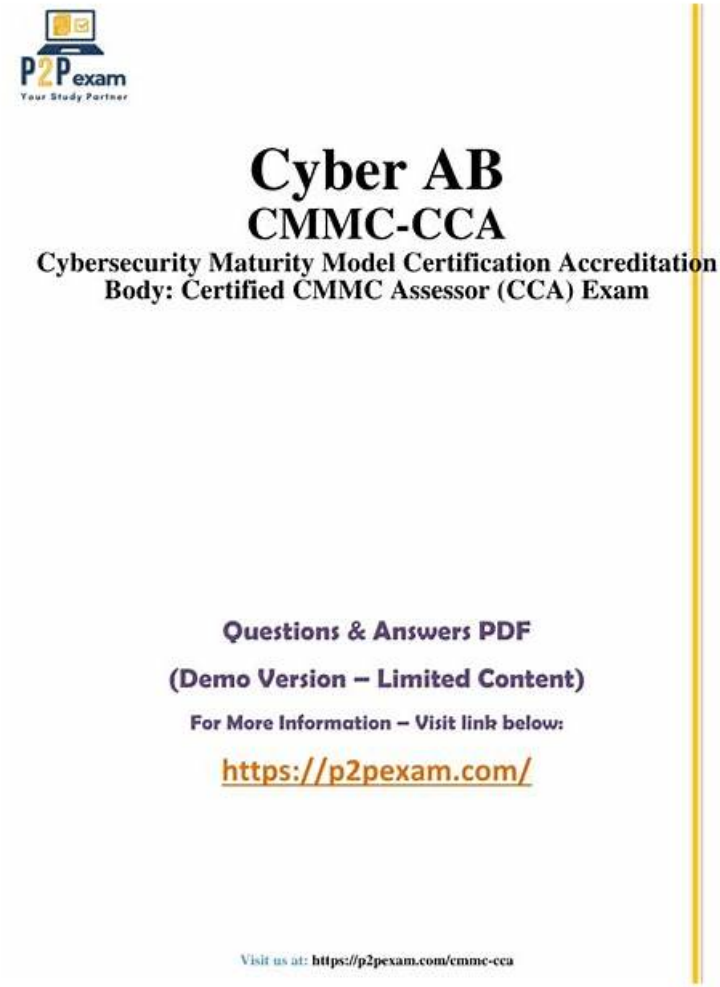
PassExamDumps Cyber AB CMMC-CCA Dumps PDF Preparation Material is Available



What's more, part of that PassExamDumps CMMC-CCA dumps now are free: https://drive.google.com/open?id=1Z5jydRjwMXZmj4qqsBvLw7Ox5AHK0MpC

We offer you free demo for you to have a try before buying for CMMC-CCA learning materials, so that you can have a deeper understanding of what you are doing to buy. We recommend you to have a try before buying. What's more, CMMC-CCA training materials cover most of knowledge points for the exam, and you can master major knowledge points for the exam as well as improve your professional ability in the process of learning. In order to build up your confidence for CMMC-CCA Exam Braindumps, we are pass guarantee and money back guarantee, and if you fail to pass the exam, we will give you refund.

Cyber AB CMMC-CCA Exam Syllabus Topics:

Topic	Details
Topic 1	• Assessing CMMC Level 2 Practices: This section of the exam measures skills of cybersecurity assessors in evaluating whether organizations meet the required practices of CMMC Level 2. It emphasizes applying CMMC model constructs, understanding model levels, domains, and implementation, and using evidence to determine compliance with established cybersecurity practices.
Topic 2	• CMMC Assessment Process (CAP): This section of the exam measures skills of compliance professionals and tests knowledge of the full assessment lifecycle. It covers the steps needed to plan, prepare, conduct, and report on a CMMC Level 2 assessment, including the phases of execution and how to document and follow up on findings in alignment with DoD and CMMC-AB expectations.

Topic 3	• Evaluating Organizations Seeking Certification (OSC) against CMMC Level 2 Requirements: This section of the exam measures skills of cybersecurity assessors and focuses on evaluating the environments of organizations seeking certification at CMMC Level 2. It covers understanding differences between logical and physical settings, recognizing constraints in cloud, hybrid, on-premises, single, and multi-site environments, and knowing what environmental exclusions apply for Level 2 assessments.
Topic 4	• CMMC Level 2 Assessment Scoping: This section of the exam measures skills of cybersecurity assessors and revolves around determining the proper scope of a CMMC assessment. It involves analyzing and categorizing Controlled Unclassified Information (CUI) assets, interpreting the Level 2 scoping guidelines, and making accurate judgments in scenario-based exercises to define what assets and systems fall within assessment boundaries.

100% Pass Cyber AB - CMMC-CCA - Certified CMMC Assessor (CCA) Exam –Reliable Pdf Braindumps

To let the client be familiar with the atmosphere of the CMMC-CCA exam we provide the function to stimulate the exam and the timing function of our study materials to adjust your speed to answer the questions. We provide the stimulation, the instances and the diagrams to explain the hard-to-understand contents of our CMMC-CCA Study Materials. For these great merits we can promise to you that if you buy our CMMC-CCA study materials you will pass the test with few difficulties.

Cyber AB Certified CMMC Assessor (CCA) Exam Sample Questions (Q54-Q59):

NEW QUESTION # 54
The OSC POC has prepared evidence from an internal pre-assessment for the C3PAO in preparation for a third-party assessment. The OSC POC has identified that there are several ESPs (External Service Providers) involved in protecting the security of the infrastructure. While reviewing the pre-assessment documentation regarding ESPs, the Lead Assessor will be looking for items that are:

- A. Marked as NOT APPLICABLE
- B. Noted as partially implemented
- C. Marked as requiring a waiver
- D. Noted as inherited

Answer: D

Explanation:
When External Service Providers are used, the OSC can inherit practices from the ESP if sufficient evidence is provided (such as FedRAMP authorization or equivalent). The Lead Assessor must verify which controls are noted as inherited, as these are assessed differently from controls implemented directly by the OSC.
Exact Extracts:
* CMMC Assessment Guide: "An OSC may inherit practices from External Service Providers when those providers demonstrate equivalent compliance (e.g., FedRAMP Moderate for CUI)."
* "Assessors must review documentation that identifies which practices are inherited, partially implemented, or implemented internally."
* CMMC Scoping Guide: "Inherited controls must be clearly documented by the OSC in the SSP." Why the other options are not correct:
* B: Waivers are not part of CMMC assessments.
* C: "Not Applicable" does not apply to ESP involvement; they either provide inherited practices or not.
* D: "Partially implemented" indicates deficiencies, not proper inheritance.
References:
CMMC Assessment Guide - Level 2, Version 2.13: External Service Providers and inheritance (pp. 10-13).
CMMC Scoping Guide - Level 2: Inherited practices documentation requirements.

NEW QUESTION # 55
A Lead Assessor is conducting an assessment for an OSC. The Lead Assessor is collecting evidence regarding the OSC's network separation techniques. Which technique would be considered a logical separation technique and would fall within the scope of the assessment?

- A. Access limitation based on badge access assigned to employees based on role
- B. Role-based access control within a properly implemented identity and access management tool
- C. A proxy-configured firewall that prevents data from flowing along the physical connection path
- D. Data loss alerting configured at the edge of the network containing CUI assets

Answer: B

Explanation:
Logical separation refers to the use of technical and access control mechanisms (e.g., role-based access, IAM tools, VLANs) to enforce boundaries between different users, roles, or networks. In contrast, physical separation relies on distinct hardware or physical barriers. Role-based access control within an IAM solution is a textbook example of logical separation, and it is specifically called out in the CMMC/NIST context.
Exact extracts:
* "Logical separation may be achieved through the use of virtualization, encryption, or access control mechanisms such as role-based access controls."
* "Assessment Objectives ... Determine if: * separation of users and information types is enforced by physical or logical means."
* "Logical separation is implemented using technical solutions such as access control lists, firewalls configured by policy, or identity and access management solutions." Why the other options are incorrect:
* A (Data loss alerting): This is monitoring, not separation.
* B (Badge access): This is a physical access control, not logical separation.
* D (Proxy-configured firewall): This is boundary protection/traffic control; depending on setup it may be physical or logical, but the scenario points to role-based IAM as the logical example.
References (CCA documents / Study Guide):
* CMMC Assessment Guide - Level 2, SC.L2-3.13.6 "Network Separation."
* NIST SP 800-171 Rev. 2, 3.13.6.

NEW QUESTION # 56
You decide to interview the IT security team to understand if and how a contractor has implemented audit failure alerting. You learn they have deployed AlienVault OSSIM, a feature-rich security information and event management (SIEM) tool. The SIEM tool has been configured to send automatic alerts to system and network administrators if an event affects the audit logging process. Alerts are generated for the defined events that lead to failure in audit logging and can be found in the notification section of the SIEM portal.
However, the alerts are sent to the specified personnel 24 hours after the occurrence of an event. As an assessor evaluating the implementation of AU.L2-3.3.4 - Audit Failure Alerting, which of the following would be a key consideration regarding the evidence provided by the contractor?

- A. Determining if the documented personnel roles for alert notification align with the organization's hierarchy
- B. Verifying that the types of audit logging failures defined cover a comprehensive range of potential scenarios
- C. Ensuring the defined alert notification methods (e.g., email, SMS) are secure and encrypted
- D. Checking if the alert notification process integrates with third-party monitoring services

Answer: B

Explanation:
Comprehensive and Detailed In-Depth Explanation:
AU.L2-3.3.4 requires "alerting personnel when audit logging fails." A 24-hour delay is concerning, but the key consideration is whether defined failure types (B) are comprehensive (e.g., software, hardware, capacity issues), ensuring effective detection. Notification methods (A), roles (C), and third-party integration (D) are secondary to failure coverage, per CMMC guidance.
Extract from Official CMMC Documentation:
* CMMC Assessment Guide Level 2 (v2.0), AU.L2-3.3.4: "Verify defined failure types are comprehensive."
* NIST SP 800-171A, 3.3.4: "Examine failure scenarios covered."
Resources:
* https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level2_MasterV2.0_FINAL_202112016_508.pdf

NEW QUESTION # 57
You are assessing an OSC that develops applications handling Controlled Unclassified Information (CUI). As part of the assessment, you review their vulnerability scanning process. According to their risk assessment policy, the OSC conducts system vulnerability scans every three months. However, they also utilize a centralized, automated vulnerability scanning tool that performs daily scans. Upon discovering any vulnerabilities, the OSC's team applies patches and rescans their systems. Their environment includes backend database servers, web applications with custom Java code, virtual machine hosts running containerized applications, network firewalls, routers, switches, and developer workstations. During the assessment, you find that their scanning solution integrates the latest vulnerability feeds from the National Vulnerability Database (NVD), Open Vulnerability and Assessment Language (OVAL), and vendor sources.
The tool generates reports using Common Vulnerability Scoring System (CVSS) metrics, and even remotely connected developer laptops are included in the scans. However, upon reviewing the vulnerability reports, you observe that the same high/critical vulnerabilities persist month after month without evidence of remediation.Furthermore, there is no record of source code scanning for their custom applications, and virtual machine hosts running the containerized applications are not included in the scans. Which of the following would be an appropriate compensating control or mitigation for the lack of source code scanning?

- A. Implement secure coding standards and practices during application development
- B. Perform periodic penetration testing and code reviews on the custom applications
- C. Increase the frequency of automated vulnerability scans on the production environment
- D. Deploy web application firewalls in front of the custom applications

Answer: B

Explanation:
Comprehensive and Detailed In-Depth Explanation:
CMMC practice RA.L2-3.11.2 - Vulnerability Scans requires organizations to "scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified." The OSC's process includes robust system scanning, but the lack of source code scanning for custom applications is a gap, as vulnerabilities in code can persist into production if not addressed at the development stage. While the practice doesn't explicitly mandate source code scanning, it's a critical component of a comprehensive vulnerability management program, especially for a software development OSC handling CUI.
Among the options,performing periodic penetration testing and code reviews (C)is the most appropriate compensating control for the absence of automated source code scanning. Penetration testing simulates attacks to identify exploitable vulnerabilities in the application, while manual code reviews can uncover issues missed by system scans (e.g., logic flaws, insecure coding practices). This directly addresses the gap by ensuring vulnerabilities in custom code are identified and mitigated, aligning with the intent of RA.L2-3.11.2 to manage vulnerabilities effectively.
* Option A (Web Application Firewalls):WAFs can mitigate some runtime exploits but don't identify or fix underlying code vulnerabilities, making them a partial solution that doesn't fully compensate for the lack of scanning.
* Option B (Increase Scan Frequency):More frequent system scans won't detect code-level issues, as they target deployed systems, not source code.
* Option D (Secure Coding Standards):While proactive and valuable, standards prevent future issues but don't address existing vulnerabilities in current code, lacking the immediate compensatory effect needed.
The CMMC Assessment Guide encourages compensating controls that directly tackle identified gaps, and penetration testing combined with code reviews is a recognized industry practice (e.g., NIST SP 800-53 CA-8, RA-5) for mitigating unaddressed code vulnerabilities.
Extract from Official CMMC Documentation:
* CMMC Assessment Guide Level 2 (v2.0), RA.L2-3.11.2: "Scan for vulnerabilities in systems and applications; remediation or mitigation required for identified issues."
* NIST SP 800-171A, 3.11.2: "Examine scanning processes; compensating controls like penetration testing can address gaps in vulnerability identification."
* Discussion Note: "Organizations may use additional methods (e.g., penetration testing) to identify vulnerabilities not covered by automated scans." Resources:
* https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level2_MasterV2.0_FINAL_202112016_508.pdf

NEW QUESTION # 58
During an assessment, the OSC IT security team provided documentation on how they use replay-resistant authentication to protect CUI. What can be used as a replay-resistant mechanism?

- A. Encrypted messages
- B. Requiring Transport Layer Security (TLS)
- C. Biometric techniques
- D. MFA devices to protect access for local users

Answer: B

Explanation:
* Applicable Requirement: IA.L2-3.5.4 - "Use replay-resistant authentication mechanisms for network access to privileged accounts and for network access to non-privileged accounts."
* Why C is Correct: Transport Layer Security (TLS) is explicitly listed in NIST SP 800-171 Rev. 2 as an acceptable replay-resistant mechanism, as it prevents intercepted credentials from being reused.
Why Other Options Are Insufficient:
* A (Encrypted messages): Provides confidentiality but not inherently replay resistance.
* B (Biometrics): Supports authentication but does not prevent replay of transmitted credentials.
* D (MFA devices): Strong authentication, but not necessarily replay-resistant for transmitted session data.
References (CCA Official Sources):
* NIST SP 800-171 Rev. 2 - IA.L2-3.5.4 (Replay Resistance)
* NIST SP 800-171A - IA.L2-3.5.4 Assessment Objectives

NEW QUESTION # 59
.....

With the rapid market development, there are more and more companies and websites to sell CMMC-CCA guide torrent for learners to help them prepare for CMMC-CCA exam. If you have known before, it is not hard to find that the CMMC-CCA study materials of our company are very popular with candidates, no matter students or businessman. Welcome your purchase for our CMMC-CCA Exam Torrent. As is an old saying goes: Client is god! Service is first! It is our tenet, and our goal we are working at!