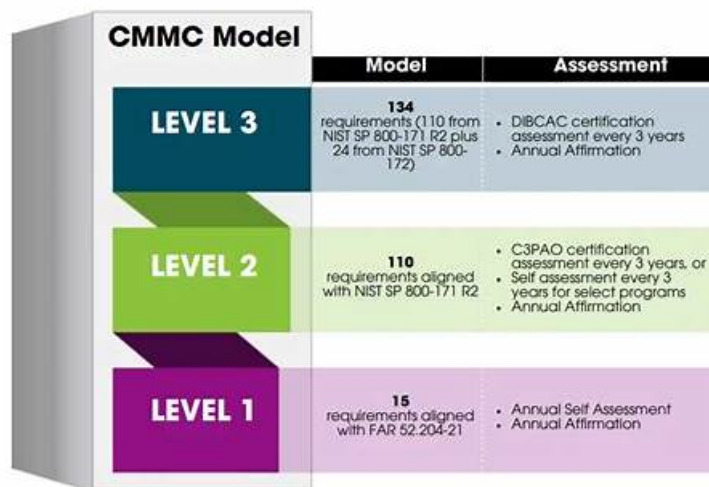


Cyber AB CMMC-CCAテスト問題集 & CMMC-CCA独学書籍



さらに、Topexam CMMC-CCAダンプの一部が現在無料で提供されています: https://drive.google.com/open?id=11bazugeFHuxICQXUOb_DbDovNqilXmKw

TopexamのCMMC-CCA教材を購入したら、あなたは一年間の無料アップデートサービスを取得しました。試験問題集が更新されると、Topexamは直ちにあなたのメールボックスにCMMC-CCA問題集の最新版を送ります。あなたは試験の最新バージョンを提供することを要求することもできます。最新のCMMC-CCA試験問題を知りたい場合、試験に合格したとしてもTopexamは無料で問題集を更新してあげます。

Cyber AB CMMC-CCA 認定試験の出題範囲:

トピック	出題範囲
トピック 1	<ul style="list-style-type: none"> 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.
トピック 2	<ul style="list-style-type: none"> 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.
トピック 3	<ul style="list-style-type: none"> 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.
トピック 4	<ul style="list-style-type: none"> 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.

素晴らしいCMMC-CCAテスト問題集一回合格-更新するCMMC-CCA独学書籍

学習者の学習条件はさまざまであり、多くの場合、CMMC-CCA学習問題を学習するためにインターネットにアクセスできない場合があります。学習者が自宅や会社を離れる場合、インターネットにリンクしてCMMC-CCAテストpdfを学習することはできません。しかし、あなたはオフラインで学ぶことができる私たちのAPPオンライン版を使用しています。初めてオンラインになる環境でCMMC-CCA学習質問を使用する場合のみ、後でオフラインで使用できます。したがって、CMMC-CCA試験の練習教材をどこでも心配する必要がないため、すべての学習者にとって非常に便利です。

Cyber AB Certified CMMC Assessor (CCA) Exam 認定 CMMC-CCA 試験問題 (Q150-Q155):

質問 # 150

An Assessor is evaluating whether an OSC has implemented adequate controls to meet AC.L2-3.1.7:

Privileged Functions. The OSC has procedures that define privileged vs. non-privileged account provisioning and an access control policy that restricts execution of certain functions only to privileged users.

What might the Assessor do to further evaluate the implementation of this practice?

- A. Examine a user access list for users that are authorized to access a key management system.
- B. Test whether a non-privileged user can log into a system where CUI is stored.
- C. Examine system logs to verify automatic updates are being applied.
- D. Test whether the application of a patch is captured in system logging.

正解: A

解説:

AC.L2-3.1.7 (Privileged Functions) requires that execution of privileged functions be restricted to authorized privileged accounts. The best evidence is an access list demonstrating who is allowed privileged access.

Extract:

"Limit the use of privileged functions to authorized users. Assessors should review access control lists or equivalent evidence to verify only privileged accounts have privileged permissions." Thus, the best next step is to examine a user access list for authorized privileged users.

Reference: CMMC Assessment Guide - Level 2, AC.L2-3.1.7.

質問 # 151

You are a CCA on an Assessment Team. During a daily checkpoint meeting, the OSC PoC complains that the assessment process is taking too long and asks if some practices can be skipped to speed things up. How should you respond?

- A. Explain that all practices must be assessed as required by the CMMC Assessment Process and cannot be skipped.
- B. Agree to skip non-critical practices to accommodate the OSC's timeline.
- C. Suggest that the OSC discuss the issue with the Lead Assessor to negotiate a reduced scope.
- D. Recommend that the OSC hire additional staff to expedite evidence collection.

正解: A

解説:

Comprehensive and Detailed in Depth Explanation:

The CAP mandates assessing all practices, making Option A correct. Options B, C, and D violate CAP and CoPC standards.

Extract from Official Document (CAP v1.0):

* Section 2.1 - Evidence Collection (pg. 24): "All practices must be assessed as required by the CMMC Assessment Process."

References:

CMMC Assessment Process (CAP) v1.0, Section 2.1.

質問 # 152

An OSC specializing in developing directed energy systems plans to bid on a DoD contract to produce a

250kW High Energy Laser Weapon System (HELWS). This system is to be deployed on military bases across the globe to protect

U.S. servicemen against aerial threats, including mortars, rockets, and unmanned aerial vehicles (UAVs), as well as swarms of mini-UAVs. Because of the sensitivity of the information, the OSC has prohibited using emails to transmit information regarding the project, whether encrypted or otherwise.

They also have instituted procedures to remove CUI from the email system. What CMMC assessment requirements must the Assessment Team follow regarding the OSC's email system?

- A. The Assessment Team must assess the email system against all CMMC practices.
- B. Since there are measures in place to prevent CUI transfer through email, the email system is out of scope and there is no need to assess it against CMMC practices.
- C. Review the SSP in accordance with CA.L2-3.12.4 - System Security Plan and assess against other CMMC practices.
- **D. Review the SSP in accordance with practice CA.L2-3.12.4 - System Security Plan.**

正解: D

解説:

Comprehensive and Detailed Explanation:

The email system is a Contractor Risk Managed Asset (CRMA), as it can but is not intended to handle CUI due to strict policies. CRMAs are in scope, and the CMMC Assessment Scope - Level 2 requires their review in the SSP per CA.L2-3.12.4 to verify compliance, but not against all practices (Options B, D). Option A is incorrect, as CRMAs are not out of scope. C is correct.

Reference:

CMMC Assessment Scope - Level 2, Section 2.3.2 (CRMAs), p. 5: "CRMAs are reviewed in the SSP per CA.L2-3.12.4."

質問 # 153

Both the SSP and network diagrams presented to the Lead Assessor by the OSC indicate managed service providers (MSPs) within the assessment boundary. In order to BEST understand the impact of the MSPs, what should the Lead Assessor do?

- A. Ascertain what employees the MSP has onsite
- B. Review the inventory to see how the assets have been classified
- C. Inspect the other initial documents presented including policies and organization charts
- **D. Request the customer responsibility matrix related to the MSPs**

正解: D

解説:

The Shared Responsibility Matrix (Customer Responsibility Matrix) is a key artifact in CMMC assessments involving MSPs or cloud service providers. It defines what security responsibilities belong to the OSC and which belong to the service provider. To evaluate the MSP's impact, the assessor must review this matrix to understand boundaries of responsibility for CUI protection.

Exact extracts:

* "When external service providers are included in the assessment boundary, organizations must provide documentation that specifies security responsibilities."

* "A Shared Responsibility Matrix (or Customer Responsibility Matrix) defines which controls are implemented by the OSC versus the external provider."

* "Assessors should request and review this matrix to understand division of responsibilities." Why the other options are incorrect:

* A: Onsite MSP staff presence does not clarify responsibility for security controls.

* C: Reviewing classification helps, but it does not explain responsibility allocation.

* D: Policies/org charts do not establish shared control responsibilities.

References:

CMMC Assessment Guide - Level 2, External Service Providers; OSC documentation requirements.

CMMC Scoping Guide - Managed Service Provider treatment.

質問 # 154

During your assessment of Defcon's (a contractor) implementation of CMMC Level 2 practices, you notice that their system for displaying security and privacy notices is insufficient. The banners currently in use lack detailed information about Controlled Unclassified Information (CUI) handling requirements and associated legal implications. Additionally, the banners are not consistently displayed across all contractor systems and workstations. Moreover, the banners on login pages disappear automatically after less than 5 seconds, providing insufficient time for users to read and acknowledge the content. Which of the following is NOT a feature Defcon's updated privacy and security notices should have?

- 正解: B**

0 FINAL 202112016 508.pdf

• • • • •

- [illegible]

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, wjhsd.instructure.com, bbs.t-firefly.com,
www.ted.com, Disposable vapes

P.S.TopexamがGoogle Driveで共有している無料の2026 Cyber AB CMMC-CCAダンプ: https://drive.google.com/open?id=11bazugeFHuxlCQXUOb_DbDovNqilXmKw