

Buy Now and Get Free Cyber AB CMMC-CCP Exam Questions Updates



BTW, DOWNLOAD part of itPass4sure CMMC-CCP dumps from Cloud Storage: https://drive.google.com/open?id=1WmQhb555Txm_Xg7iE3NhtKgdXEJYbOHY

itPass4sure team of professionals made this product after working day and night so that users can prepare from it for the Cyber AB CMMC-CCP certification test successfully. itPass4sure even guarantees that you will pass the Certified CMMC Professional (CCP) Exam (CMMC-CCP) test on the first try by preparing with real questions. If you fail to pass the certification exam, despite all your efforts, you could get a full refund from itPass4sure according to terms and conditions.

In the present situation, you will find companies laying off their employees without any notice or prior information. They are just receiving an email and the next moment they have no access to the company network. So to avoid all this, you have to keep yourself updated with the new version of technologies and applications. You have to become one of Certified CMMC Professional (CCP) Exam (CMMC-CCP) certification holders who survived the laying off situation and are still in a great position in their company. You cannot afford to lose it when you need your job the most.

>> CMMC-CCP Test Dump <<

CMMC-CCP Training Material | Exam CMMC-CCP Registration

If you choose our CMMC-CCP study materials and use our products well, we can promise that you can pass the CMMC-CCP exam and get the CMMC-CCP certification. Then you will find you have so many chances to advance in stages to a great level of social influence and success. Our CMMC-CCP Guide Torrent can also provide all candidates with our free demo, in order to exclude your concerns that you can check our CMMC-CCP exam questions. We believe that you will be fond of our CMMC-CCP learning guide.

Cyber AB CMMC-CCP Exam Syllabus Topics:

Topic	Details
Topic 1	<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
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 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 4	<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 5	<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.

Cyber AB Certified CMMC Professional (CCP) Exam Sample Questions (Q171-Q176):

NEW QUESTION # 171

The director of sales, in a meeting, stated that the sales team received feedback on some emails that were sent, stating that the emails were not marked correctly. Which training should the director of sales refer the sales team to regarding information as to how to mark emails?

- A. C3PAO CUI Introduction to Marking
- B. CMMC-AB CUI Introduction to Marking
- C. FBI CUI Introduction to Marking
- D. NARA CUI Introduction to Marking

Answer: D

Explanation:

The Controlled Unclassified Information (CUI) Program, established by Executive Order 13556, standardizes the handling and marking of unclassified information that requires safeguarding or dissemination controls across federal agencies and their contractors. The National Archives and Records Administration (NARA) serves as the Executive Agent responsible for implementing the CUI Program.

In the context of the Cybersecurity Maturity Model Certification (CMMC) 2.0, particularly at Level 2, organizations are required to protect CUI by adhering to the security requirements outlined in NIST Special Publication 800-171. This includes proper marking of CUI to ensure that all personnel recognize and handle such information appropriately.

The NARA CUI Introduction to Marking provides comprehensive guidance on the correct procedures for marking documents and communications containing CUI. This resource is essential for training purposes, as it offers detailed instructions and examples to help personnel understand and implement proper CUI markings.

By referring the sales team to the NARA CUI Introduction to Marking, the director of sales ensures that the team receives authoritative and standardized training on how to appropriately mark emails and other documents containing CUI, thereby maintaining compliance with federal regulations and CMMC requirements.

NEW QUESTION # 172

Which statement BEST describes the key references a Lead Assessor should refer to and use the:

- A. safeguarding requirements from FAR Clause 52.204-21 for a Level 2 Assessment.
- B. DoD adequate security checklist for covered defense information.
- C. CMMC Model Overview as it provides assessment methods and objects.
- D. published CMMC Assessment Guide practice descriptions for the desired certification level.

Answer: D

Explanation:

Key References for a Lead Assessor in a CMMC Assessment A Lead Assessor conducting a CMMC assessment must rely on official

CMMC guidance documents to evaluate whether an Organization Seeking Certification (OSC) meets the required cybersecurity practices.

The CMMC Assessment Guide provides detailed descriptions of each practice and process at the specific CMMC level being assessed. It defines the assessment objectives for each practice. The required evidence for compliance. The scoring criteria to determine if a practice is MET or NOT MET.

Most Relevant Reference: CMMC Assessment Guide

A). DoD adequate security checklist for covered defense information # Incorrect The DoD adequate security checklist is related to DFARS 252.204-7012 compliance, but CMMC assessments follow the CMMC Assessment Guide.

B). CMMC Model Overview as it provides assessment methods and objects # Incorrect The CMMC Model Overview provides high-level guidance, but does not contain specific assessment criteria.

C). Safeguarding requirements from FAR Clause 52.204-21 for a Level 2 Assessment # Incorrect FAR 52.204-21 is relevant to CMMC Level 1 (FCI protection), but CMMC Level 2 follows NIST SP 800-171 and requires CMMC Assessment Guides for validation.

D). Published CMMC Assessment Guide practice descriptions for the desired certification level # Correct The CMMC Assessment Guide is the official document used to determine if an OSC meets the required security practices for certification.

Why is the Correct Answer "D. Published CMMC Assessment Guide practice descriptions for the desired certification level"?

CMMC Assessment Process (CAP) Document

Specifies that Lead Assessors must use the CMMC Assessment Guide for official scoring.

CMMC Assessment Guide for Level 1 & Level 2

Provides detailed descriptions, assessment methods, and scoring criteria for each practice.

CMMC-AB Guidance for Certified Third-Party Assessment Organizations (C3PAOs) Confirms that CMMC assessments must follow the Assessment Guide, not general DoD security policies.

CMMC 2.0 References Supporting This Answer

Final Answer #D. Published CMMC Assessment Guide practice descriptions for the desired certification level.

NEW QUESTION # 173

Which statement BEST describes an assessor's evidence gathering activities?

- A. Use examinations, interviews, and tests to gather sufficient evidence.
- B. Test all practices or objectives for a Level 2 practice
- C. Use interviews for assessing a Level 2 practice.
- D. Test certain assessment objectives to determine findings.

Answer: A

NEW QUESTION # 174

Which NIST SP discusses protecting CUI in nonfederal systems and organizations?

- A. NIST SP 800-171
- B. NIST SP 800-88
- C. NIST SP 800-53
- D. NIST SP 800-37

Answer: A

Explanation:

Understanding the Role of NIST SP 800-171 in CMMC NIST Special Publication (SP) 800-171 is the definitive standard for protecting Controlled Unclassified Information (CUI) in nonfederal systems and organizations. It provides security requirements that organizations handling CUI must implement to protect sensitive government information.

This document is the foundation of CMMC 2.0 Level 2 compliance, which aligns directly with NIST SP 800-171 Rev. 2 requirements.

Breakdown of Answer Choices NIST SP

Title

Relevance to CMMC

NIST SP 800-37

Risk Management Framework (RMF)

Focuses on risk assessment for federal agencies, not directly applicable to CUI in nonfederal systems.

NIST SP 800-53

Security and Privacy Controls for Federal Systems

Provides security controls for federal information systems, not specifically tailored to nonfederal organizations handling CUI.

NIST SP 800-88

Guidelines for Media Sanitization

Covers secure data destruction and disposal, not overall CUI protection.

NIST SP 800-171

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

#Correct Answer - Directly addresses CUI protection in contractor systems.

Key Requirements from NIST SP 800-171 The document outlines 110 security controls grouped into 14 families, including:

- * Access Control (AC)- Restrict access to authorized users.
- * Audit and Accountability (AU)- Maintain system logs and monitor activity.
- * Incident Response (IR)- Establish an incident response plan.
- * System and Communications Protection (SC)- Encrypt CUI in transit and at rest.

These controls serve as the baseline requirements for organizations seeking CMMC Level 2 certification to work with CUI.

* CMMC 2.0 Level 2 aligns directly with NIST SP 800-171 Rev. 2.

* DoD contractors that handle CUI must comply with all 110 controls from NIST SP 800-171.

Official Reference from CMMC 2.0 Documentation Final Verification and Conclusion The correct answer is D.

NIST SP 800-171, as this document explicitly defines the cybersecurity requirements for protecting CUI in nonfederal systems and organizations.

NEW QUESTION # 175

A CCP is on their first assessment for CMMC Level 2 with an Assessment Team and is reviewing the CMMC Assessment Process to understand their responsibilities. Which method gathers information from the subject matter experts to facilitate understanding and achieve clarification?

- A. Assessment
- B. Examine
- C. Test
- D. Interview

Answer: D

Explanation:

Understanding CMMC Assessment Methods The CMMC Assessment Process (CAP) defines three primary assessment methods used to verify compliance with cybersecurity practices:

- * Examine- Reviewing documents, policies, configurations, and logs.
- * Interview- Engaging with subject matter experts (SMEs) to clarify processes and verify implementation.
- * Test- Observing technical implementations, such as system configurations and security measures.

Since the question asks for a method that gathers information from SMEs to facilitate understanding and achieve clarification, the correct method is Interview.

Why "Interview" is Correct? Interviews are specifically designed to gather information from SMEs to confirm understanding and clarify security processes.

#The CMMC Assessment Guide requires assessors to interview key personnel responsible for cybersecurity practices.

#Examine (Option B) and Test (Option A) are also valid assessment methods, but they do not focus on gathering insights directly from SMEs.

Breakdown of Answer Choices

Option

Description

Correct?

A: Test

#Incorrect- This method involves technical verification, not gathering SME insights.

B: Examine

#Incorrect- This method focuses on document review, not SME interaction.

C: Interview

#Correct - The method used to gather information from SMEs and achieve clarification.

D: Assessment

#Incorrect- This is a general term, not a specific assessment method.

* CMMC Assessment Process Guide (CAP)- Defines Interview as the method for obtaining information from SMEs.

Official References from CMMC 2.0 Documentation Final Verification and Conclusion The correct answer is C. Interview, as this method gathers insights from subject matter experts to verify cybersecurity implementations.

• • • • •

CMMC-CCP Training Material: <https://www.itpass4sure.com/CMMC-CCP-practice-exam.html>

- What's more, part of that iPass4sure CMMC-CCP dumps now are free: https://drive.google.com/open?id=1WmQhb555Txm_Xg7iE3NhtKgdXEJYbOHy

id=1WmQhb555Txm Xg7iE3NhtKgdXEJYbOHy