PassQueen
a.k.a dumpsqueen.com

Certified CMMC Assessor (CCA) Exam

Cyber AB CMMC-CCA

Version Demo

Total Demo Questions: 24

Total Premium Questions: 242

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, CMMC Ecosystem	17
Topic 2, CMMC Model	33
Topic 3, CMMC Assessment Process	58
Topic 4, CMMC Assessment Methodology	131
Topic 5, CMMC Assessment Reporting	2
Topic 6, Mix Questions	1
Total	242

QUESTION NO: 1

The Certification Assessment Readiness Review (CA-RR) aims to determine whether the OSC and the Assessment Team are ready to conduct the assessment as planned and within the allocated time. It addresses all of the following aspects of readiness to conduct the assessment except which one?

A. OSC cybersecurity posture.

B. Assessment readiness.

C. Assessment risk status.

D. Logistics.

ANSWER: A

Explanation:

OSC cybersecurity posture. is the correct exception because the Certification Assessment Readiness Review is a planning and readiness activity, rather than an evaluation of whether the OSC's environment satisfies CMMC practices and processes. During the CA-RR, the assessment team and the OSC confirm that the assessment can proceed as planned: appropriate participants and resources are available, the assessment scope and supporting arrangements are understood, foreseeable assessment risks are identified and managed, and logistical details support completing the work in the scheduled timeframe. This review helps prevent avoidable delays or impediments once assessment activities begin.

The OSC's cybersecurity posture is evaluated during the certification assessment itself through the assessment team's examination, interview, and test activities against the applicable CMMC assessment requirements. In other words, the readiness review confirms that the parties are prepared to perform the assessment; it does not make a determination about the adequacy of the OSC's implemented cybersecurity controls. This distinction preserves the CA-RR's purpose as an assessment-management checkpoint before substantive evidence collection and determination activities occur. The Cyber AB publishes the CMMC Assessment Process as a core ecosystem resource; see Cyber AB CMMC Ecosystem Resources and the Department of Defense's CMMC Model resources.

QUESTION NO: 2

When assessing an environment, the CCA determines that CUI is contained within an IoT device. Which statement MUST be true?

A. The IoT device is a Contractor Risk Managed Asset.

B. The IoT device must be accurately documented within the SSP.

C. An IoT device may not be utilized to process, store, or transmit CUI.

D. Access provisioned to the IoT device must be done in accordance with AC.L2-3.1.1: Limit System Access.

ANSWER: B

Explanation:

The IoT device must be accurately documented within the SSP. An Internet of Things device that contains CUI is within the CMMC assessment scope because it processes, stores, or transmits CUI. IoT devices are specifically recognized in CMMC scoping as Specialized Assets. Their technical characteristics can make full implementation of every CMMC Level 2 practice impracticable, but that status does not remove them from scope or eliminate the requirement to address them in the organization's system-security documentation.

The System Security Plan is the authoritative description of the system boundary, assets, implementations, and security responsibilities supporting protection of CUI. Accordingly, the OSC must identify the IoT device in the SSP and describe its role and relevant security treatment so an assessor can determine how it is included in the assessed environment. Accurate SSP documentation is therefore a mandatory scoping and assessment condition whenever the device contains CUI. This aligns with the Department of Defense's CMMC scoping guidance, which requires Specialized Assets that process, store, or transmit CUI to be documented in the SSP, and with NIST SP 800-171's requirement to develop and periodically update system security plans. See the DoD CMMC documentation page and NIST SP 800-171 Rev. 2.

QUESTION NO: 3

A CCA is asked to validate if an OSC has separated their systems containing CUI from other departments' systems on their local network. Which of the following MUST the CCA assess?

A. Wide Area Network (WAN)

B. Virtual Private Network (VPN)

C. Virtual Local Area Network (VLAN)

D. Network Address Translation (NAT)

ANSWER: C

Explanation:

Virtual Local Area Network (VLAN) is the correct assessment focus because a VLAN is a logical network-segmentation mechanism that can separate systems processing, storing, or transmitting CUI from other local-network systems. In this situation, the CCA should examine the implemented VLAN configuration and supporting network controls to determine whether the CUI environment is actually isolated as claimed. This includes confirming which ports, switch interfaces, wireless networks, and systems belong to the CUI VLAN; verifying that traffic between the CUI segment and other departmental segments is restricted to authorized paths; and reviewing the firewall or routing rules that enforce those restrictions. The assessment is not satisfied merely by a VLAN name or network diagram: the evidence must demonstrate effective separation in the operational environment. The CMMC scoping guidance identifies isolation through subnetworks and technologies including firewalls, routers, and VLANs as a means of separating CUI Assets from out-of-scope assets. Properly assessing the VLAN therefore helps establish both the CUI asset boundary and whether non-CUI systems are prevented from having unauthorized connectivity to CUI systems. See the DoD CMMC Model resources and the Cyber AB CMMC resources.

QUESTION NO: 4

The use of removable storage media remains a source of data breaches. The CMMC requires control of the use of removable media on system components. As a CCA, you can use different assessment methods to determine whether an OSC has met this requirement. What is the best assessment method to ascertain that MP.L2-3.8.7[a] has been met?

A. Examining System Media Protection Policy

B. Interviewing personnel with responsibilities for system media use

C. Testing mechanisms that restrict or prohibit the use of removable media on systems or system components

D. Examining System Design documentation

ANSWER: C

Explanation:

Testing mechanisms that restrict or prohibit the use of removable media on systems or system components is the best assessment method because it directly establishes whether the required control is implemented and operating on the assessed environment. MP.L2-3.8.7 requires an organization to control the use of removable media on system components. For assessment objective MP.L2-3.8.7[a], the assessor needs sufficient objective evidence that removable-media use is actually controlled, rather than merely intended or documented. A practical test can validate technical enforcement such as endpoint-device-control tooling, operating-system policies, BIOS or firmware restrictions, centrally managed allowlists, or restrictions that permit only authorized removable devices. The assessor should perform the test within the agreed assessment scope and rules of engagement, documenting the system or component tested, the attempted removable-media action, the observed enforcement result, and relevant configuration or audit evidence. This produces repeatable, observable evidence of implementation and operational effectiveness. NIST SP 800-171A identifies testing system components and mechanisms as an assessment method for determining whether removable-media controls have been implemented, while the CMMC assessment process uses examination, interview, and test methods to collect and corroborate evidence. See NIST SP 800-171A and the DoD CMMC Model resources.

QUESTION NO: 5

A CCA is assessing the concept of least functionality in accordance with **CM.L2-3.4.6: Least Functionality**.

Which method is the LEAST LIKELY to be useful as an assessment technique?

A. Interview personnel with information security responsibilities.

B. Interview personnel with application development responsibilities.

C. Interview personnel who wrote the configuration management policy.

D. Interview personnel with security configuration management responsibilities.

ANSWER: C

Explanation:

Interview personnel who wrote the configuration management policy. is the least likely useful method because CM.L2-3.4.6 assesses whether systems are actually configured to provide only essential capabilities. Evidence for this practice centers on operational decisions and technical implementation: identifying necessary services, ports, protocols, functions, and applications; disabling or restricting unneeded functionality; and maintaining secure baseline configurations. A person who authored the policy may explain the organization's intended governance language, but policy authorship alone does not establish direct knowledge of how least-functionality requirements are implemented, maintained, or verified on organizational systems. The most meaningful interview evidence therefore comes from personnel who perform, administer, develop, or oversee the relevant technical configuration activities. This distinction aligns with the assessment focus in NIST SP 800-171A, which evaluates whether organizations define and configure only essential capabilities, and with the CMMC Level 2 assessment approach for validating practice implementation through objective evidence. See NIST SP 800-171A and the DoD CMMC Model resources.

QUESTION NO: 6

While reviewing CA.L2-3.12.3: **Security Control Monitoring** , the CCA notices that the assessment period is defined as one year. An OSC ' s SSP states that under CA.L2-3.12.3, security controls are monitored using the same one-year periodicity to ensure the continued effectiveness of the controls. The assessor understands that some CMMC practices can reference other practices for the entirety of their implementation. **Is the OSC's implementation under CA.L2-3.12.3: Security Control Monitoring acceptable?**

A. No, even when referencing other practices more description is always needed.

B. No, monitoring must be conducted on an ongoing basis to ensure continued effectiveness.

C. Yes, a one-year period for security control monitoring is acceptable.

D. Yes, as long as CA.L2-3.12.1 has been scored as MET, they do need to be monitored.

ANSWER: B

Explanation:

No, monitoring must be conducted on an ongoing basis to ensure continued effectiveness. CA.L2-3.12.3 requires an organization seeking CMMC Level 2 certification to monitor its security controls on an ongoing basis so it can determine whether the controls continue to operate effectively as the environment, threats, systems, personnel, and risk conditions change. A statement that monitoring occurs only on a one-year cycle describes a periodic annual activity, rather than an ongoing monitoring process. Although an assessment period may establish the window from which an assessor collects and evaluates evidence, it does not redefine the practice's required operational frequency. The OSC must demonstrate that it performs recurring monitoring activities throughout normal operations, using methods appropriate to its environment and the controls being monitored. Evidence may include review records, alerts, vulnerability-management results, configuration or log reviews, incident-related follow-up, control performance checks, and documented actions to address identified deficiencies. The monitoring approach should provide timely awareness of control degradation or failure and support corrective action before the next annual assessment. This aligns with the CMMC Level 2 assessment objectives for CA.L2-

3.12.3 and with NIST SP 800-171, Requirement 3.12.3, from which the practice is derived. See the DoD CMMC Model resources and NIST SP 800-171 Rev. 2.

QUESTION NO: 7

Does CMMC Level 2 require that a Cloud Service Provider (CSP) hold a FedRAMP HIGH authorization hosted in a government community cloud (GCC)?

A. No. The CSP can obtain a FedRAMP MODERATE equivalency.

B. No. The CSP must hold a FedRAMP MODERATE authorization.

C. Yes. FedRAMP HIGH is required for CUI data controls due to the sensitive nature of the Defense Industrial Base systems.

D. Yes. FedRAMP HIGH authorization demonstrates the CSP compliance with NIST SP 800-53 and SP 800-171 control requirements.

ANSWER: A

Explanation:

No. The CSP can obtain a FedRAMP MODERATE equivalency. is correct because CMMC Level 2 scoping permits use of an external cloud service provider to process, store, or transmit CUI when that provider meets the FedRAMP Moderate baseline through a FedRAMP Moderate authorization or a FedRAMP Moderate equivalency. Equivalency is important: a CSP does not have to be listed as FedRAMP Authorized if it can demonstrate that its service meets the applicable FedRAMP Moderate security requirements through the recognized equivalency approach. CMMC does not itself establish FedRAMP High as the baseline for CUI handled by a CSP, nor does it require the service to be hosted in a Government Community Cloud. The organization remains responsible for correctly scoping the service, defining CUI flows, and ensuring the cloud provider's status or equivalency evidence supports the assessment. A particular DoD contract, program office, or customer may impose additional cloud, location, or authorization conditions, but those would be contractual requirements beyond the general CMMC Level 2 cloud-scoping baseline. The DoD publishes current CMMC policy and assessment documentation at DoD CMMC Documentation. FedRAMP describes its authorization framework and baselines at FedRAMP Authorization.

QUESTION NO: 8

A CMMC assessment involves testing, examining, and interviewing various assessment objects. The definition of an assessment object is provided in NIST SP 800-171A. Which of the following can an Assessment Object NOT be?

A. Activities

B. Specifications

C. Individuals

D. Examine

ANSWER: D

Explanation:

Examine is correct because it identifies an assessment method rather than an assessment object. NIST SP 800-171A distinguishes the things an assessor evaluates from the methods used to obtain and evaluate evidence. Assessment objects are the specific sources or subjects of evidence associated with a requirement, such as specifications, mechanisms, activities, and individuals. An assessor applies an assessment method to one or more of those objects to determine whether the requirement is satisfied. In this model, examining means reviewing, inspecting, observing, reading, or otherwise analyzing relevant evidence, such as policies, procedures, system configurations, records, or artifacts. It therefore describes what the assessor does during the assessment, not the item that is itself being assessed. This distinction is central to CMMC assessment execution: assessors identify appropriate evidence-bearing objects and then use examine, interview, and test

methods to produce assessment findings. NIST's assessment-procedure framework explicitly defines these assessment-object categories and the assessment methods used with them. See NIST SP 800-171A and the official publication PDF at NIST SP 800-171A Rev. 3.

QUESTION NO: 9

An OSC's network diagram shows a separate network segment (192.168.50.0/24) designated for its engineering department. This segment restricts access to specific engineering resources. While the servers are physically located in a shared data center, the network configuration isolates them logically. Through which of the following does the network segmentation create isolation for the engineering department's resources?

A. Logical separation through network configuration

B. Physical barriers within the data center

C. Encryption of engineering data at rest

D. Requirement of a security badge to access the data center

ANSWER: A

Explanation:

Logical separation through network configuration is correct because the dedicated 192.168.50.0/24 segment establishes a distinct logical network boundary for engineering resources. A subnet alone identifies an address range, while the isolation is implemented and enforced through network-device configurations such as virtual LANs, routing controls, firewall rules, access control lists, and default-deny policies that permit only authorized communications into or out of that segment. These controls can restrict access to engineering systems even when those systems share the same physical data-center space, racks, switches, or infrastructure with other organizational resources.

This approach supports CMMC Level 2 network-protection expectations derived from NIST SP 800-171. In particular, requirement 3.13.6 requires an organization to deny network communications traffic by default and allow it only by exception. Properly configured logical segmentation provides a practical mechanism for applying that principle: traffic between engineering resources and other networks is limited to explicitly authorized paths, services, users, and systems. The relevant requirement and discussion are available in NIST SP 800-171 Rev. 2. Cyber AB's official CMMC assessment guidance and model resources are available through the Cyber AB CMMC Assessment Guides.

QUESTION NO: 10

A C3PAO has contracted by an OSC to perform its assessment. Before the assessment, the Lead Assessor asks the OSC to provide an extensive list of evidence, some of which is optional and beyond the minimum requirements. The OSC is not able to fulfill the entire request. One missing document was a current and organized list of the OSC's evidence and mappings.

Given that this is a Level 2 Assessment, what should the Lead Assessor tell the OSC?

A. "The OSC's Assessment Official will be asked to collect evidence when requested by the assessment team."

B. "The OSC must provide the Assessment Team with hardcopy evidence. Electronic evidence will only be collected when needed."

C. "It's okay that the document is missing. The Assessment Team will collect all evidence themselves to ensure its integrity."

D. "The OSC should provide the Assessment Team with a current and organized list of their evidence and process mappings, but the assessment can continue."

ANSWER: D

Explanation:

“The OSC should provide the Assessment Team with a current and organized list of their evidence and process mappings, but the assessment can continue.” is correct. For a Level 2 assessment, the OSC is responsible for making the relevant assessment evidence available so the assessment team can determine whether each applicable practice and assessment objective is met. An organized evidence inventory and mapping to relevant processes, practices, and objectives is an important readiness aid: it enables the team to locate artifacts efficiently, understand what process or control an artifact supports, and plan interviews and demonstrations effectively.

That inventory is valuable because Level 2 assessments involve substantial evidence review across the CMMC Level 2 requirements. However, the assessment is based on the sufficiency, appropriateness, and traceability of the evidence actually examined, including documents, interviews, and demonstrations. A missing evidence-mapping list does not itself establish noncompliance or prevent the assessment team from proceeding. The Lead Assessor should communicate the benefit of providing the list while continuing to coordinate evidence collection within the agreed assessment process and schedule. The Department of Defense’s CMMC Model resources describe the Level 2 requirements, and The Cyber AB publishes assessment ecosystem resources and guidance.

QUESTION NO: 11

An assessor is trying to determine if an OSC performs scans of their information system and real-time scans of files from external sources as files are downloaded or executed.

Which evidence is LEAST LIKELY to help this assessor?

A. System configuration settings

B. System Information and Integrity Policy

C. Alerts from the anti-virus software

D. Interviews with personnel with configuration management responsibility

ANSWER: B

Explanation:

System Information and Integrity Policy is the least likely evidence to establish that the OSC actually performs periodic system scans and real-time scans of externally sourced files. A policy documents the organization’s required or intended approach to system and information integrity, including expectations for malicious-code protection. It can establish that management has defined scanning requirements and assigned responsibilities, but it does not by itself demonstrate that endpoint protection tools are installed, configured for scheduled and on-access scanning, current, enabled, or operating on in-scope systems.

For CMMC assessment purposes, implementation must be substantiated through objective evidence that shows the practice is performed. The CMMC Level 2 practice derived from NIST SP 800-171 requires organizations to perform periodic scans and real-time scans of files from external sources as they are downloaded, opened, or executed. Consequently, evidence demonstrating operational behavior and relevant technical settings is needed to validate the assessment objective; the policy remains useful as supporting governance evidence rather than primary proof of execution. See Cyber AB’s CMMC Assessment Process and NIST SP 800-171 Rev. 2, Requirement 3.14.2.

QUESTION NO: 12

An OSC outsources all of its security incident and event monitoring work to a third-party SO

C.

Additionally, the OSC utilizes a cloud-hosted antivirus (AV) system to fulfill the requirement of having virus protection without hosting additional servers on-site.

During the scoping discussion, both the SOC and AV should be listed as what type of asset?

A. They are CUI Assets due to their operation within a CUI network.

B. They are Out-of-Scope Assets due to being fully hosted/operated by third parties.

C. They are Security Protection Assets due to their performance of security functions.

D. They are Contractor Risk Managed Assets because they are not physically or logically isolated from CUI assets.

ANSWER: C

Explanation:

They are Security Protection Assets due to their performance of security functions. CMMC Level 2 scoping identifies Security Protection Assets as assets that provide security functions or capabilities for the protection of CUI Assets. The third-party SOC performs security event and incident monitoring, a security capability that supports detection, analysis, and response. The cloud-hosted AV system provides malware protection, another security capability required to protect the environment in which CUI is processed, stored, or transmitted. Their external hosting or operation does not remove the security function they provide to the OSC's CUI environment; they must therefore be identified during scoping and considered as part of the assessment boundary as applicable. Depending on the service arrangement and assessment role, an external service provider may also need to participate in supplying evidence for the relevant capabilities. This classification supports evaluation of the CMMC practices addressing system monitoring and malicious-code protection. The DoD's CMMC Level 2 Scoping Guidance defines the relevant asset categories, while NIST SP 800-171 Rev. 2 describes the underlying monitoring and malware-protection expectations.

QUESTION NO: 13

You are the CCA working with a client to deliver certified consulting services, and the OSC has asked how to ensure their scope is accurate. You mention the use of a data flow diagram, which intrigues the OSC. What would be the first step in constructing the data flow diagram for the OSC?

A. Implement a Data Loss Prevention (DLP) tool to monitor data flows within the OSC

B. Conduct interviews with key stakeholders to understand the organization's business processes

C. Identify how data flows through the OSC's business, including systems, subprocesses, and data stores, identifying major inputs and outputs to the environment

D. Gather information about the OSC's network infrastructure and create a network diagram

ANSWER: C

Explanation:

"Identify how data flows through the OSC's business, including systems, subprocesses, and data stores, identifying major inputs and outputs to the environment" is the correct first step because a data flow diagram must first establish what information enters, is processed within, is stored by, and leaves the organizational environment. This initial mapping identifies the business processes and technical components that handle relevant information, including CUI when applicable. It gives the OSC a defensible basis for determining which assets, people, technologies, and supporting services fall within the CMMC assessment scope. Once the major inputs, outputs, systems, subprocesses, and data stores are identified, the organization can refine the diagram with data types, transfer methods, trust boundaries, external connections, and protections. That progression supports accurate and repeatable scoping rather than beginning with a security product or a technical topology alone. CMMC scoping is centered on understanding the environment in which CUI is processed, stored, or transmitted and identifying assets that protect or support that environment. The Department of Defense publishes CMMC program documentation at DoD CMMC Documentation. The foundational protection requirements for CUI systems are also described in NIST SP 800-171 Rev. 2.

QUESTION NO: 14

You are a CCA conducting a CMMC assessment for an OSC. While evaluating Risk Assessment (RA) practices, you check how the OSC has addressed assessment objective [a] of RA.L2-3.11.1, "Determine if the frequency for assessing risk to organizational operations, organizational assets, and individuals is defined." Which Assessment Object would most likely provide the answer to this requirement?

A. Risk Assessment Policy

B. Plan of Actions

C. Risk Assessment Report

D. Vulnerability scanning results

ANSWER: A

Explanation:

Risk Assessment Policy is the assessment object most likely to establish the defined frequency for risk assessments. CMMC Level 2 practice RA.L2-3.11.1 requires an organization to periodically assess risk to organizational operations, assets, and individuals resulting from system processing, storage, or transmission of CUI. For assessment objective [a], the assessor is looking specifically for a defined cadence—not merely evidence that an assessment happened at some point. A formally approved policy is the governing specification that normally states the organization's requirements, including how often risk assessments must occur and what events trigger an out-of-cycle assessment, such as significant system, threat, or business changes. The assessor can examine the policy and any referenced procedures to determine whether the frequency is stated clearly enough to guide consistent execution. This aligns with the NIST SP 800-171A assessment procedure for 3.11.1, which directs assessors to examine the risk assessment policy and procedures for an organization-defined frequency. The CMMC assessment process uses such documented artifacts as objective evidence that the practice requirements and their assessment objectives are met. See NIST SP 800-171A and The Cyber AB CMMC Assessment Process.

QUESTION NO: 15

During the planning and preparation discussions, a key member of the C3PAO Assessment Team falls ill and is unavailable for the originally scheduled assessment dates. The OSC is eager to proceed as planned and has expressed willingness to accommodate a smaller assessment team. If the OSC Assessment Official asks the C3PAO for advice on how to proceed, the Lead Assessor, on behalf of the C3PAO, should do which of the following?

A. Provide sufficient advice and recommendations.

B. Politely refuse to provide any advice or recommendations.

C. Provide general advice but avoid specific recommendations that could be seen as implementation assistance.

D. Offer limited advice, but only if the OSC agrees to proceed with the assessment as originally scheduled.

ANSWER: B

Explanation:

"Politely refuse to provide any advice or recommendations." is the appropriate response because a C3PAO must preserve its independence and impartiality when interacting with an OSC. The CMMC Code of Professional Conduct prohibits a C3PAO from offering advice or implementation assistance. That prohibition applies even where the OSC's request appears limited to assessment scheduling or team-size decisions, and even if the OSC is eager to continue. Providing recommendations about how the OSC should proceed could place the C3PAO in an advisory role that is inconsistent with the assessor's independent role.

The Lead Assessor may communicate factual assessment constraints and coordinate administrative matters within the assessment process, but should not recommend a course of action to the OSC. The appropriate professional boundary is to decline the request for advice while maintaining courteous, clear communication. This helps ensure that any subsequent assessment remains objective, that the assessment team does not influence the OSC's decisions, and that the C3PAO remains compliant with applicable professional-conduct obligations. See the Cyber AB's CMMC Code of Professional Conduct and DoD's CMMC Model resources.

QUESTION NO: 16

An OSC is a wholly owned subsidiary of a large conglomerate (parent organization). The OSC and the parent organization use ID badges (PKI cards) that contain a PKI certificate and a radio frequency identification (RFID) tag used for building and

system access (including systems that process, transmit, or store CUI). The parent organization does not make any decisions on how the OSC runs its security program or other matters of significance. The large conglomerate operates a machine that is used to activate the badges for both itself and the OSC. This machine is isolated in a locked room and has no network connectivity to the OSC.

The badge activation system is:

A. In-scope because the parent organization acts as an External Service Provider to the OSC by providing PKI cards.

B. In-scope because the OSC is part of the large conglomerate and thus any CMMC requirements of the OSC are imputed onto the large conglomerate.

C. Out-of-scope because the OSC is the one that assigns the appropriate access to a particular PKI card.

D. Out-of-scope because the badge activation machine is physically and logically isolated from the OSC and it is under the control of the parent organization.

ANSWER: A

Explanation:

In-scope because the parent organization acts as an External Service Provider to the OSC by providing PKI cards. The badge activation system enables credentials that are used to authenticate personnel for physical access and for access to systems that process, transmit, or store CUI. Consequently, the service supports a security function protecting CUI assets: identification, authentication, and access control. Under CMMC Level 2 scoping, technology outside the OSC's direct ownership or operational control can still be in the assessment scope when it is an External Service Provider that provides security protection for CUI assets. The parent organization's lack of involvement in broader OSC security-program decisions does not change the nature of this service. Likewise, physical isolation and lack of network connectivity do not remove a system from scope when it provides a security service relied upon to control access to the OSC's CUI environment. The OSC must therefore account for the service in its CMMC boundary and ensure the applicable requirements are addressed through assessment evidence and appropriate service-provider arrangements. The Department of Defense's CMMC Model resources describe the Level 2 assessment framework, and the DoD CMMC resource page provides the official scoping guidance and program documentation.

QUESTION NO: 17

An OSC is preparing for assessment. Which item of evidence would show the OSC's efforts to restrict physical access within the OSC's environment?

A. VPN configuration

B. Switch configuration files

C. Network architecture drawings

D. Documented OSC procedures for physical access restrictions

ANSWER: D

Explanation:

Documented OSC procedures for physical access restrictions is the appropriate evidence because it directly demonstrates how the OSC defines, administers, and enforces authorized physical access to its facilities, systems, equipment, and operating environments. For CMMC Level 2 practice PE.L2-3.10.1, an assessor needs evidence that the organization limits physical access to authorized individuals. Procedures can establish the operational rules for badge issuance and revocation, visitor authorization and escorting, access to restricted areas such as server rooms, key or access-card control, and periodic review of physical access permissions. Such documentation is a foundational artifact during assessment because it describes the control's intended operation and identifies accountable personnel and processes. The assessor can then validate that the documented process is implemented through interviews, observation of physical safeguards, and supporting artifacts such as visitor logs, access-control records, and authorization lists. This aligns with NIST's requirement to limit physical access to organizational systems, equipment, and operating environments to authorized

individuals, as described in NIST SP 800-171 Rev. 2. Assessment expectations for examining documentation and corroborating implementation are further detailed in NIST SP 800-171A Rev. 2.

QUESTION NO: 18

A company mirrors its FCI/CUI data storage in a cloud environment. Data is managed across multiple virtual machines (VMs). To satisfy requirements for **data security of the LOCAL copy using physical controls**, **what should the OSC do?**

A. Use encrypted transport and storage of FCI/CUI data on the VMs.

B. Store FCI/CUI data without encryption for faster access/backup/restore.

C. Ensure that the VMs are running on hardware that is physically located in a controlled-access facility.

D. In addition to a password or personal identification number, use physical means to log in such as a smart card or hard token.

ANSWER: C

Explanation:

Ensure that the VMs are running on hardware that is physically located in a controlled-access facility. This action addresses the Physical Protection practice requiring the organization to limit physical access to information systems, equipment, and their operating environments to authorized individuals. Although virtual machines are logical constructs, they depend on physical host servers, storage devices, network equipment, and supporting infrastructure. For the local copy of FCI/CUI, the OSC must ensure that the facility housing this underlying hardware has physical-access safeguards, such as authorized-entry controls, visitor management, and protections appropriate to the environment.

This aligns with CMMC Level 2 practice PE.L2-3.10.1, which is derived from NIST SP 800-171 requirement 3.10.1. The objective is to protect the physical environment in which the local systems processing, storing, or transmitting FCI/CUI operate. The OSC remains responsible for implementing and maintaining these controls for in-scope local assets, including the hosts on which the virtual machines execute. See NIST SP 800-171 Rev. 2 and the CMMC Program rule in 32 CFR Part 170.

QUESTION NO: 19

Part of effective CUI protection involves knowing which assets process, transmit, or store CUI. This understanding is crucial for defining CUI boundaries within an OSC's systems. To achieve this, an OSC can prepare a logical data flow diagram for their information systems. Which of the following questions does a logical data flow diagram not answer?

A. How does the data recipient receive the data?

B. How is the system implemented?

C. What data is being transmitted?

D. What system, process, or individual receives the data?

ANSWER: B

Explanation:

"How is the system implemented?" is the correct answer because a logical data flow diagram is intended to show the movement and handling of information at a conceptual level, rather than the technical or physical construction of the environment. For CMMC scoping, the diagram helps an OSC identify where CUI originates, the paths it follows, the people, processes, applications, or external entities that receive it, and the mechanisms or interfaces used to exchange it. This visibility supports accurate identification of CUI assets and the CUI boundary, including systems that process, store, or transmit CUI and the connections that could affect its confidentiality.

System implementation concerns details such as particular hardware, network topology, host configuration, cloud deployment design, operating systems, ports, or physical locations. Those details may be documented in network diagrams,

architecture diagrams, asset inventories, and configuration records, but they are not the purpose of a logical data flow diagram. The distinction is important because an OSC can understand and document CUI movement even when implementation details change, provided the logical flow and relevant boundary relationships remain accurate. See the DoD's CMMC Level 2 Scoping Guidance and Cyber AB's CMMC resource repository.

QUESTION NO: 20

You are the Lead Assessor for a CMMC Level 2 assessment. During the assessment, the OSC admits that a practice was implemented only a week before the assessment began due to a last-minute effort to prepare. The practice appears to meet the objectives based on the evidence provided. How should you evaluate this evidence?

A. Accept the evidence and score the practice as "MET" since it meets the objectives at the time of assessment.

B. Document the recent implementation as an evidence gap and assess based on its effectiveness and sustainability.

C. Score the practice as "NOT MET" because it was not implemented prior to the assessment preparation.

D. Request the OSC to provide evidence of longer-term implementation before proceeding.

ANSWER: A

Explanation:

Accept the evidence and score the practice as "MET" since it meets the objectives at the time of assessment. A CMMC Level 2 assessment determines whether the assessment objectives for each practice are satisfied using sufficient, appropriate, and reliable evidence gathered through examination, interview, and testing. The CMMC assessment methodology does not establish a mandatory minimum implementation period—such as a requirement that a practice have operated for a specified number of weeks or months—before it can receive a MET finding. Therefore, recent implementation alone does not create an evidence gap or prevent a practice from being assessed as implemented.

The assessment team should still apply professional judgment when determining whether the available artifacts, interview responses, and test results are sufficient to support every assessment objective. In this scenario, the question states that the evidence provided demonstrates that the objectives are met. The Lead Assessor should document the evidence and resulting finding in the normal manner and score the practice MET based on the organization's condition during the assessment. This approach is consistent with the CMMC assessment process, which evaluates objective evidence against the practice requirements rather than imposing an unstated longevity requirement. See the CMMC Assessment Guide—Level 2 and the CMMC Program rule in 32 CFR Part 170.

QUESTION NO: 21

A company employs an encrypted VPN to enhance confidentiality over remote connections. The CCA reads a document describing the VPN. It states the VPN allows automated monitoring and control of remote access sessions, helps detect cyberattacks, and supports auditing of remote access to ensure compliance with CMMC requirements.

What document is the CCA MOST LIKELY reviewing to see how these VPNs are controlled and monitored?

A. Access Control Policy

B. Media Protection Policy

C. Audit and Accountability Policy

D. Configuration Management Policy

ANSWER: A

Explanation:

Access Control Policy is correct because VPN-based remote connectivity is an access-control matter: it governs how users and devices are granted, restricted, monitored, and terminated when accessing organizational systems remotely. In CMMC Level 2, the remote-access requirement derived from NIST SP 800-171 calls for monitoring and controlling remote access

sessions. A policy is the document that establishes the organization's management direction, roles, rules, and expectations for those activities. Accordingly, an Access Control Policy commonly addresses approved remote-access methods such as VPNs, authentication expectations, authorization of remote users, session monitoring, restrictions on remote connections, and review of access activity. The described automated monitoring and control capability provides technical support for implementing those policy requirements, while audit records generated by the VPN can provide evidence that the organization follows them. A CCA would review the policy to understand the defined remote-access governance and then validate implementation using procedures, configurations, logs, and interviews. NIST identifies remote-access monitoring and control in requirement 3.1.12 of NIST SP 800-171 Rev. 2. The corresponding CMMC assessment objectives are addressed in the DoD's CMMC Level 2 Assessment Guide.

QUESTION NO: 22

An OSC seeking Level 2 certification is migrating to a fully cloud-based environment. The organization wants to select a Cloud Service Provider (CSP) that can share responsibilities for CMMC Level 2 requirements. Assume both CSPs can equally provide the technical capabilities and business value required.

CSP A has SOC 2 certification and is California Consumer Privacy Act (CCPA) and Health Insurance Portability and Accountability Act (HIPAA) compliant.

CSP B has SOC 2 and FedRAMP Moderate certifications.

Based on this information, which CSP is MOST LIKELY to be acceptable?

A. CSP A

B. CSP B

C. Both CSP A and B

D. Neither CSP A nor B

ANSWER: B

Explanation:

CSP B is most likely to be acceptable because it has FedRAMP Moderate authorization, which provides the relevant federal cloud security baseline for a cloud service that will process, store, or transmit CUI in support of a CMMC Level 2 environment. CMMC Level 2 is aligned to the 110 security requirements in NIST SP 800-171, and the OSC remains responsible for ensuring that external service providers supporting its CUI environment provide appropriate security assurances and shared-responsibility evidence. FedRAMP Moderate is particularly meaningful because it represents an independently assessed authorization framework based on the NIST SP 800-53 Moderate baseline and is recognized for federal cloud use. The OSC must still define the shared-responsibility boundary, verify the provider's authorization scope covers the services used, and implement its own applicable CMMC practices. However, where the providers are otherwise equal, FedRAMP Moderate gives CSP B the strongest and most directly relevant assurance for supporting a Level 2 CUI environment. See the DoD's CMMC Model information and NIST's SP 800-171 Rev. 2 publication.

QUESTION NO: 23

An OSC states that it implements **CM.L2-3.4.8: Application Execution** by maintaining an inventory of approved software. During a demonstration, an employee downloads and runs an unapproved executable from a temporary folder without requesting approval. The OSC explains that the inventory is reviewed quarterly and the unapproved software will be removed during the next review.

How should the CCA evaluate the implementation?

A. As MET because the OSC maintains an inventory of approved software.

B. As NOT MET because the OSC does not prevent the execution of unauthorized software.

C. As MET because the unapproved executable will be removed during the next review.

D. As NOT MET because all software must be developed internally by the OSC.

ANSWER: B

Explanation:

As NOT MET because the OSC does not prevent the execution of unauthorized software is correct. CM.L2-3.4.8 requires the organization to apply deny-by-exception policy to prevent the use of unauthorized software or deny-all, permit-by-exception policy to allow the execution of authorized software. A software inventory is supporting documentation, but it does not itself enforce execution restrictions.

The demonstration provides direct evidence that an unapproved executable can run in the in-scope environment. A quarterly review and subsequent removal may support configuration-management activities, but they do not prevent unauthorized execution at the time it occurs. The assessor should evaluate the mechanisms, configurations, and exception process used to enforce the stated policy.

QUESTION NO: 24

Both the SSP and network diagrams presented to the Lead Assessor by the OSC indicate managed service providers (MSPs) within the assessment boundary. In order to BEST understand the impact of the MSPs, what should the Lead Assessor do?

A. Ascertain what employees the MSP has onsite

B. Request the customer responsibility matrix related to the MSPs

C. Review the inventory to see how the assets have been classified

D. Inspect the other initial documents presented including policies and organization charts

ANSWER: B

Explanation:

Request the customer responsibility matrix related to the MSPs is the best action because this matrix defines how security responsibilities are allocated between the OSC and each managed service provider. Where an MSP provides, administers, monitors, or supports systems within the CMMC assessment boundary, the Lead Assessor needs a clear understanding of which party performs each relevant security activity, maintains the associated evidence, and is accountable for meeting applicable CMMC practice requirements. The matrix helps translate the high-level system relationships shown in the SSP and network diagrams into assessable responsibility assignments. It can identify whether the OSC retains responsibility for configuration, access approvals, log review, incident reporting, vulnerability remediation, backup administration, or other activities that affect protection of CUI. It also helps the assessment team determine appropriate interviewees and evidence sources, including MSP personnel or provider-generated records, while ensuring the OSC can demonstrate implementation of its responsibilities. This is consistent with CMMC scoping, which requires consideration of external service providers and their connections to assets in scope, as well as the assessment process focus on obtaining objective evidence for implemented practices. See the DoD CMMC Model and the CMMC Assessment Process.