3.5.3: Multifactor Authentication (MFA) Requirement TheIA.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 " Rating
For 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.
Why is the Correct Answer " D " (Practice is NOT MET since the objective was not implemented)?
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.
CMMC 2.0 References Supporting This answer:
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.

NEW QUESTION: 7
Which DFARS clause considers Safeguarding CDI and Cyber Incident Reporting?
A. 252.204-7022
B. 252.204-7020
C. 252.204-7012
D. 252.204-7021
Answer: C (LEAVE A REPLY)
The correct answer is C because DFARS 252.204-7012 is explicitly titled "Safeguarding Covered Defense Information and Cyber Incident Reporting." This clause is one of the core governance and source-document foundations for CMMC because it establishes contractor obligations for protecting covered defense information, including CUI/CDI, on covered contractor information systems. It defines covered contractor information systems as unclassified systems owned or operated by or for a contractor that process, store, or transmit covered defense information. It

also requires contractors to provide adequate security and implement NIST SP 800-171 security requirements where applicable. In addition, it requires contractors to rapidly report cyber incidents affecting covered contractor systems or covered defense information, with "rapidly report" defined as within 72 hours of discovery. Options A, B, and D are not the clause titled for safeguarding CDI and cyber incident reporting. DFARS
252.204-7020 relates to NIST SP 800-171 DoD assessment requirements, while DFARS 252.204-7021 addresses CMMC requirements. Reference/topics: DFARS 252.204-7012, CDI/CUI safeguarding, cyber incident reporting, CMMC source documents.

NEW QUESTION: 8
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: (SHOW ANSWER)
Understanding the Media Protection (MP) Domain
TheMedia 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.
Why the Correct Answer is "A. Media Protection (MP)"?
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.
Why Not the Other Options?
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.
Relevant CMMC 2.0 References:

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.
Final Justification:
SinceMedia Protection (MP) directly addresses the handling of assets containing CUI, the correct answer isA.
Media Protection (MP).

NEW QUESTION: 9
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: (SHOW ANSWER)
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).
#Why the Other Options Are Incorrect
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.

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.

NEW QUESTION: 10

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?

Freecram.net

A. Final Report
B. Certification rating
C. Summary-level findings
D. All Daily Checkpoint logs
Answer: (SHOW ANSWER)
Understanding the Assessment Results Package Submission
After completing aCMMC Level 2 Assessment, theCertified Third-Party Assessment Organization (C3PAO) mustsubmit the final assessment results packageto theEnterprise Mission Assurance Support Service (eMASS) system.
Key Required Document: Final Report
TheFinal Reportis themandatory documentthatcontains all assessment details, findings, and scoring.
It serves as theofficial record of the assessmentanddetermines certification eligibility.
Why is the Correct Answer "Final Report" (A)?
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.
CMMC 2.0 References Supporting This Answer:
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.
Final Answer:
#A. Final Report

NEW QUESTION: 11
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: (SHOW ANSWER)
Understanding the " Examine " Assessment Method in CMMC 2.0
CMMC 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.
Relevant CMMC 2.0 Reference:
TheCMMC Assessment Process (CAP)definesExamineas the method used toreview or analyze assessment objects, such as policies, procedures, configurations, and logs.
Why is the Correct Answer " Examine " (C)?
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.
CMMC 2.0 References Supporting this Answer:
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.

NEW QUESTION: 12

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: (SHOW ANSWER)

Understanding DFARS Clause 252.204-7012

TheDefense 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.

Why "All DoD Solicitations and Contracts" is Correct?

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.

Official References from DoD and DFARS Documentation

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.

Final Verification and Conclusion

NEW QUESTION: 13

During a POA & M closeout assessment , the Lead Assessor and team members verified all evidence provided by the OSC and passed those that satisfied the requirements. Who MUST verify that every failed practice from the initial original assessment has been adequately addressed?

A. OSC

B. CCA

C. OSC sponsor

D. Lead Assessor

Answer: (SHOW ANSWER)

In CMMC v2.0, the closeout activity for remediating previously unmet requirements is handled through the POA & M closeout process described in the CMMC Assessment Process (CAP) v2.0 . CAP v2.0 makes clear that the C3PAO must follow DoD's POA & M closeout procedures and that the Assessment Team performs the closeout work, with the assessment results then undergoing a required quality assurance (QA) review .

Operationally, the person who must ensure that each previously failed requirement is adequately addressed during the closeout assessment is the Lead Assessor (Lead CCA) , because the Lead CCA is the individual designated to oversee and manage the Assessment Team on behalf of the C3PAO for the conduct of the certification assessment. In other words, while team members may test controls and collect evidence, the Lead CCA is accountable for directing the assessment effort and ensuring that remediation evidence supports updated determinations.

CAP v2.0 also states that a QA individual performs a quality assurance review of the POA & M closeout

"upon completion by the Assessment Team," including checks on the accuracy and completeness of evaluation of POA & M security requirements before upload to eMASS. This reinforces that verification occurs through the assessment team's work, led by the Lead Assessor , and then independently quality- checked by QA.

NEW QUESTION: 14

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: (SHOW ANSWER)

Understanding the Reporting Process in a CMMC 2.0 Level 2 Assessment

ACMMC 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.

Assessment Communication Structure

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.
Why Option C is Correct
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.
Official CMMC Documentation References
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
Final Verification Based 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.

NEW QUESTION: 15
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: (SHOW ANSWER)
According to the CMMC Assessment Process (CAP), specifically in the context of scoping and organizational structure, the term Host Unit is used to define the specific entity within an Organization Seeking Certification (OSC) that is the primary subject of the assessment.
Definition of Host Unit: Within the CAP, the Host Unit represents the specific people, processes, and technology that process, store, or transmit Controlled Unclassified Information (CUI) or Federal Contract Information (FCI) for the contract in scope. It is the " anchor " for the assessment boundary.

Context in High-Level Scoping: During the initial phases of an assessment, a C3PAO must distinguish between the entire corporation (the OSC) and the specific parts of that corporation that are actually performing the DoD work. The Host Unit is that functional or logical division that will be evaluated against the CMMC practices.
Relationship to other units:
Supporting Organization/Units (Option D): These are entities that provide services to the Host Unit (such as an enterprise IT department or a separate HR branch) but are not the primary " Host " of the CUI/FCI. They are in-scope because they provide " Security Protection " or " Administrative " functions to the Host Unit.
Coordinating Unit (Option C): This term is often used in broader organizational contexts but is not a defined scoping term for the " people, processes, and technology " being assessed under the CMMC CAP.
Reference Documents:
CMMC Assessment Process (CAP) v1.0: Glossary and Section 1 (Plan and Prepare Assessment), which defines the relationship between the OSC, the Host Unit, and Supporting Units.
CMMC Level 2 Scoping Guidance: Provides the framework for identifying the " assets " (people, technology, facilities) that reside within the Host Unit boundary.
CCP Study Guide: Section on " Scoping the Assessment, " which explains how to identify the Host Unit versus External Service Providers (ESPs).

NEW QUESTION: 16
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: (SHOW ANSWER)
Understanding the "Verify Evidence and Record Gaps" Activity in a CMMC Assessment During 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.

Valid CMMC-CCP Dumps shared by ExamDiscuss.com for Helping Passing CMMC-CCP Exam! ExamDiscuss.com now offer the **newest CMMC-CCP exam dumps**, the ExamDiscuss.com CMMC-CCP exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CMMC-CCP dumps with Test Engine here: https://www.examdiscuss.com/Cyber-AB/exam/CMMC-CCP/premium/ (**240** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 17
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: (SHOW ANSWER)
Understanding the Assessment Environment Requirement
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.
Why Option B (Production) is Correct
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.
Official CMMC Documentation References
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.) Final Verification SinceCMMC assessments require security controls to be validated in the actual production environment, the correct answer isOption B: Production.

NEW QUESTION: 18
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: (SHOW ANSWER)
Understanding the CMMC Level 2 Final Report Requirements
For 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
Why "B. Documented rationale for each failed practice" is Correct?
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.
Why Other Answers Are Incorrect?
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." Conclusion 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

NEW QUESTION: 19
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: (SHOW ANSWER)
1. Understanding CMMC 2.0 Levels and CUI Handling Requirements
UnderCMMC 2.0, contractors handlingControlled Unclassified Information (CUI)must meet aminimumcertification level to be eligible for contract awards involving CUI.
CMMC 2.0 Levels:
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.
2. Official CMMC 2.0 References Confirming Level 2 for CUI
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.
3. Why the Other Options Are Incorrect
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.

NEW QUESTION: 20
What service is the MOST comprehensive that the RPO provides?
A. Training services
B. Education services
C. Consulting services
D. Assessment services
Answer: C (LEAVE A REPLY)
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).
Why "Consulting Services" is the Correct Answer?
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.
Breakdown of Answer Choices
Option
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.
Official References from CMMC 2.0 Documentation
TheCMMC-AB RPO Programdefines an RPO as aconsulting organization that assists companies in preparing for CMMC certificationbutdoes not perform assessments.
Final Verification and Conclusion
The correct answer isC. Consulting services, asRPOs primarily provide advisory and readiness supportto organizations preparing forCMMC compliance.

NEW QUESTION: 21
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: (SHOW ANSWER)
Understanding Licensed Training Providers (LTPs) in CMMC
ALicensed Training Provider (LTP)is an entity that is authorized by theCybersecurity Maturity Model Certification Accreditation Body (CMMC-AB)todeliver CMMC trainingbased on anapproved curriculum.
Key Responsibilities of an LTP:
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).
Why is the Correct Answer " Instructs a curriculum approved by CMMC-AB " (B)?
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.
CMMC 2.0 References Supporting This answer:
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.
Final answer:
#B. Instructs a curriculum approved by CMMC-AB

NEW QUESTION: 22
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: (SHOW ANSWER)
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.

NEW QUESTION: 23
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: (SHOW ANSWER)
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.
Role of a Registered Practitioner (RP)
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.
Why "B. RP of an Organization Not Part of the Assessment" is Correct?
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.
Why Other Answers Are Incorrect?
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.
Conclusion
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

NEW QUESTION: 24
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: (SHOW ANSWER)
Understanding the Principle of Least Functionality in the CM Domain
TheConfiguration 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.
Justification for the Correct Answer: Least Functionality (C)
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.
Why Other Options Are Incorrect
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.
Official CMMC and NIST References
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.
Conclusion
Theprinciple 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.

NEW QUESTION: 25
Which statement is NOT a requirement for a Licensed Partner Publisher?
A. Must have at least two years of history in publishing
B. Must possess a Dun and Bradstreet number and background check
C. Must receive CMMC Level 3 certification
D. Must be approved by CMMC-AB or authorized organization
Answer: (SHOW ANSWER)
The correct answer is C because a Licensed Partner Publisher is an ecosystem participant that produces or distributes approved CMMC-related learning or publishing content; it is not the same thing as an Organization Seeking Assessment or a Defense Industrial Base contractor pursuing a CMMC Level 3 certification status. CMMC certification levels apply to organizations handling FCI or CUI in connection with DoD contract performance, not to every training, publishing, or ecosystem- support organization. The CMMC Assessment Process describes CMMC as the DoD initiative for assessing and certifying conformance by companies and organizations in the Defense Industrial Base, specifically to safeguard CUI and FCI processed, stored, or transmitted during DoD contract performance. A publisher may need business validation, authorization, background checks, and approval by the CMMC Accreditation Body or authorized program entity, but requiring CMMC Level
3 certification would be misaligned with the role. Level 3 is an advanced contractor cybersecurity status, not a publishing-partner qualification. Reference/topics: CMMC Ecosystem, Licensed Partner Publisher, Cyber AB ecosystem roles, CMMC certification applicability.

NEW QUESTION: 26
Who is the FedRAMP certification program for?
A. IT contractors risk management self-assessments
B. Cloud service providers for cloud products and services
C. IT contractors for cybersecurity self-assessments
D. Cloud service providers for on-premise products and services
Answer: B (LEAVE A REPLY)
The correct answer is B because FedRAMP is a federal authorization program for cloud services, not a self-assessment framework for ordinary IT contractors and not a program for on-premise products. In the CMMC context, FedRAMP becomes especially important when a contractor uses an external cloud service provider to store, process, or transmit covered defense information or CUI. DFARS 252.204-
7012 requires the contractor to ensure that the cloud service provider meets security requirements equivalent to the FedRAMP Moderate baseline when covered defense information is handled in an external cloud service. FedRAMP itself also maintains a marketplace of certified cloud services, authorizing agencies, and recognized assessors. Therefore, the target participants are cloud service providers offering cloud products and services that need federal authorization or recognition. Options A and C incorrectly frame FedRAMP as a contractor self-assessment model. Option D is wrong because FedRAMP is focused on cloud service offerings, not traditional on-premise products or services. Reference/topics: FedRAMP, cloud service providers, DFARS 252.204-7012, external cloud services, FedRAMP Moderate baseline.

NEW QUESTION: 27
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 IoT device
C. Yes. because it is a restricted IS
D. Yes, because it is government property
Answer: (SHOW ANSWER)
Step 1: Understanding CMMC Level 1 Self-Assessment Scope
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.
Step 2: Why the Thermostat is in Scope
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 Incorrect
A). 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

NEW QUESTION: 28
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: (SHOW ANSWER)
CMMC Level 2 Readiness and Certification Requirements
CMMCLevel 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).
Clarification of Incorrect Options:
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.

NEW QUESTION: 29
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: (SHOW ANSWER)
According to the CMMC Model and Assessment Guides, specifically the rules governing Plan of Action and Milestones (POA & M) and the remediation period, an Organization Seeking

Certification (OSC) is allowed a limited opportunity to remediate certain "Not Met" practices to achieve a "Met" status without failing the assessment entirely.
Here is the breakdown based on CMMC Ecosystem protocols:
The 180-Day POA & M Rule: CMMC Level 2 allows for the use of POA & Ms for specific practices, provided they are not high-priority items (typically 5-point values in the scoring methodology). If an OSC has
"Not Met" practices that are eligible for a POA & M, they have up to 180 days to remediate them.
The Remediation Period (Assessment Closeout): During the assessment process itself, there is a "remediation period" (often referred to within the 1-90 day window depending on the specific C3PAO methodology and the CMMC assessment process) where an OSC can fix minor issues identified by the assessor before the final report is submitted.
Eligibility Criteria: The question states there are 15 practices "Not Met." While this is a high number, the CMMC rule does not automatically disqualify an OSC based solely on thequantityof practices, but rather thetype(weight) of the practices and the resulting score. To be eligible for a conditional "Met" (via POA & M), the OSC must achieve a minimum score (often 80% of the total points) and none of the "Not Met" practices can be those designated as mandatory "Met" (no POA & M allowed) in the CMMC rule.
Why "C" is correct: Because we do not know the specific weights of the 15 "Not Met" practices or the total score, we cannot definitively say theywillbe remediated (A) or that they areineligible(B). However, under the CMMC assessment framework, the OSC may be eligible to enter a remediation phase or utilize a POA & M to bridge the gap, provided they meet the scoring threshold and the specific practices allow for it.
Reference Documents:
CMMC Assessment Process (CAP): Defines the phases of assessment including the "Remediation Period."
32 CFR Part 170 (CMMC Program Rule): Outlines the specific requirements for POA & Ms, the 180-day timeline, and the scoring parameters required to be eligible for a Conditional Certification.

NEW QUESTION: 30
What are CUI protection responsibilities?
A. Shielding
B. Governing
C. Correcting
D. Safeguarding
Answer: (SHOW ANSWER)
Understanding CUI Protection Responsibilities
Controlled 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.

Why "D. Safeguarding" is Correct?
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.
Why Other Answers Are Incorrect?
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.
Conclusion
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)

NEW QUESTION: 31
The director of cybersecurity is considering which company offices and data centers store FCI to ensure an accurate scope for their CMMC Level 1 Self-Assessment . Which asset type is the director considering?
A. ESP
B. People
C. Facilities
D. Technology
Answer: (SHOW ANSWER)
For CMMC Level 1 scoping , the DoD's CMMC Scoping Guide - Level 1 (v2.13) instructs an organization performing a Level 1 self-assessment to consider what is in scope for protecting Federal Contract Information (FCI) . Specifically, it states that to appropriately scope a Level 1 self-assessment, the OSA should consider the people, technology, facilities, and external service providers (ESPs) within its environment that process, store, or transmit FCI .
In this scenario, the director is evaluating company offices and data centers where FCI is stored. These are physical locations and physical environments-exactly what the scoping guidance categorizes under Facilities
. Facilities in a Level 1 context include physical sites and spaces that may house systems or media containing FCI (e.g., offices, server rooms, data centers), because those locations affect physical access controls, environmental protections, and overall safeguarding of where FCI is handled and stored.

This is distinct from Technology (devices/systems), People (personnel who handle FCI), and ESPs (external providers delivering IT/cyber services). Since the question is explicitly about which offices and data centers store FCI -a physical boundary and location question-the correct asset type is Facilities .

Valid CMMC-CCP Dumps shared by ExamDiscuss.com for Helping Passing CMMC-CCP Exam! ExamDiscuss.com now offer the **newest CMMC-CCP exam dumps**, the ExamDiscuss.com CMMC-CCP exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CMMC-CCP dumps with Test Engine here: https://www.examdiscuss.com/Cyber-AB/exam/CMMC-CCP/premium/ (**240** Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 32
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: (SHOW ANSWER)
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.

NEW QUESTION: 33

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: (SHOW ANSWER)

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.

NEW QUESTION: 34

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: (SHOW ANSWER)

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).

NEW QUESTION: 35
Which resource contains authoritative data classifications of CUI?
A. NARA
B. CMMC-AB
C. DoD Contractors FAQ
D. OSC's privacy policies
Answer: (SHOW ANSWER)
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.

NEW QUESTION: 36
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: (SHOW ANSWER)

Last Step in Developing an Assessment Plan for an OSC

Developing 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.

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

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.

CMMC 2.0 References Supporting This answer:

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.

Final answer:

#D. Obtain and record commitment to the assessment plan.

NEW QUESTION: 37

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: (SHOW ANSWER)
Understanding CMMC Asset Categorization
TheCMMC 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 Assets
As 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.
Why the Other Answers Are Incorrect
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.
CMMC Official References
CMMC 2.0 Scoping Guide - Level 1 & Level 2
CMMC Assessment Process (CAP) Document
Thus,option C (Out-of-Scope Assets) is the correct answerbased on official CMMC scoping guidance.

NEW QUESTION: 38
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: (SHOW ANSWER)
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

NEW QUESTION: 39
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: (SHOW ANSWER)
Understanding CMMC 2.0 Incident Response Practices
TheIncident Response (IR) domaininCMMC 2.0 Level 2aligns withNIST SP 800-171, Section 3.6, which defines requirements forestablishing and maintaining an incident response capability.
Why "A. IR.L2-3.6.1: Incident Handling" is Correct?
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
Why Other Answers Are Incorrect?
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.
Conclusion
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

NEW QUESTION: 40
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: (SHOW ANSWER)
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.

NEW QUESTION: 41
Which activities are involved in ALL assessment methods?
A. Exercising one or more assessment objects under specified conditions to compare actual with expected behavior
B. Conducting discussions with individuals or groups of individuals in an organization to facilitate understanding, achieve clarification, or lead to the location of evidence
C. Checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects or artifacts to facilitate understanding, achieve clarification, or obtain additional evidence
D. Determining security safeguard existence, functionality, correctness, completeness, and potential for improvement over time
Answer: (SHOW ANSWER)
The correct answer is D because the question asks what is involved in all assessment methods, not what defines a single assessment method. Options A, B, and C describe the three individual assessment methods. Option A describes Test, where assessment objects are exercised under specified conditions and actual behavior is compared with expected behavior. Option B describes Interview, where discussions are held with personnel to clarify implementation and locate evidence. Option C describes Examine, where artifacts, specifications, mechanisms, or records are reviewed, inspected, studied, or analyzed. The common purpose across all three is to support a determination about whether the safeguard exists, functions correctly, is complete, and is capable of supporting the required security outcome. NIST SP 800-171A explains that assessment methods are used to facilitate understanding, achieve clarification, or obtain evidence, and that the assessment process gathers information and produces evidence to determine security requirement effectiveness. Therefore, D captures the cross- method assessment purpose, while A, B, and C each capture only one method. Reference/topics: assessment methods, Examine/Interview/Test, assessment objectives, evidence-based determination.

NEW QUESTION: 42
What technical means can an OSC have in place to limit individuals who are authorized to post or process information on publicly accessible systems?
A. Enable cookies to track who has accessed certain websites.
B. Ensure procedural documentation is in place on how to access website consoles.
C. Ensure marketing team trainings are required so that any changes to the website go through proper review.
D. Enable administrative access roles to those that need them so that only those people can post items to the website.
Answer: (SHOW ANSWER)
This question aligns to the CMMC requirement to control information posted or processed on publicly accessible information systems , which appears in the CMMC Model Overview as AC.L1-3.1.22 (Control Public Information) and maps to FAR 52.204-21(b)(1)(iv) and NIST SP 800-171 Rev. 2 / r2 requirement

3.1.22 .
NIST explains that publicly accessible systems are typically those accessible to the public without identification or authentication , and that individuals authorized to post nonpublic information (including CUI/FCI and proprietary information) are designated . It also emphasizes controlling what gets posted and ensuring nonpublic information is not exposed.
The most direct technical way to "limit individuals who are authorized to post or process information" is to implement role-based administrative access (least privilege) to the website/CMS/admin console-granting publish/edit privileges only to approved roles (e.g., "Web Publisher," "Content Approver"), and keeping all other users read-only or without access to posting functions. This directly enforces the requirement by using access control to restrict who can post/process content on the public system.
Options B and C are helpful procedural/administrative controls , but the question asks for technical means
. Option A (cookies) does not control authorization to post; it's not an access control mechanism.
Therefore, D is best.

NEW QUESTION: 43
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: (SHOW ANSWER)
According to the CMMC Scoping Guidance, Level 2, assets are categorized into specific groups to determine how they are treated during an assessment. One of these categories is Specialized Assets.
The CMMC Scoping Guidance defines Specialized Assets as a specific group that includes:
Government Property: Any property owned or leased by the government and provided to the contractor (Government Furnished Equipment or GFE).
Internet of Things (IoT): Physical objects that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data.
Operational Technology (OT): Programmable systems or devices that interact with the physical environment (e.g., Industrial Control Systems).
Restricted Information Systems: Systems that have specific configurations or constraints that prevent standard security controls from being applied (e.g., legacy systems).
Test Equipment: Specialized equipment used for testing, such as oscilloscopes or signal generators.
Why other options are incorrect:
Option A (SOCs): A Security Operations Center is typically considered a Security Protection Asset (SPA) because it provides security functions (monitoring/response) for the assessment scope.

Option B (Hosted VPN services): These are generally categorized as External Service Providers (ESPs) or part of the Security Protection Assets, depending on how they are managed and their role in protecting CUI.
Option C (Consultants): These are External Service Providers (ESP) (personnel/organizations), not specialized hardware/software assets.
Treatment of Specialized Assets: Under CMMC Level 2 scoping rules, Specialized Assets must be identified in the Asset Inventory and documented in the System Security Plan (SSP), but they are generally not managed against the CMMC practices unless they process, store, or transmit CUI in a way that falls outside their specialized function.
Reference Documents:
CMMC Scoping Guidance, Level 2 (Version 2.0/2.1): Section 3.1, "Specialized Assets" and Table 3.
32 CFR Part 170 (CMMC Program Rule): Definitions of asset categories and their associated assessment requirements.

NEW QUESTION: 44
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: (SHOW ANSWER)
Step 1: Understanding AC.L1-3.1.22
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 Release
If 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 Incorrect
A). 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

NEW QUESTION: 45
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: (SHOW ANSWER)
Background on Legacy Markings and CUI
Legacy markings refer to classification labels used before the implementation of the Controlled Unclassified Information (CUI) Program under DoD 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 with CUI 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 about CUI, not classified information. Secret-level documents follow different marking rules under DoD Manual 5200.01.
If a document is being shared externally (Answer C - Correct):
According to DoD Instruction 5200.48, Section 3.6(a), organizations must review legacy markings before sharing documents outside the organization.
The document must be re-marked in 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 is C: Documents with legacy markings must be re-marked or redacted when being shared outside the organization to comply with DoD CUI guidelines.
References:

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

NEW QUESTION: 46
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. IoT
B. Restricted IS
C. Test equipment
D. Operational technology
Answer: (SHOW ANSWER)
Understanding Specialized Assets in a CMMC Self-Assessment
DuringCMMC Level 1 Self-Assessments, organizations must classify theirassetsin theSystem Security Plan (SSP).
Specialized Asset Type: Operational Technology (OT)
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).
Why is the Correct Answer "D. Operational Technology"?
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).
CMMC 2.0 References Supporting This Answer:
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.

Valid CMMC-CCP Dumps shared by ExamDiscuss.com for Helping Passing CMMC-CCP Exam! ExamDiscuss.com now offer the **newest CMMC-CCP exam dumps**, the ExamDiscuss.com CMMC-CCP exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CMMC-CCP dumps with Test Engine here: https://www.examdiscuss.com/Cyber-AB/exam/CMMC-CCP/premium/ (**240** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 47
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: (SHOW ANSWER)
Understanding Scoping in CMMC 2.0
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.
Why the Correct Answer is " D. Nonfederal systems that process, store, or transmit CUI, or that provide protection for the system components " ?
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.
Why Not the Other Options?
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.
Relevant CMMC 2.0 References:
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.
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.

NEW QUESTION: 48
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: (SHOW ANSWER)
Interview Selection in CMMC Assessments
During 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.
Why "Providing Clarity and Understanding" Is Key
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.

Thus,option D is the correct choicebecause the Lead Assessor should prioritizeinterviewing personnel who can clearly explain how CMMC practices are implemented.
Why the Other Answers Are Incorrect
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.
CMMC Official References
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.
Thus,option D (Provide clarity and understanding of their practice activities) is the correct answeras per official CMMC assessment guidelines.

NEW QUESTION: 49
Which CMMC Levels meet the standards of protecting FCI (Federal Contract Information) ?
A. Level 1
B. Level 2
C. Levels 2 and 3
D. Levels 1, 2, and 3
Answer: D (LEAVE A REPLY)
In CMMC v2.0, Level 1 is explicitly the level that "focuses on the protection of FCI " and is composed of the basic safeguarding requirements aligned to FAR 52.204-21 . This directly establishes Level 1 as meeting the standard for protecting FCI.
However, the question asks which levels meet the standard of protecting FCI-not which level is primarily intended for FCI. The official CMMC Model Overview (Version 2.0) states that the CMMC levels and associated sets of practices are cumulative , meaning that to achieve a higher level, an organization must also demonstrate achievement of the preceding lower levels. Because Level 2 and Level 3 certifications require meeting lower-level requirements as part of achieving the higher certification, an organization certified at Level 2 or Level 3 necessarily satisfies the Level 1 requirements that protect FCI.
In addition, the later Model Overview v2.13 reiterates the structure of the model: Level 1 requirements correspond to FAR 52.204-21 safeguards (FCI), while Level 2 and Level 3 focus on CUI protection at increasing rigor. Taken together, the official documents support that Levels 1, 2,

and 3 all meet the standard for protecting FCI, with Level 1 being the foundational baseline and Levels 2/3 building on it.

NEW QUESTION: 50

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: (SHOW ANSWER)

Understanding " Adequate Evidence " in the CMMC Assessment Process

In 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.

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

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.

CMMC 2.0 References Supporting this answer:

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

NEW QUESTION: 51
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: (SHOW ANSWER)
How Many Practices Are Included in CMMC Level 2?
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.
Breakdown of Practices in CMMC 2.0
CMMC 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.
Why the Other Answers Are Incorrect
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.
CMMC Official References
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).
Thus,option C (110 practices) is the correct answer, as per official CMMC guidance.

NEW QUESTION: 52
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: (SHOW ANSWER)
Understanding Configuration Management (CM) in CMMC Level 2
InCMMC 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 Choices
Option
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
Official Reference from CMMC 2.0 Documentation
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.
Final Verification and Conclusion
The correct answer isA. Controlled and monitored, as perCM.3.068inNIST SP 800-171andCMMC 2.0 documentation.

NEW QUESTION: 53
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: (SHOW ANSWER)
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.

NEW QUESTION: 54
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: (SHOW ANSWER)
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.

NEW QUESTION: 55
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: (SHOW ANSWER)
Understanding Ethical Responsibility in the CMMC Ecosystem
Ethics 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.
Key Ethical Responsibilities Include:
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.
Why is the Correct Answer " CMMC-AB and Members of the CMMC Ecosystem " (C)?
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.
CMMC 2.0 References Supporting this answer:
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.

NEW QUESTION: 56
Which document is used to protect sensitive and confidential information from being made available by the recipient of that information?
A. Legal agreement
B. CMMC agreement

C. Assessment agreement
D. Non-disclosure agreement
Answer: (SHOW ANSWER)
The correct document is a Non-Disclosure Agreement (NDA) , because its specific purpose is to restrict a receiving party from disclosing sensitive or confidential information to unauthorized parties. In the official CMMC Assessment Process (CAP) v2.0 , NDAs are called out directly as a required element of the contracting relationship for a Level 2 certification assessment.
CAP v2.0 states that the C3PAO and the OSC must execute a written contractual agreement for the assessment and then specifies that "A mutual non-disclosure agreement (NDA) between the parties shall be incorporated into the contractual agreement or negotiated and executed in a separate document (e.
g., stand-alone NDA, master services agreement, etc.)."
This is important because CMMC assessments can involve access to highly sensitive organizational information, including details about system architectures, security implementations, and potentially CUI handling processes. The CAP's NDA requirement supports controlling dissemination of that information and reinforces the broader confidentiality expectations placed on assessment participants.
While an "assessment agreement" or generic "legal agreement" might contain confidentiality clauses, CAP v2.
0 explicitly identifies the NDA instrument (either embedded or standalone) as the mechanism to protect information exchanged during the assessment engagement. Therefore, the best answer-consistent with CMMC v2.0 official process documentation-is D (Non-disclosure agreement) .

NEW QUESTION: 57
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: (SHOW ANSWER)
Understanding SI.L2-3.14.6: Monitor Communications for Attacks
The 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.
Why "Review an artifact to check key references for the configuration of the IDS or IPS" is Correct?
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.
Breakdown of Answer Choices
Option
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.
Official References from CMMC 2.0 and NIST SP 800-171 Documentation
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.
Final Verification and Conclusion
The 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.

NEW QUESTION: 58
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: (SHOW ANSWER)

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.

NEW QUESTION: 59

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. Out of scope

B. Assessment Team Member

C. In scope

D. OSC point of contact

Answer: (SHOW ANSWER)

NEW QUESTION: 60

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?

Freecram.net

A. 90 days

B. 180 days

C. 270 days

D. 360 days

Answer: B (LEAVE A REPLY)

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.

Relevant CMMC 2.0 Reference:

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.
Why is the Correct Answer 180 Days (B)?
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.
CMMC 2.0 References Supporting this Answer:
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.

NEW QUESTION: 61
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: (SHOW ANSWER)
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.
Final Validation from CMMC Documentation:
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.

Valid CMMC-CCP Dumps shared by ExamDiscuss.com for Helping Passing CMMC-CCP Exam! ExamDiscuss.com now offer the **newest CMMC-CCP exam dumps**, the ExamDiscuss.com CMMC-CCP exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CMMC-CCP dumps with Test Engine here: https://www.examdiscuss.com/Cyber-AB/exam/CMMC-CCP/premium/ (**240** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 62
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: (SHOW ANSWER)

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).
Why "Implements, Performs, or Supports That Practice" is Correct?
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.
Breakdown of Answer Choices
Option
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.
Official References from CMMC 2.0 Documentation
CMMC Assessment Process Guide (CAP)- Requires that interviewees bedirectly responsiblefor implementing, performing, or supporting the practice.
Final Verification and Conclusion
The correct answer isD. Implements, performs, or supports that practice, as the interviewee mustactively contribute to the execution of the practice.

NEW QUESTION: 63
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: (SHOW ANSWER)

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.

NEW QUESTION: 64
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: (SHOW ANSWER)
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).

NEW QUESTION: 65
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: (SHOW ANSWER)
Understanding the Phases of the CMMC Assessment Process
TheCMMC 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.
Key Activities in Phase 1 - Pre-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.
Why is the Correct Answer "Phase 1" (A)?
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.
CMMC 2.0 References Supporting this Answer:
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.

NEW QUESTION: 66
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: (SHOW ANSWER)
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.
Why is the Correct Answer "At the Time of Award" (A)?
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.
CMMC 2.0 References Supporting This Answer:
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.

NEW QUESTION: 67
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: (SHOW ANSWER)
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

NEW QUESTION: 68
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: (SHOW ANSWER)
Federal Contract Information (FCI) is defined in FAR 52.204-21 as information provided by or generated for the government under contract but not intended for public release. Under CMMC 2.0, organizations handling FCI must implement FAR 52.204-21 Basic Safeguarding Requirements, ensuring proper protection in processing, storing, and transmitting FCI.
Analyzing the Given Options
The question involves an email system that is used to send FCI 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 is sending FCI via email, this falls under transmitting the 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 Answer
CMMC 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 of transmitting information.
Conclusion
Since the contractor is sending FCI via email, the correct answer is C. Transmit FCI. This aligns with CMMC
2.0 Level 1 practices under FAR 52.204-21 and NIST SP 800-171, which emphasize securing transmitted data.

NEW QUESTION: 69
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 (LEAVE A REPLY)
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.

NEW QUESTION: 70

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?

Freecram.net

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: (SHOW ANSWER)
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.

NEW QUESTION: 71
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: (SHOW ANSWER)

Understanding SI.L1-3.14.2: Provide Protection from Malicious Code

The 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.

Why Are the Other Answers Incorrect?

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.

CMMC 2.0 References Supporting This Answer:

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.

Final Answer:

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

NEW QUESTION: 72

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: (SHOW ANSWER)

Understanding the Definition of an Agreement in the CMMC-AB Code of Professional Conduct

TheCMMC-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.

Why is the Correct Answer "D. Agreement"?

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.

CMMC 2.0 References Supporting This Answer:

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.

NEW QUESTION: 73

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: (SHOW ANSWER)

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.

Step-by-Step Breakdown:

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.

Official Reference:

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.

Thus, theCMMC Assessment Reporting Requirementsdocument is the authoritative source that dictates the reporting procedures for CMMC assessments.

NEW QUESTION: 74
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: (SHOW ANSWER)
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.
Step-by-Step Breakdown:
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.
Final Validation from CMMC Documentation:
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.
Thus, the correct answer is:
B). Consult the CMMC Assessment Guides and NIST SP 800-171.

NEW QUESTION: 75
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: (SHOW ANSWER)
Understanding the Role of CAICO in the CMMC Ecosystem
TheCMMC 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.
Why Option D (CAICO) is Correct
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.
Official CMMC Documentation References
CMMC Ecosystem Overview - Role of the CAICO
CMMC Assessment Process (CAP) Guide - Assessor Certification and Training Final Verification
SinceCAICO is responsible for training, testing, and certifying CMMC assessors and instructors, the correct answer isOption D: CMMC Assessors and Instructors Certification Organization.

NEW QUESTION: 76
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 (LEAVE A REPLY)
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.

Valid CMMC-CCP Dumps shared by ExamDiscuss.com for Helping Passing CMMC-CCP Exam! ExamDiscuss.com now offer the **newest CMMC-CCP exam dumps**, the ExamDiscuss.com CMMC-CCP exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CMMC-CCP dumps with Test Engine here: https://www.examdiscuss.com/Cyber-AB/exam/CMMC-CCP/premium/ (**240** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 77
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: (SHOW ANSWER)
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.

Final Validation from CMMC Documentation:
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.

NEW QUESTION: 78
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: (SHOW ANSWER)
Understanding the Role of an FCI Asset in CMMC
Adedicated 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.
Final Validation from CMMC Documentation:
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.

NEW QUESTION: 79
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: (SHOW ANSWER)
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

NEW QUESTION: 80
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?
Freecram.net
A. CCP
B. C3PAO
C. Lead Assessor
D. Advisory Board
Answer: (SHOW ANSWER)
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.
Roles and Responsibilities in CMMC Assessments:
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.
Official References Supporting the Correct Answer:
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.
Conclusion:
TheLead Assessoris the correct answer because they have the authority to verify scope determinations during the assessment.
#Correct Answer: C. Lead Assessor

NEW QUESTION: 81
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: (SHOW ANSWER)
According to the CMMC Scoping Guidance, Level 1, the scope of an assessment includes all assets that process, store, or transmit Federal Contract Information (FCI). CMMC is "information-centric," meaning the security requirements apply to the information itself, regardless of the media it resides on (digital or physical).
Asset Identification: In a Level 1 assessment, assets are categorized as either FCI Assets or Out-of-Scope Assets. Since the file cabinet is explicitly identified as containing paper FCI, it meets the definition of an asset that stores the protected information.
Basic Safeguarding (FAR 52.204-21): The 17 practices of CMMC Level 1 are derived from the FAR clause for the "Basic Safeguarding of Covered Contractor Information Systems." However, the physical protection requirements within that set (such as PE.L1-3.10.1, which requires limiting physical access to organizational information systems and equipment) extend to the physical storage locations of that data.

Media Neutrality: CMMC documentation emphasizes that "information systems" include the physical components and the information processed by them. If FCI is printed and stored in a cabinet, that cabinet becomes a physical storage asset within the assessment boundary.
Why other options are incorrect:
Option B: Physical location alone does not bring an asset into scope. For example, a coffee machine in the same room as an FCI computer remains out of scope because it doesn't handle FCI. Thecontent(FCI) makes the cabinet in-scope, not its proximity.
Option C: CMMC and the underlying FAR clause do not exempt paper-based information. Protected data must be secured whether it is on a hard drive or a printed sheet.
Option D: While a file cabinet may not "process" or "transmit" data like a computer does, it absolutely stores it. The definition of the scope includes all three functions (process, store, or transmit).
Reference Documents:
CMMC Scoping Guidance, Level 1: Section 2.0 (CMMC Level 1 Asset Categories), which defines FCI Assets as those that process, store, or transmit FCI.
CMMC Assessment Guide, Level 1: Discussion on Physical Protection (PE) practices and their application to physical media.
32 CFR Part 170 (CMMC Program Rule): Definitions of FCI and the requirements for contractor self- assessments.

NEW QUESTION: 82
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: (SHOW ANSWER)
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.
Step-by-Step Explanation:
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 Phases

The 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.
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.

NEW QUESTION: 83
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: (SHOW ANSWER)
Understanding CMMC 2.0 Levels and Their Descriptions
TheCybersecurity 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 Why "B. Advanced" is Correct?
TheCMMC 2.0 framework explicitly describes Level 2 as "Advanced."
Italigns with NIST SP 800-171to ensure robustCUI protection.
Why Other Answers Are Incorrect?
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.
Conclusion
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

NEW QUESTION: 84
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. IoT
B. Restricted IS
C. Test equipment
D. Government property
Answer: (SHOW ANSWER)
Understanding Restricted Information Systems (IS) in CMMC Scoping
InCMMC 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.
Why "B. Restricted IS" is Correct?

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.
Why Other Answers Are Incorrect?
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.
Conclusion
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

NEW QUESTION: 85
A program manager for a defense contractor saves all FCI data relevant to a contract on a flash drive. Why is the flash drive categorized as an FCI Asset ?
A. It is storing FCI.
B. It is testing FCI.
C. It is distributing FCI.
D. It is properly marked as FCI.
Answer: (SHOW ANSWER)
CMMC v2.0 scoping defines "in-scope" assets for Level 1 (FCI protection) based on whether the asset processes, stores, or transmits FCI . The DoD CMMC Assessment Scope - Level 1 (v2.13) states: "Assets in scope ... are all assets that **process, store, or transmit Federal Contract Information (FCI)." It then defines these terms. Critically for this question, Store is defined as when "FCI is inactive or at rest on an asset (e.g., located on electronic media...)." A flash drive is "electronic media." If the program manager places contract-relevant FCI onto the flash drive, the flash drive is now an asset that stores FCI (FCI at rest). Under the scoping guidance, that alone is enough to classify it as an in-scope FCI asset for Level 1 purposes, meaning it falls within the Level 1 assessment scope and must be protected by applicable Level 1 requirements.
The other answer choices do not align to the scoping definitions. "Testing FCI" (B) is not one of the scope- determining criteria in the Level 1 scoping guide. "Distributing FCI" (C) is not the

formal criterion either (the guide uses Transmit , not "distribute"). Finally, being "properly marked" (D) does not determine whether something is in scope; the decisive factor is whether the asset processes, stores, or transmits FCI.

NEW QUESTION: 86
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: (SHOW ANSWER)
Understanding C3PAO Requirements
ACertified 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.
Why is the Correct Answer " D " (A C3PAO must be authorized by CMMC-AB before being able to conduct assessments)?
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.
CMMC 2.0 References Supporting This Answer:
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.

NEW QUESTION: 87
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: (SHOW ANSWER)
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 .

NEW QUESTION: 88
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: (SHOW ANSWER)
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.

NEW QUESTION: 89
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: (SHOW ANSWER)
Understanding Who Must Perform Tests in a CMMC Assessment
During 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.
Who Performs Tests?
Operational personnel (OSC employees) must conduct the actual work while assessors observe.
Certified CMMC Professionals (CCPs) or Lead Assessorsoversee and document the testing process.
Why is the Correct Answer "A" (OSC personnel who normally perform that work as the CCP observes)?
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.
CMMC 2.0 References Supporting This Answer:
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.

NEW QUESTION: 90

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?

Freecram.net

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 (LEAVE A REPLY)

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.

NEW QUESTION: 91
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: (SHOW ANSWER)
Understanding CUI Markings and the Role of NARA
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.
Clarification of Incorrect Options:
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

Valid CMMC-CCP Dumps shared by ExamDiscuss.com for Helping Passing CMMC-CCP Exam! ExamDiscuss.com now offer the **newest CMMC-CCP exam dumps**, the ExamDiscuss.com CMMC-CCP exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CMMC-CCP dumps with Test Engine here: https://www.examdiscuss.com/Cyber-AB/exam/CMMC-CCP/premium/ (**240** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 92
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: (SHOW ANSWER)
Key References for a Lead Assessor in a CMMC Assessment
ALead Assessorconducting aCMMC assessmentmust rely onofficial CMMC guidance documentsto evaluate whether anOrganization Seeking Certification (OSC)meets the required cybersecurity practices.
Most Relevant Reference: CMMC Assessment Guide
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.
Why is the Correct Answer "D. Published CMMC Assessment Guide practice descriptions for the desired certification level"?
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.
CMMC 2.0 References Supporting This Answer:
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.
Final Answer:
#D. Published CMMC Assessment Guide practice descriptions for the desired certification level.

NEW QUESTION: 93
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. transmit CUI.
B. generate CUI
C. store CUI.
D. protect CUI.
Answer: (SHOW ANSWER)

NEW QUESTION: 94
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: (SHOW ANSWER)
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.

NEW QUESTION: 95
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: (SHOW ANSWER)

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

Valid CMMC-CCP Dumps shared by ExamDiscuss.com for Helping Passing CMMC-CCP Exam! ExamDiscuss.com now offer the **newest CMMC-CCP exam dumps**, the ExamDiscuss.com CMMC-CCP exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CMMC-CCP dumps with Test Engine

here: https://www.examdiscuss.com/Cyber-AB/exam/CMMC-CCP/premium/ (**240** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)