PassQueen
a.k.a dumpsqueen.com

Certified CMMC Professional (CCP) Exam

Cyber AB CMMC-CCP

Version Demo

Total Demo Questions: 25

Total Premium Questions: 256

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, CMMC Ecosystem	48
Topic 2, CMMC Model	49
Topic 3, CMMC Assessment Process	108
Topic 4, CMMC Scoping	51
Total	256

QUESTION NO: 1

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

A. It handles CUI

B. It is a restricted IS

C. It is government property

D. It is operational technology

ANSWER: B

Explanation:

It is a restricted IS is correct because CMMC scoping recognizes that an irreplaceable legacy information system may be unable to support modern security requirements while remaining necessary to perform contract work. A Windows 95 system that is the sole platform capable of operating required contract software is the type of legacy constraint contemplated by the restricted information system concept. The basis for excluding such a system from the normal assessment scope is not its age alone; it is the combination of an operational necessity, the inability to reasonably apply the required protections, and the use of documented alternative risk treatment. The OSC must identify the asset and establish appropriate isolation and compensating safeguards so that its residual risk is managed rather than ignored. This treatment preserves the assessment boundary while acknowledging that immediate replacement or modernization may not be feasible. CMMC scoping is asset- and information-flow-based, so the OSC should maintain an accurate inventory and supporting boundary documentation for the restricted system and the protections around it. See the DoD's CMMC Model resources and Cyber AB's CMMC Model overview for CMMC scoping and assessment information.

QUESTION NO: 2

A C3PAO has conducted a CMMC Level 2 Assessment for an OS

C.

The results have been reviewed by a CMMC Quality Assurance Professional. What is the final step in the process of submitting assessment results?

A. The C3PAO submits the results to the CMMC-A

B. The OSC submits the results, as provided by the Lead Assessor, to the CMMC-A

C. The C3PAO submits the results to Enterprise Mission Assurance Support Service.

D. The Lead Assessor submits the results to the CMMC-A

ANSWER: C

Explanation:

The C3PAO submits the results to Enterprise Mission Assurance Support Service. Following completion of the assessment and the required quality-assurance review, the authorized C3PAO submits the final CMMC assessment results into the CMMC instance of the Enterprise Mission Assurance Support Service (eMASS). This submission records the assessment outcome in the Department of Defense's designated system of record and enables the government's CMMC certification decision process. The assessment record includes the final result and associated assessment artifacts required by the CMMC assessment process. The C3PAO, rather than an individual assessor or the organization seeking certification, is responsible for making this formal system submission because it is the authorized assessment organization and is accountable for the integrity of the reported result. The Lead Assessor's assessment work and the CMMC Quality Assurance Professional's review are essential controls before submission, but the completed, quality-reviewed result is ultimately transmitted by the C3PAO to eMASS. This workflow is described in the DoD CMMC Assessment Process Guide and aligns with the Cyber AB's overview of the CMMC assessment process.

QUESTION NO: 3

What service is the MOST comprehensive that the RPO provides?

A. Training services

B. Education services

C. Consulting services

D. Assessment services

ANSWER: C

Explanation:

Consulting services is the most comprehensive service an RPO provides because a Registered Provider Organization supports organizations preparing for CMMC by delivering advisory and implementation-readiness assistance across a range of activities. This can include interpreting applicable CMMC requirements, identifying gaps in an organization's existing cybersecurity program, assisting with plans of action and milestones, developing or improving policies and procedures, and helping prepare objective evidence for a future assessment. Consulting is therefore an umbrella service that can incorporate targeted education or training while remaining focused on the organization's overall CMMC readiness.

Cyber AB describes RPOs as organizations authorized to provide CMMC consulting services to organizations seeking to improve their cybersecurity posture and prepare for CMMC assessments. Their role is distinct from performing a CMMC certification assessment, preserving the independence of the assessment process. A prospective organization may use an RPO for broad, tailored readiness support before engaging an authorized assessment organization. See Cyber AB's Registered Provider Organizations information and the Department of Defense's CMMC Program resource page.

QUESTION NO: 4

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

A. PE.L2-3.10.5: Control and manage physical access devices

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

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

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

ANSWER: A

Explanation:

PE.L2-3.10.5: Control and manage physical access devices is met because badge readers, PIN code pads, and keys are physical access devices used to permit, restrict, and manage entry to facilities, rooms, and other areas containing organizational systems or CUI. For a Level 2 assessment, the OSC must demonstrate that such devices are controlled and managed, not merely that they exist. Relevant evidence can include documented procedures for issuing, tracking, securing, recovering, changing, and disabling keys, badges, codes, and similar devices, along with records showing the procedures are implemented. The scenario states that the OSC has several types of access devices and documentation demonstrating that it meets the practice, which supports a finding that the practice is satisfied. This practice derives from NIST SP 800-171 requirement 3.10.5 and is included in the CMMC Level 2 practices. See the Department of Defense CMMC Model resources and NIST SP 800-171 Rev. 2 for the source requirement and associated assessment context.

QUESTION NO: 5

A contractor has implemented IA.L2-3.5.3: Multifactor Authentication practice for their privileged users, however, during the assessment it was discovered that the OSC's standard users do not require MFA to access their endpoints and network resources. What would be the BEST finding?

A. The process is running correctly.

B. It is out of scope as this is a new acquisition.

C. The new acquisition is considered Specialized Assets.

D. Practice is NOT MET since the objective was not implemented.

ANSWER: D

Explanation:

Practice is NOT MET since the objective was not implemented. is the best finding because IA.L2-3.5.3 requires the organization to use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. The stated condition establishes that standard users can access network resources without MFA. Because those users are non-privileged accounts and the access is network access, a required portion of the practice is absent.

In a CMMC assessment, an assessment objective must be satisfied for the practice to receive a MET determination. Applying MFA to privileged users demonstrates implementation for the privileged-account portion of the requirement, but it does not fulfill the separate non-privileged network-access portion. The assessor should document the condition and determine the practice is NOT MET based on the unmet assessment objective. The reference to endpoint access should be read carefully: the underlying requirement specifically calls for MFA for *local and network* access to privileged accounts, while MFA for non-privileged accounts is required for *network* access. The lack of MFA for standard-user network-resource access is sufficient to support this finding.

The authoritative requirement appears in NIST SP 800-171 Rev. 2, requirement 3.5.3 and is incorporated into the CMMC Level 2 requirements at 32 CFR Part 170.

QUESTION NO: 6

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

A. to conduct self-assessments.

B. opt out of CMMC Assessments.

C. have assessment costs reimbursed by the DoD.

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

ANSWER: A

Explanation:

to conduct self-assessments. is correct because CMMC Level 1 (Foundational) is designed for organizations that process, store, or transmit Federal Contract Information and requires implementation of the basic safeguarding requirements derived from FAR 52.204-21. Under the CMMC Program rule, the Level 1 assessment requirement is an annual self-assessment performed by the organization seeking certification rather than a required assessment conducted by an authorized third-party assessment organization. The organization records the results in the Supplier Performance Risk System and a senior official provides an annual affirmation that the assessment was completed and that the organization meets the applicable requirements. This approach supports the CMMC 2.0 objective of reducing the assessment burden and associated costs for the foundational level while retaining an annual accountability mechanism. The self-assessment is not merely an informal internal review: it is a defined CMMC assessment type with required scoring, reporting, and affirmation activities when included in the applicable solicitation or contract. The Department of Defense's CMMC information is available at DoD CIO: CMMC, and the formal Level 1 self-assessment and affirmation requirements appear in 32 CFR Part 170.

QUESTION NO: 7

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: D

Explanation:

“insufficient, and re-rate the audit finding after a quarter two assessment report is examined.” is correct because the available evidence does not yet establish that the organization performed the required quarterly assessment for the second quarter. At that point, the Lead Assessor cannot determine that the practice is satisfied based solely on the first-quarter report, so the evidence is insufficient and the finding should initially reflect that status.

However, the scenario identifies a specific, imminent source of potentially relevant evidence: the individual responsible for the second-quarter assessment will return in two hours. Assessment evidence collection occurs throughout the assessment activity, and assessors may examine additional evidence and update a preliminary determination before assessment results are finalized. Once the second-quarter report is produced and examined, it may demonstrate that the organization followed its documented quarterly assessment frequency and that the assessment was performed effectively. The Lead Assessor should therefore re-rate the finding based on the complete evidence set available before finalizing the assessment result.

This approach aligns with the CMMC assessment process, which requires objective evidence to support findings while allowing the assessment team to evaluate evidence obtained during the assessment. See the Cyber AB CMMC Assessment Process resources and the DoD CMMC Model documentation.

QUESTION NO: 8

What type of information is NOT intended for public release and is provided by or generated for the government under a contract to develop or deliver a product or service to the government, but not including information provided by the government to the public (such as on public websites) or simple transactional information, such as necessary to process payments?

A. CDI

B. CTI

C. CUI

D. FCI

ANSWER: D

Explanation:

FCI is correct because the wording in the question tracks the federal definition of Federal Contract Information. FCI is information that is not intended for public release and is provided by, or generated for, the Government under a contract to develop or deliver a product or service to the Government. This category includes information a contractor creates, receives, stores, or transmits while performing a federal contract when that information has not been designated for public release. The definition expressly excludes information the Government provides to the public, including material published on public-facing websites, as well as simple transactional information needed to process payments. In CMMC, protection of FCI is addressed through the foundational safeguarding requirements aligned to FAR 52.204-21. An organization handling FCI

must apply the required basic safeguards to systems that process, store, or transmit that information. The regulatory definition and exclusions appear in FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems. Cyber AB's CMMC model materials also identify FCI as a protected information type within CMMC assessment and scoping considerations; see the CMMC Model Overview.

QUESTION NO: 9

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: B

Explanation:

Restricted IS is correct because the defining facts are that the systems are contractor-owned, are used in support of a government contract, and must be configured according to government-specified requirements. In CMMC scoping terminology, Restricted Information Systems are a Specialized Asset category for contractor systems subject to particular contractual or government configuration requirements. Their classification turns on the required restricted configuration and contractual purpose, rather than on who owns the business network over which Federal Contract Information transactions occur.

Asset ownership is particularly important here: contractor ownership is fully consistent with a Restricted Information System. The stated government requirements also establish that these are not simply ordinary contractor IT assets; their required configuration is tied to supporting the contract. CMMC scoping requires an organization to identify assets and categorize them appropriately so that the assessment boundary and treatment of Specialized Assets can be determined consistently. The official CMMC Level 2 Scoping Guide describes Specialized Assets and the Restricted Information Systems category in the context of scoping systems that support contractual obligations. See the DoD CMMC Level 2 Scoping Guide and Cyber AB's CMMC ecosystem resources.

QUESTION NO: 10

When a conflict of interest is unavoidable, a CCP should NOT:

A. Inform their organization

B. Take action to minimize its impact

C. Disclose it to affected stakeholders

D. Conceal it from the Assessment Team lead

ANSWER: D

Explanation:

"Conceal it from the Assessment Team lead" is correct because a conflict of interest that cannot be avoided must be handled transparently, not hidden. A Certified CMMC Professional has an ethical duty to preserve the independence, objectivity, and credibility of CMMC assessment activities. Prompt disclosure enables the relevant organization and assessment leadership to evaluate the conflict, determine whether mitigation is sufficient, and document or implement appropriate safeguards. Depending on the circumstances, safeguards may include limiting the individual's role, assigning work to another qualified person, or otherwise managing the conflict so that assessment conclusions remain trustworthy. Concealment prevents

informed oversight and undermines confidence that assessment evidence and findings were reached impartially. It also conflicts with the professional-conduct expectation that CMMC ecosystem participants avoid actual or perceived circumstances that could improperly influence professional judgment. The CMMC Assessment Process describes the formal assessment framework and the importance of objective, defensible assessment results, while Cyber AB professional standards establish ethical expectations for people performing CMMC-related services. See the Department of Defense's CMMC Model and assessment resources and Cyber AB's professional ecosystem information.

QUESTION NO: 11

Which domains are a part of a Level 1 Self-Assessment?

A. Access Control (AC), Risk Management < RM), and Media Protection (MP)

B. Risk Management (RM). Access Control (AC), and Physical Protection (PE)

C. Access Control (AC), Physical Protection (PE), and Identification and Authentication (IA)

D. Risk Management (RM). Media Protection (MP), and Identification and Authentication (IA)

ANSWER: C

Explanation:

Access Control (AC), Physical Protection (PE), and Identification and Authentication (IA) is correct because each of these three domains contains CMMC Level 1 practices that an organization must address during its annual Level 1 self-assessment. Level 1 is aligned to the Federal Acquisition Regulation basic safeguarding requirements for Federal Contract Information and consists of 17 practices across six domains. Access Control includes practices such as limiting system access to authorized users and controlling external connections. Physical Protection addresses safeguards for physical access to organizational systems, equipment, and operating environments. Identification and Authentication requires organizations to identify system users, processes acting on behalf of users, and devices, and to authenticate identities before granting access. These requirements support the foundational objective of Level 1: protecting Federal Contract Information through basic cyber hygiene. The assessment is performed by the organization and affirmed annually by a senior official, using the applicable CMMC assessment requirements and evidence for each Level 1 practice. Cyber AB's CMMC resources describe the Level 1 scope and assessment ecosystem, while the DoD assessment guide maps the Level 1 practices to their domains and assessment objectives. See Cyber AB: CMMC Assessment Process and the DoD CMMC Level 1 Assessment Guide.

QUESTION NO: 12

How many domains does the CMMC Model consist of?

A. 14 domains

B. 43 domains

C. 72 domains

D. 110 domains

ANSWER: A

Explanation:

14 domains is correct. The current CMMC 2.0 Model organizes its security requirements into 14 domains that align with the control families in NIST Special Publication 800-171 Rev. 2. For CMMC Level 2, these domains provide the structure for the 110 security requirements used to protect Federal Contract Information and, particularly, Controlled Unclassified Information in the defense industrial base. The domains include areas such as access control, audit and accountability, configuration management, incident response, media protection, personnel security, risk assessment, security assessment, system and communications protection, and system and information integrity. A domain is a logical grouping of related cybersecurity requirements; it is not a count of practices, assessment objectives, or total requirements. Consequently, the number 110

commonly associated with CMMC refers to Level 2 security requirements, whereas the Model's organizational framework consists of 14 domains. Cyber AB's CMMC Model resources describe the model and its alignment with NIST SP 800-171, and the Department of Defense CMMC Program page provides the authoritative program context. See The Cyber AB CMMC Model and DoD CMMC Program.

QUESTION NO: 13

During a Level 2 assessment, the OSC provides a policy stating that removable media are restricted on CUI workstations. Endpoint-management screenshots show that USB storage is disabled for most users. An engineer explains that several users receive exceptions, but the OSC cannot provide approved exception records or demonstrate how those exceptions are reviewed. What is the BEST next assessment activity?

A. Accept the policy because it establishes the OSC's intended restriction.

B. Examine the exception process and test whether unauthorized removable-media use is prevented.

C. Exclude the affected workstations because they use removable media only occasionally.

D. Record all removable-media exceptions as automatically authorized.

ANSWER: B

Explanation:

Examine the exception process and test whether unauthorized removable-media use is prevented is correct. The policy and general endpoint configuration are relevant evidence, but the stated exceptions may materially affect implementation across the assessment scope. The Assessment Team should obtain evidence that exceptions are authorized and controlled, then test or demonstrate that the implemented restrictions operate as described.

Relying only on the policy or on the engineer's interview response would not provide sufficient corroboration. The team should evaluate the actual configuration and exception controls to determine whether use of removable media is limited to authorized purposes and users.

QUESTION NO: 14

A CCP is on their first assessment for CMMC Level 2 with an Assessment Team and is reviewing the CMMC Assessment Process to understand their responsibilities. Which method gathers information from the subject matter experts to facilitate understanding and achieve clarification?

A. Test

B. Examine

C. Interview

D. Assessment

ANSWER: C

Explanation:

Interview is correct because it is the assessment method used to obtain information directly from people who are knowledgeable about the assessed environment, including subject matter experts and personnel responsible for implementing or operating a practice. During an interview, assessors ask targeted questions to understand how an activity is performed, clarify the scope and operation of systems or processes, and corroborate their understanding of implementation. This enables the Assessment Team to resolve ambiguities and obtain context that may not be apparent from artifacts or technical observations alone.

CMMC Level 2 assessments use the assessment methods derived from NIST SP 800-171A: examine, interview, and test. NIST describes interviews as a means to obtain information from individuals or groups, including clarification of assessment evidence and implementation details. A CCP supporting an assessment should understand that interviews are conducted as

part of the evidence-gathering process and should be planned and documented consistently with the assessment objectives. The official CMMC assessment guidance applies these methods when determining whether practices are met. See NIST SP 800-171A and the DoD's CMMC Assessment Guides.

QUESTION NO: 15

Which statement BEST describes the key references a Lead Assessor should refer to and use the:

A. DoD adequate security checklist for covered defense information.

B. CMMC Model Overview as it provides assessment methods and objects.

C. safeguarding requirements from FAR Clause 52.204-21 for a Level 2 Assessment.

D. published CMMC Assessment Guide practice descriptions for the desired certification level.

ANSWER: D

Explanation:

Published CMMC Assessment Guide practice descriptions for the desired certification level is correct because the Assessment Guide supplies the authoritative, practice-level criteria an assessment team uses to determine whether the organization satisfies CMMC requirements. For each practice, the guide identifies the assessment objectives that must be addressed and provides the discussion, examination, interview, and test considerations that support a consistent evidence-based assessment. A Lead Assessor uses these descriptions to plan the assessment, direct the collection and review of objective evidence, record findings, and support the final determination of whether requirements have been met at the scope and certification level requested by the organization seeking certification.

This aligns with the CMMC assessment approach: certification assessments are performed against the requirements and assessment objectives applicable to the selected CMMC level, rather than against a generalized compliance checklist. The CMMC Assessment Guides are published by the Department of Defense and are intended to be used with the applicable CMMC model requirements. The Cyber AB's assessment-process materials likewise describe use of the relevant CMMC Assessment Guide as part of conducting a CMMC assessment. See the DoD's CMMC documentation library and The Cyber AB's assessment information.

QUESTION NO: 16

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

A. NARA

B. CMMC-AB

C. DoD Contractors FAQ page

D. DoD 239.7601 Definitions page

ANSWER: A

Explanation:

NARA is correct because the National Archives and Records Administration administers the federal Controlled Unclassified Information Program and maintains the authoritative CUI Registry. An OSC can use the Registry to identify the meaning of CUI category markings, including the controlled-unclassified designation, the specified privacy category indicator, and applicable dissemination controls such as "FED Only." The Registry supplies the category definitions, required handling authorities, marking syntax, and guidance needed to interpret CUI markings consistently. This is especially important for an organization seeking CMMC compliance because protecting CUI begins with correctly recognizing the information and understanding the handling restrictions attached to it. The CUI Registry is the government's central reference point for these determinations; it is not merely general awareness material. NARA's CUI Program page explains the program's government-

wide role and links to authoritative program resources, while the Registry provides the detailed category and marking information needed to evaluate markings encountered in operational communications. See the NARA Controlled Unclassified Information Program and the CUI Registry Category List.

QUESTION NO: 17

An Assessment Team is conducting a Level 2 Assessment at the request of an OS

C.

The team has begun to score practices based on the evidence provided. At a MINIMUM what is required of the Assessment Team to determine if a practice is scored as MET?

A. All three types of evidence are documented for every control.

B. Examine and accept evidence from one of the three evidence types.

C. Complete one of the following; examine two artifacts, either observe a satisfactory demonstration of one control or receive one affirmation from the OSC personnel.

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

ANSWER: D

Explanation:

“Complete two of the following: examine one artifact, either observe a satisfactory demonstration of one control or receive one affirmation from the OSC personnel.” is correct because a Level 2 assessment requires the Assessment Team to obtain sufficient, objective evidence using at least two assessment methods to determine that a practice is implemented. The CMMC assessment methodology uses examination, interview, and test as its evidence-gathering methods. For a practice to be scored MET, the minimum evidence combination is examination of at least one artifact plus either an interview-based affirmation from appropriate personnel or a test/observation demonstrating that the practice operates as intended. This combination provides both documented evidence and corroboration of implementation in the OSC environment. The artifacts examined should be relevant to the specific practice and can include policies, procedures, records, configurations, system settings, or other implementation evidence. An affirmation is obtained through discussion with personnel who have knowledge of or responsibility for the practice, while an observation or demonstration allows the assessor to validate operational performance. This minimum evidence standard supports a consistent, defensible determination that the requirement is in place and functioning. See the DoD CMMC documentation library and the CMMC Assessment Process.

QUESTION NO: 18

The Assessment Team has completed the assessment and determined the preliminary practice ratings. The preliminary practice ratings must be shared with the OSC prior to being finalized for submission. Based on this information, the assessor should present the preliminary practice ratings:

A. During the final Daily Checkpoint

B. After discussing with the CMMC-AB

C. Via email after the final Daily Checkpoint

D. Over the phone after the final Daily Checkpoint

ANSWER: A

Explanation:

During the final Daily Checkpoint is correct because Daily Checkpoint Meetings provide the Assessment Team’s structured opportunity to communicate assessment progress and preliminary results with the Organization Seeking Certification during the assessment. Once the team has completed its evidence review and arrived at preliminary practice ratings, the final

checkpoint is the appropriate forum to present those ratings before the results proceed through quality assurance and report-finalization activities. This communication supports transparency, gives the OSC visibility into the team's preliminary determinations, and enables the OSC to identify relevant information or evidence for the team's consideration within the applicable assessment process. The distinction between preliminary ratings and finalized results is important: preliminary determinations are communicated before formal submission, while the completed assessment results are conveyed through the established reporting and out-brief process after the required review steps. The Department of Defense CMMC rule also provides an opportunity for re-evaluation of a requirement assessed as not met before delivery of the assessment findings report, reinforcing the need for timely communication of preliminary findings. See the CMMC Program rule in 32 CFR Part 170 and the DoD CMMC Program resources.

QUESTION NO: 19

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

A. OSC

B. C3PAO

C. C3PAO and OSC

D. OSC and Lead Assessor

ANSWER: B

Explanation:

The C3PAO selects the Lead Assessor for the assessment. The C3PAO is the authorized assessment organization that contracts with the OSC, assembles and manages the assessment team, and is accountable for conducting the assessment in accordance with the CMMC Assessment Process. Selecting a qualified, available CMMC Certified Assessor as Lead Assessor is therefore an assessment-organization responsibility. The Lead Assessor directs assessment planning and execution, ensures the team applies the applicable assessment procedures consistently, manages the collection and review of objective evidence, and is responsible for the assessment results submitted through the CMMC ecosystem. This assignment also supports the independence and integrity expected of a third-party assessment: although the OSC coordinates logistics, provides evidence, and identifies assessment scope, it does not appoint the individual who leads the independent assessment. Cyber AB's assessment-process materials describe the C3PAO's responsibility for establishing the assessment team and designating the Lead Assessor. See the CMMC Assessment Process (CAP) and Cyber AB's CMMC Ecosystem Roles resources for the respective responsibilities of C3PAOs, Lead Assessors, and OSCs.

QUESTION NO: 20

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

A. At the time of award

B. Upon solicitation submission

C. Thirty days from the award date

D. Before the due date of submission

ANSWER: A

Explanation:

At the time of award is correct because the CMMC requirement applies as a condition of receiving an applicable DoD contract, rather than as a prerequisite to merely submitting an offer. When a solicitation incorporates the relevant DFARS CMMC clause and identifies a required CMMC Level, the apparently successful offeror must have a current CMMC status at that Level before the Government awards the contract. The contractor's status must be available in DoD's Supplier Performance Risk System (SPRS), which is the system used to record and verify applicable assessment and CMMC status information. This timing supports acquisition continuity: organizations may compete for an opportunity while completing their

compliance preparation, but the Government cannot make the award until the awardee satisfies the solicitation's specified CMMC condition. The precise applicability and timing of the clause are also subject to DoD's phased CMMC implementation, so a contractor should always review the individual solicitation and incorporated clauses. The authoritative DFARS clause language is available at DFARS 252.204-7021. DoD's program materials, including implementation resources and status information, are available through the DoD CMMC Program.

QUESTION NO: 21

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

A. Objectivity, classification, and information accuracy

B. Objectivity, confidentiality, and information integrity

C. Responsibility, classification, and information accuracy

D. Responsibility, confidentiality, and information integrity

ANSWER: D

Explanation:

Responsibility, confidentiality, and information integrity is correct because these concepts express essential professional obligations for individuals participating in the CMMC ecosystem. Responsibility requires a professional to be accountable for actions, judgments, and adherence to applicable program requirements. Confidentiality requires appropriate protection of nonpublic information encountered through CMMC-related work, including sensitive organizational and assessment information. Information integrity requires professionals to ensure that information they create, handle, report, or rely on is accurate, complete, protected from improper alteration, and communicated honestly. Together, these principles support trustworthy assessment activities and confidence in CMMC program outcomes. They are particularly important because CMMC work can involve sensitive defense-industrial-base information and determinations that affect an organization's contractual cybersecurity posture. The Cyber AB administers the CMMC ecosystem and establishes expectations for qualified ecosystem participants; see the Cyber AB website. CMMC's role in protecting Federal Contract Information and Controlled Unclassified Information is described by the Department of Defense at DoD CMMC.

QUESTION NO: 22

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

Explanation:

Levels 1, 2, and 3 is correct because protection of Federal Contract Information is established at CMMC Level 1 and remains encompassed as an organization progresses to the higher CMMC levels. Level 1 requires implementation of the basic safeguarding requirements in FAR 52.204-21 for contractor information systems that process, store, or transmit FCI. These practices provide the foundational protections for information supplied by or generated for the government under a federal contract that is not intended for public release. CMMC Level 2 adds the substantially broader set of security requirements derived from NIST SP 800-171 to protect Controlled Unclassified Information, while Level 3 adds further enhanced requirements for organizations facing more advanced threats. Since the model is cumulative in its protection expectations, an organization meeting the requirements at Level 2 or Level 3 also maintains safeguards appropriate for FCI. The applicable level for a contract is determined by the sensitivity of the information involved and the requirements stated in

the solicitation or contract. See the DoD's CMMC Model Overview and the FAR text for Basic Safeguarding of Covered Contractor Information Systems.

QUESTION NO: 23

Which domain references the requirements needed to handle physical or digital assets containing CUI?

A. Media Protection (MP)

B. Physical Protection (PE)

C. System and Information Integrity (SI)

D. System and Communications Protection (SC)

ANSWER: A

Explanation:

Media Protection (MP) is correct because this CMMC domain addresses the safeguarding, handling, storage, transport, access, sanitization, and disposal of media that contains Controlled Unclassified Information (CUI). "Media" includes both physical formats, such as paper records, removable storage, and backup devices, and digital media or media-resident data. The intent is to ensure that CUI remains protected throughout the media lifecycle, including when media is accessed by authorized users, moved outside controlled areas, reused, or destroyed. In CMMC assessments, the Media Protection practices are derived from the NIST SP 800-171 media-protection requirements, including limiting access to CUI on media, marking media appropriately, controlling media transport, sanitizing media before reuse or disposal, and prohibiting the use of portable storage when not authorized. These controls directly address the question's focus on handling assets that contain CUI. NIST describes these requirements in its SP 800-171 Rev. 2 publication; the CMMC program's relationship to NIST requirements is also described in the DoD CMMC Model.

QUESTION NO: 24

An employee transports backup media containing CUI from the OSC's facility to an offsite storage location. The media are placed in a locked container, but the OSC has no record identifying who received the container, when custody changed, or whether all media arrived at the storage location. Which improvement is needed?

A. Maintain accountability for the media during transport

B. Mark the media only with the employee's name

C. Require the employee to memorize the media serial numbers

D. Delay backup-media transport until the annual media review

ANSWER: A

Explanation:

The OSC should **maintain accountability for the media during transport**. CMMC Level 2 practice MP.L2-3.8.3 requires the organization to control access to media containing CUI and maintain accountability for media during transport outside controlled areas.

A locked container can help restrict physical access, but it does not establish accountability for the media throughout the transfer. Custody records or equivalent tracking should enable the OSC to determine who had responsibility for the media and confirm that it reached the intended destination.

QUESTION NO: 25

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: D

Explanation:

Operational technology is correct because machine controllers and assembly machines are systems that monitor or control physical processes in an industrial or manufacturing environment. In CMMC scoping terminology, Operational Technology (OT) is a Specialized Asset category. OT commonly includes industrial control systems and their components, such as programmable logic controllers, production-line machinery, and other devices used to automate or directly control manufacturing operations.

Documenting these assets in the SSP supports accurate system scoping and helps the organization identify the technologies that require security planning. OT environments often have operational characteristics that distinguish them from conventional business IT, including requirements for availability, safety, predictable timing, and compatibility with industrial equipment. Those characteristics make clear asset identification particularly important when establishing the system boundary and describing how the environment is managed.

The Cyber AB's CMMC Assessment Scope guidance identifies OT as a Specialized Asset type and gives examples including machine controllers and assembly machines. NIST's SP 800-82 Rev. 3 also describes OT and industrial control systems as technologies used to control industrial processes.