Download Cyber AB CMMC-CCA Exam Dumps Free

Shared by Weaver on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A C3PAO and OSC have agreed to proceed with CMMC assessment planning. The OSC assessment official and the C3PAO are working to determine the planning details and purview of the Assessment, which includes scoping. When should the C3PAO and OSC conduct the high-level contract framing?

Options:

A- After the C3PAO has assigned the Lead Assessor and Assessment Team.
B- At the beginning of their engagement for the CMMC assessment.
C- During Phase 2 of the CMMC assessment process.
D- After the OSC has determined the CMMC Assessment Scope.

Answer:

B

Explanation:

Comprehensive and Detailed in Depth

The CAP requires high-level contract framing at the engagement's start to set expectations, not later (Options A, C, D). Option B ensures alignment from the outset.

Extract from Official Document (CAP v1.0):

Section 1.1 -- Purpose (pg. 7):'High-level contract framing shall be performed jointly by the C3PAO and OSC at the beginning of their engagement.'

CMMC Assessment Process (CAP) v1.0, Section 1.1.

Question 2

Question Type: MultipleChoice

During a social event after work, a CCA from your C3PAO team brags about providing ''consulting advice'' to an OSC they recently assessed for CMMC compliance. You know this directly violates the CoPC's restrictions on CCAs offering such services during an assessment. What is your ethical obligation in this situation?

Options:

A- Publicly confront the CCA and remind them of the CoPC violation.
B- Discreetly approach the CCA and offer to help them understand the CoPC guidelines.
C- Immediately report the incident to the Cyber AB.
D- Ignore the situation, as it doesn't involve you directly.

Answer:

B

Explanation:

Comprehensive and Detailed in Depth

The CoPC encourages internal resolution first (Option B). Option A risks unprofessionalism, Option C skips internal steps, and Option D neglects duty.

Extract from Official Document (CoPC):

Paragraph 4.1(1)(a) -- Violation Reporting (pg. 10):'Attempt to rectify the violation with the individual in question prior to reporting.'

CMMC Code of Professional Conduct, Paragraph 4.1(1)(a).

Question 3

Question Type: MultipleChoice

An OSC is planning a CMMC Level 2 assessment that your C3PAO will conduct. In Phase 1.6.1 -- Access and Verify Evidence, as the Lead Assessor, you are verifying the existence and accessibility of the evidence provided by the OSC. While reviewing the list of evidence mapped against the CMMC practices, you discover that the OSC cannot locate several critical system security policies for key IT systems supporting their DoD contracts. These missing policies are essential for demonstrating compliance with various CMMC practices related to access control, incident response, and system maintenance. Based on the CMMC Assessment Process (CAP), which of the following is not permitted for the Lead Assessor to do during the evidence verification stage?

Options:

A- Review the content of the evidence to identify potential weaknesses.
B- Ensure that no proprietary data is included in the evidence for review.
C- Verify that the evidence exists and is accessible.
D- Offer advice on how the OSC can improve the sufficiency of their evidence.

Answer:

D

Explanation:

Comprehensive and Detailed in Depth

During Phase 1.6.1, the Lead Assessor's role is to verify the existence, accessibility, and relevance of evidence, not to provide consulting or improvement advice, which is explicitly prohibited by the CAP to maintain objectivity. Option A (reviewing content) is part of the verification process. OptionB (ensuring no proprietary data) is a reasonable precaution, though not explicitly mandated. Option C (verifying existence and accessibility) is a core duty. Option D (offering advice) violates the CAP's strict separation between assessment and consulting roles, ensuring impartiality.

Extract from Official Document (CAP v1.0):

Section 1.6.1 -- Access and Verify Evidence (pg. 19):'At no time during this preliminary review of the Evidence shall the Assessment Team provide any advice or recommendation on how the OSC could improve or enhance the sufficiency or adequacy of their presented Evidence.'

CMMC Assessment Process (CAP) v1.0, Section 1.6.1.

Question 4

Question Type: MultipleChoice

Ron is the Lead Assessor for an OSC's CMMC assessment. His team has scheduled interviews and demonstrations with the OSC's system administrator, Olivia. However, on the first day, the CEO informs Ron that Olivia is very ill and is unavailable. The CEO offers to be interviewed about Olivia's responsibilities instead, even though he does not actually perform those tasks. What should Ron do in this scenario?

Options:

A- Have the CEO accompanied by another IT rep during the interview.
B- Interview the CEO.
C- It depends on the specific details discussed during the interview with the CEO.
D- Reschedule the interviews with Olivia or continue with another person who understands and performs Olivia's duties while she is away.

Answer:

D

Explanation:

Comprehensive and Detailed in Depth

The CAP requires interviews with individuals who perform the tasks, not proxies like the CEO (Options A, B, C). Option D ensures compliance by seeking the appropriate personnel.

Extract from Official Document (CAP v1.0):

Section 2.2 -- Conduct Assessment (pg. 25):'Interviews and demonstrations must be conducted with the person responsible for carrying out the work.'

CMMC Assessment Process (CAP) v1.0, Section 2.2; CoPC Paragraph 2.4.

Question 5

Question Type: MultipleChoice

You are the Lead Assessor for an upcoming CMMC assessment with an OSC. You meet with the OSC's Assessment Official to identify and manage any potential conflicts of interest (COIs) that may arise. You explain the importance of avoiding or mitigating COIs to maintain objectivity and impartiality throughout the assessment process. Together, you review the CMMC Code of Professional Conduct and discuss any circumstances that could create a real or perceived COI for you or the assessment team members. What is the primary responsibility of the Lead Assessor regarding conflicts of interest?

Options:

A- Developing mitigation plans independently for any identified COIs.
B- Ensuring that all assessment team members sign the 'Absence of Conflict-of-Interest Confirmation Statement.'
C- Identifying potential COIs and documenting them in the Pre-Assessment Plan.

D- Submitting the signed 'Absence of Conflict-of-Interest Confirmation Statement' to the CMMC Accreditation Body.

Answer:

C

Explanation:

Comprehensive and Detailed in Depth

The CAP designates the Lead Assessor as responsible for identifying and documenting potential conflicts of interest (COIs) in the Pre-Assessment Plan to ensure transparency and objectivity. Option A (developing mitigation plans independently) is incomplete, as mitigation involves collaboration, not unilateral action. Option B (ensuring signatures) is a task but not the primary responsibility. Option D (submitting statements to Cyber AB) is a C3PAO duty, not the Lead Assessor's primary role. Option C aligns with CAP's explicit guidance.

Extract from Official Document (CAP v1.0):

Section 1.5.4 -- Conflict of Interest (pg. 17):'The Lead Assessor is the responsible party for identifying potential COIs and documenting them in the Pre-Assessment Plan.'

CMMC Assessment Process (CAP) v1.0, Section 1.5.4.

Question 6

Question Type: MultipleChoice

When assessing an OSC's compliance with IR requirements, you realize they have deployed a system that tracks incidents, documents details, and updates the status throughout the incident response process. Personnel to whom incidents must be reported are identified and designated. While examining their documentation, you come across an incident response template that they use to capture all relevant information and ensure consistency in reporting to the identified authorities and organizational officials. Interviewing the IR team, you learn there is an escalation process that the contractor's cybersecurity team can use to address more serious incidents. From the scenario, the contractor has met all the required objectives for CMMC practice IR.L2-3.6.2 -- Incident Reporting, meaning its implementation of the said practice will be scored MET with a total of 5 points. For how long must the OSC retain the incident records?

Options:

A- 72 hours
B- 90 days
C- 90 hours
D- 72 days

Answer:

B

Explanation:

Comprehensive and Detailed In-Depth Explanatio n:

IR.L2-3.6.2 requires 'tracking and documenting security incidents.' While CMMC doesn't specify a retention period, DFARS 252.204-7012 mandates retaining incident records for 90 days (B) to support DoD investigations, serving as a practical baseline for CMMC-aligned contractors. Other options (A, C, D) lack regulatory support and are either too short or arbitrary. The CMMC guide references DFARS for operational consistency.

Extract from Official CMMC Documentation:

CMMC Assessment Guide Level 2 (v2.0), IR.L2-3.6.2: 'Document incidents; retention aligns with applicable regulations like DFARS.'

DFARS 252.204-7012: 'Retain incident-related information for at least 90 days.'

Resources:

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

Question 7

Question Type: MultipleChoice

During a CMMC Level 2 assessment, the Assessment Team discovers that the OSC has implemented a practice using a tool that is not listed in their System Security Plan (SSP). The tool appears to meet the assessment objectives for the practice, but its absence from the SSP raises concerns about documentation accuracy. How should the Lead Assessor proceed?

Options:

A- Accept the tool's use as evidence of compliance and proceed without further action, as it

meets the objectives.
B- Request the OSC to update the SSP to include the tool and provide the revised document before continuing the assessment.
C- Document the discrepancy as an evidence gap and assess the practice based on the tool's effectiveness, continuing the assessment.
D- Mark the practice as 'NOT MET' due to the inaccurate SSP, regardless of the tool'seffectiveness.

Answer:

C

Explanation:

Comprehensive and Detailed in Depth

The CAP instructs documenting discrepancies as evidence gaps and assessing based on available evidence (Option C). Option A ignores documentation issues, Option B delays unnecessarily, and Option D is premature without full assessment.

Extract from Official Document (CAP v1.0):

Section 2.2 -- Conduct Assessment (pg. 25):'Incomplete or inaccurate documents should be recorded as evidence gaps, with the practice assessed based on available evidence.'

CMMC Assessment Process (CAP) v1.0, Section 2.2.

Question 8

Question Type: MultipleChoice

During your review of an OSC's system security control, you focus on CMMC practice SC.L2-3.13.9 -- Connections Termination. The OSC uses a custom web application for authorized personnel to access CUI remotely. Users log in with usernames and passwords. The application is hosted on a dedicated server within the company's internal network. The server operating system utilizes default settings for connection timeouts. Network security is managed through a central firewall, but no specific rules are configured for terminating inactive connections associated with the CUI access application. Additionally, there is no documented policy or procedure outlining a defined period of inactivity for terminating remote access connections. Interviews with IT personnel reveal that they rely solely on users to remember to log out of the application after completing their work. Based on the scenario, what is the MOST concerning aspect from a CMMC compliance perspective regarding CMMC practice SC.L2-3.13.9 -- Connections Termination?

Options:

A- The application is hosted on a dedicated server within the company's internal network
B- Users log in with usernames and passwords, potentially lacking multi-factor authentication
C- The lack of a documented policy or a defined period of inactivity for terminating remote access connections creates uncertainty and inconsistency
D- The server operating system utilizes default settings for connection timeouts, which may be insufficient

Answer:

C

Explanation:

Comprehensive and Detailed In-Depth Explanatio n:

SC.L2-3.13.9 requires 'terminating connections after a defined period of inactivity.' The absence of a documented policy and defined inactivity period (C) is most concerning, as it fails the practice's core requirement, leaving termination inconsistent and user-dependent. Hosting location (A) is neutral, MFA (B) relates to AC.L2-3.1.3, and default timeouts (D) are a symptom of the policy gap. The CMMC guide prioritizes defined inactivity controls.

Extract from Official CMMC Documentation:

CMMC Assessment Guide Level 2 (v2.0), SC.L2-3.13.9: 'Define and document inactivity period for termination; lack thereof is non-compliant.'

NIST SP 800-171A, 3.13.9: 'Examine policy for defined inactivity period.'

Resources:

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

Question 9

Question Type: MultipleChoice

During a CMMC assessment, the OSC provides a service-level agreement (SLA) with an external provider as evidence for an inherited practice. The SLA outlines general security commitments but lacks specific details on how the practice's objectives are met. How should the Lead Assessor proceed?

Options:

A- Accept the SLA as sufficient evidence since it shows a contractual obligation.
B- Request additional detailed evidence from the external provider to demonstrate compliance with the practice's objectives.
C- Score the practice as 'NOT MET' due to the lack of specific details.
D- Ask the OSC to renegotiate the SLA to include detailed compliance information.

Answer:

B

Explanation:

Comprehensive and Detailed in Depth

The CAP requires specific evidence for inherited practices beyond general agreements (Option B). Option A lacks detail, Option C is premature, and Option D is consulting, which is prohibited.

Extract from Official Document (CAP v1.0):

Section 2.2 -- Conduct Assessment (pg. 25):'Request detailed evidence from external providers to verify inherited practice objectives beyond general SLAs.'

CMMC Assessment Process (CAP) v1.0, Section 2.2.

Question 10

Question Type: MultipleChoice

A CCA who works for a C3PAO doubles as a penetration tester. When conducting a CMMC assessment for an OSC, he realizes their cybersecurity practices are lacking. Recognizing potential vulnerabilities in their systems, the CCA approaches the OSC's cyber team and offers his penetration testing services. Which CoPC guiding principle or practice has the CCA failed to live up to?

Options:

A- Assurance
B- Conflict of Interest
C- Professionalism
D- Confidentiality

Answer:

C

Explanation:

Comprehensive and Detailed in Depth

Soliciting business during an assessment violates Professionalism (Option C) by misusing the CCA role. Options A (not a CoPC principle), B (related but not primary), and D (unrelated) are incorrect.

Extract from Official Document (CoPC):

Paragraph 2.1 -- Professionalism (pg. 4):'Never actively solicit business from customers during an assessment.'

CMMC Code of Professional Conduct, Paragraph 2.1.