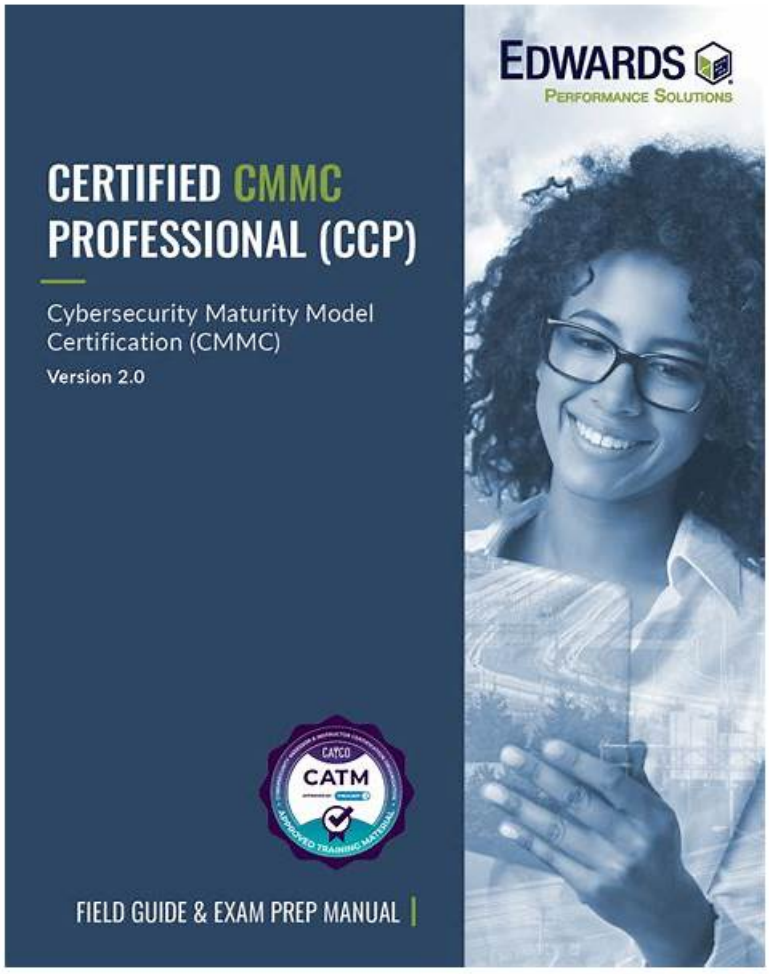
100% Pass 2026 Cyber AB Pass-Sure CMMC-CCP: Certified CMMC Professional (CCP) Exam Testing Center



P.S. Free 2026 Cyber AB CMMC-CCP dumps are available on Google Drive shared by ValidTorrent: https://drive.google.com/open?id=1_EywlCZUsopuZEWCqU8UggYItBzQfbA7

On the one hand, the software version can simulate the real examination for you and you can download our study materials on more than one computer with the software version of our study materials. On the other hand, you can finish practicing all the contents in our CMMC-CCP practice materials within 20 to 30 hours. What's more, during the whole year after purchasing, you will get the latest version of our study materials for free. You can see it is clear that there are only benefits for you to buy our CMMC-CCP learning guide, so why not just have a try right now?

Even the fierce competition cannot stop demanding needs from exam candidates. To get more specific information about our CMMC-CCP learning quiz, we are here to satisfy your wish with following details. So you can get detailed information with traits and information about our CMMC-CCP Real Exam requested on the website. You can free download the demos of our CMMC-CCP exam questions and click on every detail that you are interested.

>> CMMC-CCP Testing Center <<

Free PDF Quiz CMMC-CCP - Certified CMMC Professional (CCP) Exam – High Pass-Rate Testing Center

Facts proved that if you do not have the certification, you will be washed out by the society. So it is very necessary for you to try

your best to get the CMMC-CCP certification in a short time. It is known to us that getting the CMMC-CCP certification has become more and more popular for a lot of people in different area, including students, teachers, and housewife and so on. Everyone is desired to have the certification. Because The CMMC-CCP Certification can bring a lot of benefits for people, including money, a better job and social status and so on.

Cyber AB CMMC-CCP Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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	• 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 4	• CMMC-AB Code of Professional Conduct (Ethics): This section of the exam measures the integrity of cybersecurity professionals by evaluating their understanding of the CMMC-AB Code of Professional Conduct. It emphasizes ethical responsibilities, including confidentiality, objectivity, professionalism, conflict-of-interest avoidance, and respect for intellectual property, ensuring candidates can uphold ethical standards throughout their CMMC-related duties.
Topic 5	• 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.

Cyber AB Certified CMMC Professional (CCP) Exam Sample Questions (Q221-Q226):

NEW QUESTION # 221
When planning an assessment, the Lead Assessor should work with the OSC to select personnel to be interviewed who could:

- A. provide clarity and understanding of their practice activities.
- B. have a security clearance.
- C. demonstrate expertise on the CMMC requirements.
- D. be a senior person in the company.

Answer: A

Explanation:
Interview Selection in CMMC AssessmentsDuring aCMMC assessment, theLead Assessormust work with theOrganization Seeking Certification (OSC)to select personnel for interviews. The goal is to:
#Verify that personnel understand andperform security-related practices.
#Ensure that individuals canexplain how they implement CMMC requirements.
#Gain insight intoactual cybersecurity operationsrather than just documented policies.
The best interviewees are those whodirectly engage with security practicesand canclearly explain how they perform their duties.
CMMC assessmentsrely on interviewsto validate that security practices areimplemented effectively.

Themost valuable intervieweesare those who canexplainhow security measures are appliedin day-to-day operations.
CMMC Assessment Process (CAP)emphasizes that assessors should speak tothose actively involved in security practicesrather than just senior management or policy owners.
Why "Providing Clarity and Understanding" Is KeyThus,option D is the correct choicebecause the Lead Assessor should prioritizeinterviewing personnel who can clearly explain how CMMC practices are implemented.
A). Have a security clearance.#Incorrect.Security clearance is not a requirementfor CMMC assessments. The focus is onpractical implementation of security controls, not classified work.
B). Be a senior person in the company.#Incorrect. Senior executives may not be involved in theactual implementation of security controls. The best interviewees are those whoperform the work, not just oversee it.
C). Demonstrate expertise on the CMMC requirements.#Incorrect. Whileunderstanding CMMC is important, expertise alonedoes not guarantee practical knowledgeof security controls. The key is thatinterviewees must provide clarity on how they perform security tasks.
Why the Other Answers Are Incorrect
CMMC Assessment Process (CAP) Document- Guides interview selection based on personnel who perform security functions.
NIST SP 800-171 & CMMC 2.0- Emphasize that cybersecurity controls must beactively implemented, not just documented.
CMMC Official ReferencesThus,option D (Provide clarity and understanding of their practice activities) is the correct answeras per official CMMC assessment guidelines.

NEW QUESTION # 222
In performing scoping, what should the assessor ensure that the scope of the assessment covers?

- A. All assets regardless if they do or do not process, store, or transmit FCI/CUI
- B. All assets processing, storing, or transmitting FCI/CUI and security protection assets
- C. All assets documented in the business plan
- D. All entities, regardless of the line of business, associated with the organization

Answer: B

Explanation:
Scoping Requirements in CMMC Assessments
TheCMMC 2.0 Scoping GuideandCMMC Assessment Process (CAP) Documentclearly define what should be included in the scope of an assessment.
The assessment scope must cover:
All assets that process, store, or transmit FCI/CUI
Security Protection Assets (ESP)- these assets help protect FCI/CUI, such as firewalls, endpoint detection systems, and encryption mechanisms.
Thus, thecorrect scope includes both:
#FCI/CUI Assets(Data storage, processing, or transmission assets)
#Security Protection Assets (ESP)(Firewalls, security tools, etc.)
Why the Other Answers Are Incorrect
A). All assets documented in the business plan
#Incorrect.Business plans may include assets unrelated to FCI/CUI, making this scopetoo broad. Only assets relevant to FCI/CUI should be assessed.
B). All assets regardless if they do or do not process, store, or transmit FCI/CUI
#Incorrect. CMMC doesnotrequire organizations to include assets thathave no connection to FCI/CUI.
C). All entities, regardless of the line of business, associated with the organization
#Incorrect.Only the assets relevant to FCI/CUI or security protection should be assessed. Unrelated business divisions (like a non-federal commercial division) areout-of-scope.
CMMC Official References
CMMC 2.0 Scoping Guide - Level 1 & Level 2
CMMC Assessment Process (CAP) Document
Thus,option D (All assets processing, storing, or transmitting FCI/CUI and security protection assets) is the correct answeras per official CMMC assessment scoping requirements.

NEW QUESTION # 223
The IT manager is scoping the company's CMMC Level 1 Self-Assessment. The manager considers which servers, laptops. databases, and applications are used to store, process, or transmit FCI. Which asset type is being considered by the IT manager?

- A. Technology
- B. People
- C. ESP
- D. Facilities

Answer: A

Explanation:
Understanding Asset Types in CMMC 2.0In CMMC 2.0, assets are categorized based on their role in handling Federal Contract Information (FCI)orControlled Unclassified Information (CUI). TheCybersecurity Maturity Model Certification (CMMC) Scoping GuidanceforLevel 1andLevel 2provides asset definitions to help organizations identify what needs protection.
According toCMMC Scoping Guidance, there are five primary asset types:
* Security Protection Assets (ESP - External Service Providers & Security Systems)
* People (Personnel who interact with FCI/CUI)
* Facilities (Physical locations housing FCI/CUI)
* Technology (Hardware, software, and networks that store, process, or transmit FCI/CUI)
* CUI Assets (For Level 2 assessments, assets specifically storing CUI) Why "Technology" Is the Correct AnswerThe IT manager is evaluatingservers, laptops, databases, and applications-all of which aretechnology assetsused to store, process, or transmit FCI.
According toCMMC Scoping Guidance,Technology assetsinclude:
#Endpoints(Laptops, Workstations, Mobile Devices)
#Servers(On-premise or cloud-based)
#Networking Devices(Routers, Firewalls, Switches)
#Applications(Software, Cloud-based tools)
#Databases(Storage of FCI or CUI)
Since the IT manager is focusing on these components, the correct asset category isTechnology (Option D).
* A. ESP (Security Protection Assets)#Incorrect. ESPs refer tosecurity-related assets(e.g., firewalls, monitoring tools, managed security services) thathelp protectFCI/CUI but do notstore, process, or transmitit directly.
* B. People#Incorrect. While employees play a role in handling FCI, the question focuses onhardware and software-which falls underTechnology, not People.
* C. Facilities#Incorrect. Facilities refer tophysical buildingsor secured areas where FCI/CUI is stored or processed. The question explicitly mentionsservers, laptops, and applications, which arenot physical facilities.
Why the Other Answers Are Incorrect
* CMMC Level 1 Scoping Guide (CMMC-AB)- Defines asset categories, including Technology.
* CMMC 2.0 Scoping Guidance for Assessors- Provides clarification on FCI assets.
CMMC Official ReferencesThus,option D (Technology) is the most correct choiceas per official CMMC 2.0 guidance.

NEW QUESTION # 224
In late September. CA.L2-3.12.1: Periodically assess the security controls in organizational systems to determine if the controls are effective in their application is assessed. Procedure specifies that a security control assessment shall be conducted quarterly. The Lead Assessor is only provided the first quarter assessment report because the person conducting the second quarter's assessment is currently out of the office and will return to the office in two hours. Based on this information, the Lead Assessor should determine that the evidence is;

- A. insufficient, and rate the audit finding as NOT MET.
- B. insufficient, and re-rate the audit finding after a quarter two assessment report is examined.
- C. sufficient, and re-rate the audit finding after a quarter two assessment report is examined.
- D. sufficient, and rate the audit finding as MET

Answer: A

Explanation:
CA.L2-3.12.1:"Periodically assess the security controls in organizational systems to determine if the controls are effective in their application." This control is derived fromNIST SP 800-171, Requirement 3.12.1, which mandates organizations to performregular security control assessmentsto ensure compliance and effectiveness.
Evidence Review & Assessment Timeline:
The organization's procedureexplicitly statesthat security control assessments must be conductedquarterly (every three months).
Since the Lead Assessor only has access to thefirst-quarter report, the second-quarter report is missing at the time of assessment.
CMMC Audit Requirements:
For an assessor to rate a control asMET, sufficient evidence must bereadily availableat the time of evaluation.

Since the second-quarter report is missingat the time of assessment, the Lead Assessorcannot verify compliancewith the organization's own stated frequency of assessment.
Why the Answer is NOT A, C, or D:
A (Sufficient, MET)#Incorrect: The control assessment frequency is quarterly, but the evidence for Q2 is not available. Compliance cannot be confirmed.
C (Sufficient, and re-rate later)#Incorrect: If evidence is not available during the audit, the controlcannot be rated as MET initially. There is no provision in CMMC 2.0 to "conditionally" pass a control pending future evidence.
D (Insufficient, but re-rate later)#Incorrect: Once a control is ratedNOT MET, it staysNOT METuntil a re- assessment is conducted in a new audit cycle. The assessordoes not adjust ratings retroactivelybased on future evidence.
Control Reference: CA.L2-3.12.1Assessment Criteria & Justification for the Correct Answer CMMC Assessment Process (CAP) Guide (2023):
"For a control to be rated as MET, the assessed organization must provide sufficient evidence at the time of the assessment."
"If evidence is missing or incomplete, the finding shall be rated as NOT MET." NIST SP 800-171A (Security Requirement Assessment Guide):
"Evidence must be current, relevant, and sufficient to demonstrate compliance with stated periodicity requirements." Since the procedure mandatesquarterly assessments, missing evidence means compliancecannot be validated.
DoD CMMC Scoping Guidance:
"Assessors shall base their determination on the evidence provided at the time of assessment. If required evidence is not available, the control shall be rated as NOT MET." Official CMMC 2.0 References Supporting the Answer Final Conclusion:Thecorrect answer is Bbecause the required evidence (the second-quarter report) is not availableat the time of assessment, making itinsufficientto validate compliance. The Lead Assessormust rate the control as NOT METin accordance with CMMC 2.0 assessment rules.

NEW QUESTION # 225
What type of information is NOT intended for public release and is provided by or generated for the government under a contract to develop or deliver a product or service to the government, but not including information provided by the government to the public (such as on public websites) or simple transactional information, such as necessary to process payments?

- A. CTI
- B. CDI
- C. FCI
- D. CUI

Answer: C

Explanation:
Understanding Federal Contract Information (FCI)Federal Contract Information (FCI) is defined by48 CFR 52.204-21(Basic Safeguarding of Covered Contractor Information Systems). FCI refers to information that:
* Is NOT intended for public release.
* Is provided by or generated for the government under a contract.
* Is necessary to develop or deliver a product or service to the government.
* Excludes publicly available government information(such as information on public websites).
* Excludes simple transactional information(e.g., necessary to process payments).
In the context ofCMMC 2.0, organizations thatprocess, store, or transmit FCImust meetCMMC Level 1 (Foundational), which requires implementing17 basic safeguarding practicesoutlined inFAR 52.204-21.
* A. CDI (Controlled Defense Information)# Incorrect
* This term was used inDFARS 252.204-7012but has been replaced byCUI (Controlled Unclassified Information)in CMMC discussions.
* B. CTI (Cyber Threat Intelligence)# Incorrect
* This refers to intelligence on cyber threats, tactics, and indicators, not contractual data.
* C. CUI (Controlled Unclassified Information)# Incorrect
* CUI is sensitive information requiring additional safeguarding but is a separate category from FCI.
* D. FCI (Federal Contract Information)#Correct
* The definition of FCI explicitly matches the description given in the question.
Why is the Correct Answer FCI (D)?
* FAR 52.204-21 (Basic Safeguarding of Covered Contractor Information Systems)
* Defines FCI and the required safeguards.
* Establishes17 cybersecurity practicesfor FCI protection.
* CMMC 2.0 Framework
* Level 1 (Foundational)is required for contractors handlingFCI.

* Ensures compliance withbasic safeguarding requirementsoutlined inFAR 52.204-21.
* NIST SP 800-171 and DFARS 252.204-7012
* FCI doesnotrequire compliance withNIST SP 800-171, butCUI does.
CMMC 2.0 References Supporting this answer:

NEW QUESTION # 226
.....

The Cyber AB CMMC-CCP exam questions are being updated on a regular basis. As you know the CMMC-CCP exam syllabus is being updated on a regular basis. To add all these changes in the CMMC-CCP exam dumps we have hired a team of exam experts. They regularly update the Cyber AB CMMC-CCP Practice Questions as per the latest Cyber AB CMMC-CCP exam syllabus. So you have the option to get free CMMC-CCP exam questions update for up to 1 year from the date of Cyber AB CMMC-CCP PDF dumps purchase.