



Cyber AB CMMC-CCA Practice Questions

Shared by Shepherd on 12-10-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page



Question 1

Question Type: MultipleChoice

What should the Lead Assessor do to BEST ensure the evidence supplied effectively meets the intent of the standard for a practice?

Options:

- A- Ensure the evidence for each objective under a practice is adequate.
- B- Ensure the evidence is sufficient to meet the requirements for a practice.
- C- Ensure the evidence is complete, validated, and can be mapped to the practice requirements.
- D- Ensure the evidence covers all the scope and the identified organizations and corresponds to the practice and objectives.

Answer:

C

Explanation:

The CAP defines evidence evaluation requirements. Evidence must not only exist but must also be:

Complete (addresses all assessment objectives for the practice)

Validated (verified by the assessor)

Mapped to the practice requirements (traceable to objectives)

Extract:

"The assessor must confirm that the evidence is complete, validated, and mapped directly to the practice requirements in order to conclude that a practice is MET."

Question 2

Question Type: MultipleChoice

Prior to starting an assessment, an OSC must develop a data flow diagram. This diagram can then be used as a tool to help establish the context and boundaries of the CMMC assessment activities. What is critical to capture while developing the data flow diagram?

Options:

- A- The organization's network topology and hardware configurations
- B- A list of all employees and their job functions
- C- The physical layout of the organization's office spaces
- D- Business processes, subprocesses, and assets and systems used to support the process

Answer:

D

Explanation:

Comprehensive and Detailed in Depth

The CMMC Assessment Guide Level 2 requires data flow diagrams to map CUI flows, identifying business processes, subprocesses, and supporting systems/assets to define assessment scope. Option A (network topology) is secondary to data flow. Option B (employees) and Option C (physical layout) are unrelated to logical data mapping. Option D is critical per CMMC guidance, making it the correct answer.

Reference Extract:

CMMC AG Level 2, Section 1.3:"Data flow diagrams capture processes, subprocesses, and systems handling CUI."Resources:https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level2_MasterV2.0_FINAL_202112016_508.pdf

Question 3

Question Type: MultipleChoice

You are assessing a contractor that develops software for air traffic control systems. In reviewing their documentation, you find that a single engineer is responsible for designing new ATC system features, coding the software updates, testing the changes on the development network, and deploying the updates to the production ATC system for customer delivery. What would you recommend the contractor do to avert the risk?

Options:

- A- Institute mandatory overtime for the engineer to complete tasks faster
- B- Fully implement AC.L2-3.1.4, Separation of Duties by assigning different engineers responsibility for design, coding, testing, and deployment. Implement peer code reviews and

separate test and deployment duties

C- Invest in more powerful development machines

D- Increase the engineer's salary to incentivize careful work

Answer:

B

Explanation:

Comprehensive and Detailed In-Depth Explanation:

AC.L2-3.1.4 -- Separation of Duties aims to 'reduce unauthorized activity risk by separating duties.' A single engineer handling all tasks concentrates privileges, increasing error or malice risks. Assigning separate roles and adding peer reviews (B) mitigates this, aligning with CMMC intent. Overtime (A), hardware (C), and salary (D) don't address duty separation or risk reduction.

Extract from Official CMMC Documentation:

CMMC Assessment Guide Level 2 (v2.0), AC.L2-3.1.4: 'Separate duties to reduce risk; implement peer reviews.'

NIST SP 800-171A, 3.1.4: 'Recommend role distribution.'

Resources:

https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level2_MasterV2.0_FINAL_202112016_508.pdf

Question 4

Question Type: MultipleChoice

When assessing a contractor's implementation of CMMC requirements, you realize they have multiple data centers and regional offices, each having its access control mechanisms and security perimeter. The contractor uses a remote access solution to allow external partners and employees to collaborate on projects that involve CUI. The solution requires routing configuration to ensure the remote access to CUI is not compromised. Why should all traffic be routed through a managed Access Control point?

Options:

A- It simplifies network architecture and reduces complexity

- B- Reduces the susceptibility to unauthorized access to organizational systems
- C- It enables easier troubleshooting and monitoring of network traffic
- D- It provides better performance and lower latency for remote users

Answer:

B

Explanation:

Comprehensive and Detailed In-Depth Explanation:

AC.L2-3.1.14 -- Remote Access Routing requires 'routing remote access through managed access control points.' This reduces unauthorized access risk (B) by centralizing control and security, per CMMC intent. Simplification (A), troubleshooting (C), and performance (D) are secondary benefits, not the primary purpose.

Extract from Official CMMC Documentation:

CMMC Assessment Guide Level 2 (v2.0), AC.L2-3.1.14: 'Route traffic to reduce unauthorized access risk.'

NIST SP 800-171A, 3.1.14: 'Examine routing to enhance security.'

Resources:

https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level2_MasterV2.0_FINAL_202112016_508.pdf

Question 5

Question Type: MultipleChoice

Jane is a CCA leading a CMMC assessment for an OSC. During the evaluation, Jane discovers that the OSC's Chief Information Security Officer (CISO) is a former colleague with whom she had a contentious relationship in the past. Unbeknownst to the OSC, Jane still harbors resentment toward the CISO due to their previous conflicts. As the assessment progresses, Jane becomes increasingly critical of the CISO's security practices, scrutinizing every detail and finding fault despite the OSC's best efforts to demonstrate compliance. Given this scenario, how can a Certified CMMC Assessor's personal bias impact the assessment of the OSC?

Options:

- A- Assessor bias has no effect on the assessment process and outcomes

- B- Assessor bias is not a concern in CMMC assessments
- C- Personal bias may result in an unfairly harsh and critical assessment of the OSC
- D- Assessor bias can lead to an overly lenient evaluation of the OSC

Answer:

C

Explanation:

Comprehensive and Detailed in Depth

The CMMC Assessment Process (CAP) warns that personal bias, like Jane's resentment, can skew evidence interpretation, leading to an unfairly harsh assessment. This negative bias contrasts with positive bias (Option D), which causes leniency. Jane's critical stance risks misrepresenting the OSC's compliance, undermining assessment integrity. Options A and B deny bias's documented impact, making Option C the correct answer per CAP.

Reference Extract:

CMMC Assessment Process (CAP) v1.0, Section 2.3:"Negative bias may result in overly critical evaluations, compromising fairness."Resources:<https://cyberab.org/Portals/0/Documents/Process-Documents/CMMC-Assessment-Process-CAP-v1.0.pdf>

Question 6

Question Type: MultipleChoice

When assessing a contractor's implementation of CMMC practices, you examine its SystemSecurity Plan (SSP) to identify its documented measures for audit reduction and reporting. They have a dedicated section in their SSP addressing the Audit and Accountability requirements. You proceed to interview their information security personnel, who informed you that the contractor has a dedicated Security Operations Center (SOC) and uses Splunk to reduce and report audit logs. What key features regarding the deployment of Splunk for AU.L2-3.3.6 -- Reduction & Reporting would you be interested in assessing?

Options:

- A- Ensure that Splunk is configured with appropriate RBAC to restrict access to log data, reports, and dashboards, ensuring that only authorized personnel can view or modify audit logs
- B- Ensure Splunk can retain audit records for a protracted amount of time
- C- Ensure that Splunk employs various filter rules for reducing audit logs to eliminate non-

essential data and processes to analyze large volumes of log files or audit information, identifying anomalies and summarizing the data in a format more meaningful to analysts, thus generating customized reports

D- Ensure Splunk can support compliance dashboards that provide real-time visibility into CMMC compliance status

Answer:

C

Explanation:

Comprehensive and Detailed In-Depth Explanation:

AU.L2-3.3.6 requires 'audit reduction and report generation capabilities.' Key features to assess in Splunk are filtering to reduce logs and analysis/reporting (C), directly meeting objectives [a] and [b]. RBAC (A) relates to AU.L2-3.3.8, retention (B) to AU.L2-3.3.2, and dashboards (D) aren't required, per CMMC focus.

Extract from Official CMMC Documentation:

CMMC Assessment Guide Level 2 (v2.0), AU.L2-3.3.6: 'Assess tools for [a] reducing logs via filters, [b] generating reports with analysis.'

NIST SP 800-171A, 3.3.6: 'Examine reduction and reporting functions.'

Resources:

https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level2_MasterV2.0_FINAL_202112016_508.pdf

Question 7

Question Type: MultipleChoice

You are a Lead Assessor, and an OSC has engaged your C3PAO firm to conduct a CMMC assessment. As the Lead Assessor, you are responsible for identifying, documenting, and communicating any potential risks that could impact the successful completion of the planned assessment. You need to evaluate various risk categories and develop mitigation plans to ensure a smooth assessment process. If a member of the Assessment Team is at risk of being delayed and is unable to start the assessment on time, which of the following would be an appropriate mitigation plan?

Options:

- A- Proceed with the assessment without the delayed team member
- B- Request additional resources from the OSC to compensate for the delayed team member
- C- Reschedule the assessment for a later date
- D- Identify an alternate resource to shadow the Assessment Team member and potentially act as a successor

Answer:

D

Explanation:

Comprehensive and Detailed in Depth

The CMMC Assessment Process (CAP) assigns the Lead Assessor responsibility for risk management, including personnel delays. Identifying an alternate resource to shadow the delayed team member (Option D) ensures continuity by preparing a backup, aligning with CAP's proactive mitigation approach. Option A (proceeding without the member) risks incomplete assessments. Option B (requesting OSC resources) shifts burden inappropriately. Option C (rescheduling) is less efficient than a successor plan. Option D is the correct answer per CAP guidance.

Reference Extract:

CMMC Assessment Process (CAP) v1.0, Section 2.4: "Lead Assessors must mitigate risks, such as identifying alternates for delayed team members." Resources: <https://cyberab.org/Portals/0/Documents/Process-Documents/CMMC-Assessment-Process-CAP-v1.0.pdf>

Question 8

Question Type: MultipleChoice

To showcase progress on the performance of their contract, a contractor provides semi-annual demonstrations to their federal client at the client's conference room. The conference room is inside the client's facility, meaning the contractor does not have control over security. All prototypes and documents subject to the contract are guarded by the contractor's staff whenever they are in transit and at the conference room. How should you, the CCA, handle the conference room when validating the OSC's assessment scope?

Options:

- A- List it as in scope.
- B- List it as a Contractor Risk Managed Asset (CRMA).
- C- More information is needed.
- D- List it as out of scope.

Answer:

D

Explanation:

Comprehensive and Detailed

The CMMC Assessment Scope - Level 2 specifies that the scope includes assets under the OSC's control that process, store, or transmit CUI, or provide security protections for such assets. The conference room, located in the federal client's facility, is not under the OSC's control, and the temporary presence of prototypes and documents does not change this. The OSC mitigates risk by guarding these items, but the room itself is managed by the government's security measures, placing it outside the OSC's assessment boundary. Per the scoping guide, facilities not owned or controlled by the OSC are typically out of scope unless they are integral to CUI handling, which is not the case here due to the temporary nature of use.

Option A is incorrect as the room is not OSC-controlled. Option B misapplies CRMA, which pertains to OSC-managed assets. Option C is unnecessary given the clear lack of OSC control. D is correct per the guidance.

CMMC Assessment Scope - Level 2, Section 2.3.5 (Out-of-Scope Assets), p. 7: 'Assets not under the OSC's control, such as government facilities, are out of scope.'

To Get Premium Files for CMMC-CCA Visit

<https://www.p2pexams.com/products/cmmc-cca>

For More Free Questions Visit

<https://www.p2pexams.com/cyber-ab/pdf/cmmc-cca>

20%
DISCOUNT

P2P
exams