

Exam CMMC-CCP Braindumps & Reliable CMMC-CCP Source

CMMC CCP PRACTICE EXAM QUESTIONS (DERIVED FROM SHANE'S PRACTICE TEST AND DIRECTLY FROM THE CAP) QUESTIONS WITH COMPLETE SOLUTIONS!!

What is a CUI Asset? Answer - Asset that stores, processes, or transmits CUI
Examples: Servers, Printers, Endpoints, Cloud Services, ERP Systems

Where do you document a CUI Asset? Answer - Document in Asset Inventory
Document in SSP
Document in Network Diagram

What practices do you apply to a CUI Asset? Answer - CMMC Level 2

What does CMMC stand for? Answer - Cybersecurity Maturity Model Certification

How many controls are in CMMC L2? Answer - 110 controls

What impact level is required when storing CUI? Answer - IL4

What contract clause is used for CMMC L1? Answer - FAR 52.204-21 (17 practices in total)

If you want to be CMMC L2 compliant, do you need to also be CMMC L1 compliant?
Answer - Yes

What do you call the part before the first period in the following control? AC.L1-3.1.1
Answer - Domain

What do you call the part after the first period in the following control? AC.L1-3.1.1
Answer - Level

What do you call the part after the dash in the following control? AC.L1-3.1.1 Answer - Security Practice Number

What is confidentiality? Answer - Information Access and disclosure includes means for protecting personal privacy and proprietary information.

P.S. Free 2026 Cyber AB CMMC-CCP dumps are available on Google Drive shared by TrainingQuiz:
https://drive.google.com/open?id=1YDxq3nNDZqrLP93pHnwnyYv_y6wjXCCs

Now it is wise choice for you to choose our CMMC-CCP actual test guide materials. Valid exam questions help you study and prepare double results with half works. You will get high-quality 100% pass rate CMMC-CCP learning prep so that you can master the key knowledge and clear exam easily. You can Pass CMMC-CCP Exam in the shortest time and obtain a certification soon. It will benefit you more. Instead of admiring others' redoubtable life, start your new life from choosing valid test dumps. Our CMMC-CCP actual test guide is the pass king in this field which will be the best option for you.

Cyber AB CMMC-CCP Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none">CMMC Ecosystem: This section of the exam measures the skills of consultants and compliance professionals and focuses on the different roles and responsibilities across the CMMC ecosystem. Candidates must understand the functions of entities such as the Department of Defense, CMMC-AB, Organizations Seeking Certification, Registered Practitioners, and Certified CMMC Professionals, as well as how the ecosystem supports cybersecurity standards and certification.

Topic 2	<ul style="list-style-type: none"> CMMC Governance and Source Documents: This section of the exam measures the capabilities of legal or compliance advisors, covering key regulatory frameworks that govern cybersecurity compliance. Topics include Federal Contract Information, Controlled Unclassified Information, the role of NIST SP 800-171, DFARS, FAR, and the structure and requirements of CMMC v2.0, including self-assessments and certification levels.
Topic 3	<ul style="list-style-type: none"> CMMC Model Construct and Implementation Evaluation: This section of the exam measures the evaluative skills of cybersecurity assessors, focusing on the application and assessment of the CMMC model. It includes understanding its levels, domains, practices, and implementation criteria, and how to assess whether organizations meet the required cybersecurity practices using evidence-based evaluation.
Topic 4	<ul style="list-style-type: none"> CMMC Assessment Process (CAP): This section of the exam measures the planning and execution skills of audit and assessment professionals, covering the end-to-end CMMC Assessment Process. This includes planning, executing, documenting, reporting assessments, and managing Plans of Action and Milestones (POA&M) in alignment with DoD and CMMC-AB methodology.
Topic 5	<ul style="list-style-type: none"> Scoping: This section of the exam measures the analytical skills of cybersecurity practitioners, highlighting their ability to properly define assessment scope. Candidates must demonstrate knowledge of identifying and classifying Controlled Unclassified Information (CUI) assets, recognizing the difference between in-scope, out-of-scope, and specialized assets, and applying logical and physical separation techniques to determine accurate scoping for assessments

>> **Exam CMMC-CCP Braindumps <<**

Reliable CMMC-CCP Source - Exam CMMC-CCP Review

The certification of Cyber AB CMMC-CCP exam is what IT people want to get. Because it relates to their future fate. Cyber AB CMMC-CCP exam training materials are the learning materials that each candidate must have. With this materials, the candidates will have the confidence to take the exam. Training materials in the TrainingQuiz are the best training materials for the candidates. With TrainingQuiz's Cyber AB CMMC-CCP Exam Training materials, you will pass the exam easily.

Cyber AB Certified CMMC Professional (CCP) Exam Sample Questions (Q52-Q57):

NEW QUESTION # 52

In the Code of Professional Conduct, what does the practice of Professionalism require?

- A. Ensure the security of all information discovered or received.
- B. Do not make assertions about assessment outcomes.
- C. Do not copy materials without permission to do so.
- D. Refrain from dishonesty in all dealings regarding CMMC.**

Answer: D

Explanation:

What Does the Practice of Professionalism Require in the CMMC Code of Professional Conduct? The CMMC Code of Professional Conduct (CoPC) sets ethical and professional standards for Certified CMMC Assessors (CCAs) and Certified CMMC Professionals (CCPs). Professionalism requires honesty and integrity in all CMMC-related activities.

Step-by-Step Breakdown:#1. Professionalism Requires Ethical Behavior

* The CoPC states that professionalism includes:

- * Acting with integrity in all assessment-related activities.
- * Providing truthful and objective assessments of cybersecurity practices.
- * Avoiding deceptive or misleading claims about assessments or compliance.

#2. Why the Other Answer Choices Are Incorrect:

- * (A) Do not copy materials without permission to do so#
- * This falls under Intellectual Property (IP) protection, not Professionalism
- * (B) Do not make assertions about assessment outcomes#

* Assessors must provide findings based on evidence. The rule is about not making false or misleading claims, not about avoiding assertions altogether.

* (D) Ensure the security of all information discovered or received#

* This falls under Confidentiality, not Professionalism.

* The CMMC Code of Professional Conduct (CoPC) defines Professionalism as requiring honesty and integrity in all CMMC-related activities.

Final Validation from CMMC Documentation: Thus, the correct answer is:

#C. Refrain from dishonesty in all dealings regarding CMMC.

NEW QUESTION # 53

Ethics is a shared responsibility between:

- A. OSC and sponsors.
- B. members of the CMMC Ecosystem and Lead Assessors.
- **C. CMMC-AB and members of the CMMC Ecosystem**
- D. DoD and CMMC-AB.

Answer: C

NEW QUESTION # 54

An OSC lead has provided company information, identified that they are seeking CMMC Level 2, stated that they handle FCI, identified stakeholders, and provided assessment logistics. The OSC has provided the company's cyber hygiene practices that are posted on every workstation, visitor logs, and screenshots of the configuration of their FedRAMP-approved applications. The OSC has not won any DoD government contracts yet but is working on two proposals. Based on this information, which statement BEST describes the CMMC Level 2 Assessment requirements?

- A. Ready because there is no need to certify this company until after they win a DoD contract.
- B. Ready because all DoD contractors are required to achieve CMMC Level 2; therefore, they are being proactive in seeking certification.
- C. Not ready because the OSC is not on contract because they do not know the scope of FCI protection required by the contract.
- **D. Not ready because the OSC still lacks artifacts that prove they have implemented all the CMMC Level 2 Assessment requirements.**

Answer: D

Explanation:

CMMC Level 2 Readiness and Certification Requirements CMMC Level 2 is required for Organizations Seeking Certification (OSCs) that handle Controlled Unclassified Information (CUI) and aligns with NIST SP 800-171's 110 security controls.

Key Readiness Indicators for a Level 2 Assessment:

The OSC must have implemented all 110 security practices from NIST SP 800-171.

Documented and validated cybersecurity policies and procedures must exist.

The OSC must be prepared to provide objective evidence (artifacts) proving compliance.

Why the OSC in the Question is Not Ready:

They have not won a DoD contract yet# This means they do not yet have a contractually defined CUI environment, which is the foundation for defining their security scope.

They have only provided FCI-related artifacts (e.g., visitor logs, workstation policies, FedRAMP configurations).

Lack of full documentation of CMMC Level 2 controls# The assessment requires evidence for all 110 security practices (e.g., system security plans, incident response records, security awareness training documentation).

A). "Ready because there is no need to certify this company until after they win a DoD contract." Incorrect# Some organizations seek certification proactively before winning contracts. However, readiness depends on implementing all 110 required controls, not contract status alone.

B). "Not ready because the OSC is not on contract because they do not know the scope of FCI protection required by the contract." Incorrect# CMMC Level 2 focuses on CUI, not just FCI. While FCI protection is important, the assessment's focus is on CUI security requirements, which are not fully addressed by the provided artifacts.

D). "Ready because all DoD contractors are required to achieve CMMC Level 2; therefore, they are being proactive in seeking certification." Incorrect# While it is commendable that the OSC is being proactive, readiness is based on full compliance with NIST SP 800-171, not just intent.

References:NIST SP 800-171 Rev. 2(NIST Official Site)
CMMC 2.0 Level 2 Assessment Guide(Cyber AB)
DFARS 252.204-7012 & CMMC 2.0 Requirements(DoD CIO)
#Final Answer C. Not ready because the OSC still lacks artifacts that prove they have implemented all the CMMC Level 2 Assessment requirements.

NEW QUESTION # 55

An OSC lead has provided company information, identified that they are seeking CMMC Level 2, stated that they handle FCI identified stakeholders, and provided assessment logistics. The OSC has provided the company's cyber hygiene practices that are posted on every workstation, visitor logs, and screenshots of the configuration of their FedRAMP-approved applications. The OSC has not won any DoD government contracts yet but is working on two proposals Based on this information, which statement BEST describes the CMMC Level 2 Assessment requirements?

- A. Ready because there is no need to certify this company until after they win a DoD contract.
- B. Ready because all DoD contractors are required to achieve CMMC Level 2; therefore, they are being proactive in seeking certification.
- C. Not ready because the OSC is not on contract because they do not know the scope of FCI protection required by the contract.
- D. Not ready because the OSC still lacks artifacts that prove they have implemented all the CMMC Level 2 Assessment requirements.

Answer: D

Explanation:

CMMC Level 2 Readiness and Certification Requirements CMMC Level 2 is required for Organizations Seeking Certification (OSCs) that handle Controlled Unclassified Information (CUI) and aligns with NIST SP 800-171's 110 security controls.

* Key Readiness Indicators for a Level 2 Assessment:

* The OSC must have implemented all 110 security practices from NIST SP 800-171.

* Documented and validated cybersecurity policies and procedures must exist.

* The OSC must be prepared to provide objective evidence (artifacts) proving compliance.

* Why the OSC in the Question is Not Ready:

* They have not won a DoD contract yet# This means they do not yet have a contractually defined CUI environment, which is the foundation for defining their security scope.

* They have only provided FCI-related artifacts (e.g., visitor logs, workstation policies, FedRAMP configurations).

* Lack of full documentation of CMMC Level 2 controls# The assessment requires evidence for all 110 security practices (e.g., system security plans, incident response records, security awareness training documentation).

* A. "Ready because there is no need to certify this company until after they win a DoD contract."

* Incorrect# Some organizations seek certification proactively before winning contracts. However, readiness depends on implementing all 110 required controls, not contract status alone.

* B. "Not ready because the OSC is not on contract because they do not know the scope of FCI protection required by the contract."

* Incorrect# CMMC Level 2 focuses on CUI, not just FCI. While FCI protection is important, the assessment's focus is on CUI security requirements, which are not fully addressed by the provided artifacts.

* D. "Ready because all DoD contractors are required to achieve CMMC Level 2; therefore, they are being proactive in seeking certification."

* Incorrect# While it is commendable that the OSC is being proactive, readiness is based on full compliance with NIST SP 800-171, not just intent.

References:NIST SP 800-171 Rev. 2(NIST Official Site)

CMMC 2.0 Level 2 Assessment Guide(Cyber AB)

DFARS 252.204-7012 & CMMC 2.0 Requirements(DoD CIO)

#Final Answer: C. Not ready because the OSC still lacks artifacts that prove they have implemented all the CMMC Level 2 Assessment requirements.

NEW QUESTION # 56

According to the Configuration Management (CM) domain, which principle is the basis for defining essential system capabilities?

- A. Essential concern

- B. Least functionality
- C. Separation of duties
- D. Least privilege

Answer: B

Explanation:

Understanding the Principle of Least Functionality in the CM DomainThe Configuration Management (CM) domain in CMMC 2.0 focuses on maintaining the security and integrity of an organization's systems through controlled configurations and restrictions on system capabilities.

The principle of Least Functionality refers to limiting a system's features, services, and applications to only those necessary for its intended purpose. This principle reduces the attack surface by minimizing unnecessary components that could be exploited by attackers.

* CMMC Practice CM.L2-3.4.6 (Use Least Functionality) explicitly states: "Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities."

* The goal is to prevent unauthorized or unnecessary applications, services, and ports from running on the system.

* Examples of Implementation:

* Disabling unnecessary services, such as remote desktop access if not required.

* Restricting software installation to approved applications.

* Blocking unused network ports and protocols.

* A. Least Privilege

* This principle (associated with Access Control) ensures that users and processes have only the minimum level of access necessary to perform their jobs.

* It is relevant to CMMC Practice AC.L2-3.1.5 (Least Privilege) but does not define system capabilities.

* B. Essential Concern

* There is no officially recognized cybersecurity principle called "Essential Concern" in CMMC, NIST, or related frameworks.

* D. Separation of Duties

* This principle (covered under CMMC AC.L2-3.1.4) ensures that no single individual has unchecked control over critical functions, reducing the risk of fraud or abuse.

* While important for security, it does not define essential system capabilities.

* CMMC 2.0 Level 2 Assessment Guide - Configuration Management (CM) Domain

* CM.L2-3.4.6 mandates least functionality to enhance security by removing unnecessary features.

* NIST SP 800-171 (which CMMC is based on) - Requirement 3.4.6

* States: "Limit system functionality to only the essential capabilities required for organizational missions or business functions."

* NIST SP 800-53 - Control CM-7 (Least Functionality)

* Provides detailed recommendations on configuring systems to operate with only necessary features.

Justification for the Correct Answer: Least Functionality (C) Why Other Options Are Incorrect

Official CMMC and NIST References Conclusion The principle of Least Functionality (C) is the basis for defining essential system capabilities in the Configuration Management (CM) domain of CMMC 2.0. By applying this principle, organizations reduce security risks by ensuring that only the necessary functions, services, and applications are enabled.

NEW QUESTION # 57

.....

Passing the CMMC-CCP exam requires the ability to manage time effectively. In addition to the Certified CMMC Professional (CCP) Exam (CMMC-CCP) exam study materials, practice is essential to prepare for and pass the Cyber AB CMMC-CCP exam on the first try. It is critical to do self-assessment and learn time management skills. Because the CMMC-CCP test has a restricted time constraint, time management must be exercised to get success. Only with enough practice one can answer real Cyber AB CMMC-CCP exam questions in a given amount of time.

Reliable CMMC-CCP Source: <https://www.trainingquiz.com/CMMC-CCP-practice-quiz.html>

- Exam CMMC-CCP Braindumps | Professional Reliable CMMC-CCP Source: Certified CMMC Professional (CCP) Exam 100% Pass Search for 「 CMMC-CCP 」 and download it for free immediately on "www.exam4labs.com" CMMC-CCP Minimum Pass Score
- CMMC-CCP Latest Mock Test CMMC-CCP PDF Question CMMC-CCP Online Exam Search on 「 www.pdfvce.com 」 for ⇒ CMMC-CCP ⇌ to obtain exam materials for free download Valid Exam CMMC-CCP Practice
- Study Guide CMMC-CCP Pdf CMMC-CCP Latest Mock Test CMMC-CCP Real Dumps Free The page for free download of 「 CMMC-CCP 」 on ⇒ www.pdfdumps.com will open immediately CMMC-CCP Free

Updates

BONUS!!! Download part of TrainingQuiz CMMC-CCP dumps for free: https://drive.google.com/open?id=1YDxq3nNDZqrLP93pHnwnyYv_y6wjXCcS