Vendor: Cyber AB

Exam Code: CMMC-CCA

Exam Name: Certified CMMC Assessor (CCA) Exam

Version: DEMO

QUESTION 1
A company has a firewall to regulate how data flows into and out of its network. Based on an interview with their IT staff, all connections to their systems are logged, and suspicious traffic generates alerts. Examination of which artifact should give the CCA the details on how these are implemented?

A. Physical access logs
B. Boundary protection procedures
C. Account management document
D. Configuration management policy

Answer: B
Explanation:
The control SC.L2-3.13.5: Boundary Protection requires that organizations monitor and control communications at the external boundary and at key internal boundaries. The CMMC Assessment Guide states that assessors should examine boundary protection procedures to verify logging, monitoring, and alerting are defined and implemented. Physical access logs, account management documents, and configuration management policies do not provide details of how network boundaries are monitored and protected.

QUESTION 2
A Lead Assessor is conducting an assessment for an OSC. The Lead Assessor is collecting evidence regarding the OSC's network separation techniques. Which technique would be considered a logical separation technique and would fall within the scope of the assessment?

A. Data loss alerting configured at the edge of the network containing CUI assets
B. Access limitation based on badge access assigned to employees based on role
C. Role-based access control within a properly implemented identity and access management tool
D. A proxy-configured firewall that prevents data from flowing along the physical connection path

Answer: C
Explanation:
Logical separation refers to the use of technical and access control mechanisms (e.g., role-based access, IAM tools, VLANs) to enforce boundaries between different users, roles, or networks. In contrast, physical separation relies on distinct hardware or physical barriers. Role-based access control within an IAM solution is a textbook example of logical separation, and it is specifically called out in the CMMC/NIST context.

QUESTION 3
An OSC has a headquarters (HQ) site and satellite offices A and B. The two satellite offices are connected to the HQ through a VPN. CUI is stored within the HQ LAN room and used by staff at HQ and Site

A. When categorizing assets for this assessment, assets at the HQ:
B. and Site A contain CUI assets and Site B is out of scope.
C. and Site A and Site B contain CUI assets since all have access to CUI.
D. contain CUI assets and Site A and Site B contain only Certification in Risk Management Assurance.
E. and Site A contain CUI assets and Site B contains only Certification in Risk Assurance.

Answer: A
Explanation:

In CMMC scoping, assets are categorized based on where CUI is processed, stored, or transmitted. According to the CMMC Scoping Guide for Level 2, if CUI is only stored and used in HQ and Site A, those locations contain CUI Assets. Since Site B neither stores, processes, nor transmits CUI, its assets are considered Out of Scope.

QUESTION 4
The audit team is discussing the OSC's Risk Managed Assets. For these types of assets, the contractor need NOT:

A. Provide a network diagram of the assessment scope.
B. Ensure they are included in the pre-assessment discussion.
C. Prepare for the assets to be assessed against CMMC practices.
D. Show how they are being managed using organizational security policies.

Answer: C
Explanation:
Risk Managed Assets are not assessed against CMMC practices, but OSCs must demonstrate that they are identified and that the risk they pose to CUI is managed in accordance with organizational policies. The Scoping Guide specifies that these assets must be addressed in pre-assessment discussions and described in the scope diagram, but they are explicitly excluded from practice-by-practice assessment.

QUESTION 5
A CCA is prohibited from doing which of the following?

A. Verifying key internal system boundaries
B. Determining if physically separated assets contain CUI
C. Ensuring the external system boundary is fully defined
D. Examining whether communications are monitored at the external system boundary

Answer: B
Explanation:
The OSC is responsible for identifying and declaring where CUI is processed, stored, or transmitted. A Certified CMMC Assessor (CCA) may verify boundaries, examine evidence, and confirm monitoring or control practices, but cannot independently determine if a physically separated asset contains CUI. That determination is the responsibility of the OSC, not the assessor.

QUESTION 6
The client has a Supervisory Control and Data Acquisition (SCADA) system as OT to be evaluated as part of its assessment. In reviewing network architecture and conducting interviews, the assessor determines that a firewall separates the SCADA system from the client's enterprise network and that CUI is not processed by the SCADA system. Based on this information, what is an appropriate outcome?

A. The assessor includes the OT within the assessment
B. The assessor determines the SCADA system is out-of-scope for the assessment
C. The assessor includes all systems identified by the client as part of the assessment
D. The assessor determines that all Specialized Assets are within the scope of the assessment

Answer: B

Explanation:
In CMMC scoping, only assets that process, store, or transmit CUI (CUI Assets) or that can access them (Security Protection, Contractor Risk Managed, Specialized Assets) are in-scope. Since the SCADA system is firewalled off and does not handle CUI, it does not fall under CUI Asset classification and is considered Out-of-Scope.

QUESTION 7
An OSC has a testing laboratory. The lab has several pieces of equipment, including a workstation that is used to analyze test information collected from the test equipment. All equipment is on the same VLAN that is part of the certification assessment. The OSC claims that the workstation is part of the test equipment (Specialized Asset) and only needs to be addressed under risk-based security policies. However, the OSC states that the data analysis output is CUI. What is the assessor's BEST response?

A. Disagree with the OSC and include the workstation in the full assessment.
B. Disagree with the OSC and score practice CA.L2-3.12.4: System Security Plan as NOT MET.
C. Agree with the OSC but perform a limited check of the system, not increasing the assessment cost or duration.
D. Agree with the OSC and determine if it is managed using the contractor's risk-based information security procedures and practices.

Answer: A
Explanation:
If an asset processes or generates CUI, it is a CUI Asset by definition, regardless of whether it is also part of a test lab or claimed as a Specialized Asset. Specialized Asset handling applies only when the asset does not process, store, or transmit CUI. Since the workstation outputs CUI, it must be assessed fully against CMMC practices.

QUESTION 8
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:
The Shared Responsibility Matrix (Customer Responsibility Matrix) is a key artifact in CMMC assessments involving MSPs or cloud service providers. It defines what security responsibilities belong to the OSC and which belong to the service provider. To evaluate the MSP's impact, the assessor must review this matrix to understand boundaries of responsibility for CUI protection.

QUESTION 9
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:
When an OSC leverages cloud providers in a CMMC Level 2 assessment, the provider should have FedRAMP Moderate or higher authorization to align with NIST SP 800-171 requirements. SOC 2, HIPAA, or CCPA compliance do not demonstrate federal-level assurance for protecting CUI. Thus, CSP B is the most appropriate choice.

QUESTION 10
An OSC has a minimal physical footprint consisting only of network equipment, workstations, and a centralized domain environment. File storage is centralized in a third-party vendor's FedRAMP Moderate authorized cloud environment, and employees access files using the cloud integration with their workstations. Since CUI is stored in the FedRAMP Moderate authorized environment, the OSC should prepare to have which environment(s) assessed?

A. Cloud environment only
B. OSC's physical network only
C. Cloud environment and the OSC's physical network
D. OSC's physical network, the cloud environment, and the cloud vendor's employee network

Answer: C
Explanation:
Both the CSP's cloud environment and the OSC's on-premises network/workstations are in-scope because CUI is stored in the cloud but also accessed and transmitted by OSC assets. The cloud vendor's internal employee network is not in-scope because only the customer-facing FedRAMP environment is within the assessment boundary.

QUESTION 11
An OSC assigns new hires to work on their hire date. Human Resources ensures that all screening activities are completed before the end of the employees' first week. How should the CCA score PS.L2-3.9.1: Screen Individuals?

A. As NOT MET but it can be remediated post-assessment
B. As NOT MET and this will cause the assessment to fail
C. As MET since the OSC ensured Human Resources was handling the screening
D. As NOT MET because all screening must be completed prior to the start of employment

Answer: D
Explanation:
The control PS.L2-3.9.1: Screen Individuals requires that individuals be screened before authorizing access to organizational systems and CUI. Since employees are assigned to work immediately upon hire, before screenings are complete, this practice is NOT MET. Completing screenings within the first week does not satisfy the requirement.

QUESTION 12
Video monitoring is used by an OSC to help meet PE.L2-3.10.2: Monitor Facility. The OSC's building has three external doors, each with badge access and a network-connected video camera above the door. The video cameras are connected to the same network as employee computers. The OSC contracted a local security company to provide surveillance services. The security company stores the recordings at its premises and requires access to the OSC's network to manage the video cameras. Which factor is a clear negative finding for the OSC's assessment?

A. Video surveillance needs to be of both private and public areas of the building
B. A non-certified third party accesses the OSC's network to manage the cameras
C. Video surveillance alone does not satisfy the facility monitoring requirement of PE.L2-3.10.2
D. A non-certified third party's data center may not store video recordings for a company authorized to process CUI

Answer: B
Explanation:
The negative finding is that the OSC permits an uncertified external security provider to access the OSC's internal network. This introduces unmanaged risk to the CUI environment. CMMC requires the OSC to control and monitor external service provider access. The storage of recordings externally is not inherently noncompliant if properly controlled, and video monitoring is a valid method of meeting PE.L2-3.10.2. The key failure is giving unmanaged third-party access.

QUESTION 13
Both FCI and CUI are stored by an OSC on the same network. Server A contains file shares with FCI, and Server B contains file shares with CUI. The OSC hopes each server would only undergo the assessment for the classification of data it contains. What is the MOST correct assessment situation in this scenario?

A. Due to the presence of CUI on the network, a Level 2 certification is required for the network
B. Server A may undergo a Level 1 self-assessment, while Server B must obtain a Level 2 certification
C. Due to the presence of FCI on the network, only a Level 1 self-assessment is required for the network
D. The network must be segmented to separate FCI from CUI before any assessments can be conducted

Answer: A
Explanation:
When CUI and FCI reside on the same network, the entire environment is considered a CUI environment. The presence of CUI drives the assessment requirement to CMMC Level 2, regardless of whether FCI also exists. Assets cannot be assessed separately under Level 1 vs. Level 2 within the same network boundary.

QUESTION 14
While completing the Level 2 Assessment, the Lead Assessor found that the OSC was deficient on a number of CMMC practices. Forty practices were scored as NOT MET, all on the Authorized Deficiency Corrections list. The OSC remediated 17 of those during closeout, leaving 23 practices still NOT MET. What should the Lead Assessor recommend?

A. Pass the OSC but put the 23 remaining on a POA&M
B. Fail the OSC and require them to remediate and reapply for Level 2 certification
C. Recommend an interim certification and put the 23 remaining practices on a POA&M
D. Recommend an interim certification and revisit the failed practices upon certification renewal

Answer: B
Explanation:
Under CMMC 2.0 Level 2, POA&Ms are permitted only for a limited subset of practices and only if the organization achieves at least 80% compliance, with no high-weight practices failed. With 23 practices NOT MET, the OSC falls below this threshold. Therefore, the Lead Assessor must recommend a Fail, requiring remediation and reassessment.

QUESTION 15
When a CCA is assessing a control through Examine, what MUST they meet?

A. Documents utilized for review must be in their mailed form
B. Documents must be policy, process, and procedure documents
C. Training materials reviewed can be in-process as they are for educational purposes
D. System-level, network, and data flow diagrams must be completed in draft format

Answer: B
Explanation:
The Examine assessment method requires the assessor to review policies, processes, and procedures that are finalized and approved, not drafts or informal materials. This ensures the OSC has formally documented, management-approved artifacts supporting each practice. Drafts, in-process training materials, or incomplete diagrams do not satisfy the "Examine" method requirements.

QUESTION 16
The Lead Assessor is reviewing the Assessment Plan to identify people for interviews regarding a specific Level 2 practice. Some OSC personnel previously interviewed provided only brief answers without meaningful verification. What can the Lead Assessor do to improve this situation going forward?

A. Ensure the people from the training matrix are made available
B. Ensure and verify confidentiality and non-attribution of responses
C. Ensure the respondents sign a non-disclosure agreement for the OSC
D. Ensure and verify the responses map to the documented artifacts

Answer: B
Explanation:
The CMMC Assessment Process emphasizes the importance of confidentiality and non-attribution in interviews to ensure OSC personnel provide candid, accurate information. Interviewees may give shallow or evasive answers if they fear attribution. Assuring confidentiality and non-attribution improves the quality and reliability of responses.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**