KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

Exam : **CMMC CCP**

Title : Certified CMMC Professional (CCP) Exam

Version : DEMO

1.Plan of Action defines the clear goal or objective for the plan.
What information is generally NOT a part of a plan of action?
A. Completion dates
B. Milestones to measure progress
C. Ownership of who is accountable for ensuring plan performance
D. Budget requirements to implement the plan's remediation actions
Answer: D
Explanation:
Under the Cybersecurity Maturity Model Certification (CMMC) 2.0, a Plan of Action (POA) is a critical document that outlines the specific actions a contractor needs to take to remediate cybersecurity deficiencies. While POAs serve as a roadmap for achieving compliance with required controls, the inclusion of certain elements is standardized.
Key Elements of a Plan of Action (POA)
According to the CMMC guidelines and NIST SP 800-171, which underpins many CMMC requirements, a POA typically includes:
Completion Dates: Identifies target deadlines for resolving deficiencies.
Milestones to Measure Progress: Includes interim steps or markers to ensure progress is monitored over time.
Ownership or Accountability: Clearly assigns responsibility for each action item to specific personnel or teams.
What is Generally NOT Part of a POA?
Budget requirements to implement the plan's remediation actions (Option D) are generally not included in a POA. While budgeting is critical for ensuring the plan's success, it is considered a part of the broader project management or resource planning process, not the POA itself. This distinction is intentional to keep the POA focused on actionable items rather than resource allocation.
Supporting Reference
NIST SP 800-171A, Appendix D: Provides an overview of POA components, emphasizing the prioritization of corrective actions, responsibility, and measurable outcomes.
CMMC Level 2 Practices (Aligned with NIST SP 800-171): Specifically, the focus is on actions, timelines, and accountability rather than financial planning.
By excluding budget details, the POA remains a tactical document that supports immediate action and compliance tracking, separate from financial considerations.

2.During a Level 2 Assessment, an OSC provides documentation that attests that they utilize multifactor authentication on nonlocal remote maintenance sessions. The OSC feels that they have met the controls for the Level 2 certification.
What additional measures should the OSC perform to fully meet the maintenance requirement?
A. Connections for nonlocal maintenance sessions should be terminated when maintenance is complete.
B. Connections for nonlocal maintenance sessions should be unlimited to ensure maintenance is performed properly
C. The nonlocal maintenance personnel complain that restrictions slow down their response time and should be removed.
D. The maintenance policy states multifactor authentication must have at least two factors applied for nonlocal maintenance sessions.

Answer: A
Explanation:
Under CMMC 2.0 Level 2, which aligns with the requirements of NIST SP 800-171, maintaining robust control over nonlocal maintenance sessions is critical. While multifactor authentication (MFA) is a required safeguard for secure access, additional measures must be implemented to fully meet the maintenance requirements as outlined in Control 3.3.5:
Key Requirements for Nonlocal Maintenance:
Termination of Nonlocal Maintenance Sessions:
To reduce the attack surface and prevent unauthorized access, nonlocal maintenance connections must be terminated immediately after the maintenance activity is completed. This is a direct requirement to mitigate risks associated with lingering remote sessions that could be exploited by threat actors.
Supporting
Reference: NIST SP 800-171, Control 3.3.5 states: "Ensure that remote maintenance is conducted in a controlled manner and disable connections immediately after use."
Multifactor Authentication (MFA):
OSCs are required to implement MFA for nonlocal remote maintenance sessions. MFA must include at least two factors (e.g., something you know, something you have, or something you are).
While the OSC's use of MFA satisfies part of the requirement, it does not complete the control unless proper termination procedures are in place.
Policy and Procedure Adherence:
The OSC must also document a maintenance policy and ensure it reflects the need for terminating connections post-maintenance. The policy should outline roles, responsibilities, and steps for ensuring secure nonlocal maintenance practices.
Incorrect Options:
B. Unlimited connections: Allowing unrestricted nonlocal maintenance sessions is a significant security risk and violates the principle of least privilege.
C. Removing restrictions: Removing restrictions for convenience directly undermines compliance and security.
D. Multifactor authentication details: While MFA is necessary, the question states the OSC already uses it. Termination of sessions is the missing requirement.
Conclusion:
The requirement to terminate nonlocal maintenance sessions after maintenance is complete (Option A) is critical for compliance with CMMC 2.0 Level 2 and NIST SP 800-171, Control 3.3.5. This ensures that nonlocal maintenance activities are secured against unauthorized access and potential vulnerabilities.

3.While developing an assessment plan for an OSC. it is discovered that the certified assessor will be interviewing a former college roommate.
What is the MOST correct action to take?
A. Do not inform the OSC and the C3PAO of the possible conflict of interest, and continue as planned.
B. Inform the OSC and the C3PAO of the possible conflict of interest, and start the entire process over without the conflicted team member.
C. Inform the OSC and the C3PAO of the possible conflict of interest but since it has been an acceptable amount of time since college, no conflict of interest exists, and continue as planned.

D. Inform the OSC and the C3PAO of the possible conflict of interest, document the conflict and mitigation actions in the assessment plan, and if the mitigation actions are acceptable, continue with the assessment.

Answer: D

Explanation:

The Cybersecurity Maturity Model Certification (CMMC) Assessment Process (CAP) outlines strict guidelines regarding conflicts of interest (COI) to ensure the integrity and impartiality of assessments conducted by Certified Third-Party Assessment Organizations (C3PAOs) and Certified Assessors (CAs). The scenario presented involves a potential conflict of interest due to a prior relationship (former college roommate) between the certified assessor and an individual at the Organization Seeking Certification (OSC). While this prior relationship does not automatically disqualify the assessor, it must be disclosed, documented, and mitigated appropriately.

CMMC Conflict of Interest Handling Process

Inform the OSC and C3PAO of the Potential Conflict of Interest

The CMMC Code of Professional Conduct (CoPC) requires assessors to disclose any potential conflicts of interest.

Transparency ensures that all parties, including the OSC and C3PAO, are aware of the situation.

Document the Conflict and Mitigation Actions in the Assessment Plan

Per CMMC CAP documentation, potential conflicts should be assessed based on their material impact on the objectivity of the assessment.

The conflict and proposed mitigation strategies must be formally recorded in the assessment plan to provide an audit trail.

Determine If the Mitigation Actions Are Acceptable

If the OSC and C3PAO determine that the mitigation actions adequately eliminate or reduce the risk of bias, the assessment may proceed.

Common mitigation strategies include:

Assigning another assessor for interviews with the conflicted individual.

Ensuring that decisions regarding the OSC's compliance are reviewed independently.

Proceed with the Assessment If Mitigation Is Acceptable

If the mitigation actions sufficiently address the conflict, the assessment may continue under strict adherence to documented procedures.

Why the Other Answers Are Incorrect

A. Do not inform the OSC and the C3PAO of the possible conflict of interest, and continue as planned.

❌Incorrect. This violates CMMC 's integrity requirements and could result in disciplinary actions against the assessor or invalidation of the assessment. Transparency is mandatory.

B. Inform the OSC and the C3PAO of the possible conflict of interest, and start the entire process over without the conflicted team member.

❌Incorrect. The CAP does not mandate immediate reassignment unless the conflict is unresolvable. Instead, mitigation strategies should be considered first.

C. Inform the OSC and the C3PAO of the possible conflict of interest but since it has been an acceptable amount of time since college, no conflict of interest exists, and continue as planned.

❌Incorrect. The passage of time alone does not automatically eliminate a conflict of interest. Proper documentation and mitigation are still required.

CMMC Official Reference

CMMC Assessment Process (CAP) Document – Defines COI requirements and mitigation actions.
CMMC Code of Professional Conduct (CoPC) – Outlines ethical responsibilities of assessors.
CMMC Accreditation Body (Cyber-AB) Guidance – Provides rules on conflict resolution.
Thus, option D is the most correct choice, as it aligns with the official CMMC conflict of interest procedures.

4.A defense contractor needs to share FCI with a subcontractor and sends this data in an email.
The email system involved in this process is being used to:
A. manage FCI.
B. process FCI.
C. transmit FCI.
D. generate FCI
Answer: C
Explanation:
Federal Contract Information (FCI) is defined in FAR 52.204-21 as information provided by or generated for the government under contract but not intended for public release. Under CMMC 2.0, organizations handling FCI must implement FAR 52.204-21 Basic Safeguarding Requirements, ensuring proper protection in processing, storing, and transmitting FCI.
Analyzing the Given Options
The question involves an email system that is used to send FCI to a subcontractor. Let’s break down the possible answers:
A. Manage FCI → Incorrect
Managing FCI involves activities like organizing, storing, and maintaining access to FCI. Sending an email does not fall under management; it is an act of transmission.
B. Process FCI → Incorrect
Processing refers to actively using FCI for operational or analytical purposes, such as analyzing, modifying, or computing data. Simply sending an email does not constitute processing.
C. Transmit FCI → Correct
Transmission refers to the act of sending FCI from one entity to another. Since the contractor is sending FCI via email, this falls under transmitting the data.
Reference: NIST SP 800-171 Rev. 2, 3.1.3 – "Control CUI (or FCI) by transmitting it using authorized mechanisms."
D. Generate FCI → Incorrect
Generating FCI means creating new contract-related information. The contractor is not creating FCI in this scenario but merely transmitting it.
Official Reference Supporting the Correct Answer
CMMC 2.0 Level 1 Practices (FAR 52.204-21 Basic Safeguarding Controls)
3.1.3: "Control CUI (or FCI) by transmitting it using authorized mechanisms."
This confirms that email transmission falls under "transmitting" FCI, not managing or processing.
NIST SP 800-171 Rev. 2 (Protecting CUI in Non-Federal Systems)
Requirement 3.13.8: "Implement cryptographic methods to protect CUI when transmitted."
While this applies more to CUI, FCI should also be protected during transmission, confirming that email is a form of transmitting information.
Conclusion

Since the contractor is sending FCI via email, the correct answer is
C. Transmit FCI. This aligns with CMMC 2.0 Level 1 practices under FAR 52.204-21 and NIST SP 800-171, which emphasize securing transmitted data.

5.Which statement BEST describes an assessor's evidence gathering activities?
A. Use interviews for assessing a Level 2 practice.
B. Test all practices or objectives for a Level 2 practice
C. Test certain assessment objectives to determine findings.
D. Use examinations, interviews, and tests to gather sufficient evidence.
Answer: D
Explanation:
Under the CMMC Assessment Process (CAP) and CMMC 2.0 guidelines, assessors must gather objective evidence to validate that an organization meets the required security practices and processes. This evidence collection is performed through three primary assessment methods:
Examination – Reviewing documents, records, system configurations, and other artifacts.
Interviews – Speaking with personnel to verify processes, responsibilities, and understanding of security controls.
Testing – Observing system behavior, performing technical validation, and executing controls in real-time to verify effectiveness.
Why Option D is Correct
The CMMC Assessment Process (CAP) states that an assessor must use a combination of evidence-gathering methods (examinations, interviews, and tests) to determine compliance.
CMMC 2.0 Level 2 (Aligned with NIST SP 800-171) requires assessors to verify not only that policies and procedures exist but also that they are implemented and effective.
Solely relying on one method (like interviews in Option A) is insufficient.
Testing all practices or objectives (Option B) is unnecessary, as assessors follow scoping guidance to determine which objectives need deeper examination.
Testing only "certain" objectives (Option C) does not fully align with the requirement of gathering sufficient evidence from multiple methods.
CMMC 2.0 and Official Documentation Reference
CMMC Assessment Process (CAP) Guide, Section 3.5 – Assessment Methods explicitly defines the use of examinations, interviews, and tests as the foundation of an effective assessment.
CMMC 2.0 Level 2 Practices and NIST SP 800-171 require assessors to validate the presence, implementation, and effectiveness of security controls.
CMMC Appendix E: Assessment Procedures states that an assessor should use multiple sources of evidence to determine compliance.
Final Verification
To ensure compliance with CMMC 2.0 guidelines and official documentation, an assessor must use examinations, interviews, and tests to gather evidence effectively, making Option D the correct answer.