Certified CMMC Assessor (CCA) Exam

Free Practice Test — 30 Real Exam-Style Questions

with full answer key & explanations

Unlock the full bank of 1051 questions
+ unlimited timed mock exams + mistake book

Practice on the web: https://certs.theorypractice.app/cca
$2.99 / week · $6.99 / month · cancel anytime

What you unlock: all 1051 questions • unlimited timed mock exams • mistake book • instant explanations

Study offline on the free app — search your exam on the App Store or Google Play

Practice Questions

Try all 30 first, then check the answer key at the back.

1. You are a CCA working with a client who is preparing for a CMMC assessment. The organization has requested your help in creating an information flow diagram of their document management system to ensure readiness. What would be the first step in constructing this information flow diagram? Module Major Inputs Major Outputs Document Creation Raw text, Templates Digital documents Document Storage Digital documents Archived documents Document Retrieval User requests Accessed documents Document Deletion Deletion requests Removed documents

A. Implement an Information Rights Management (IRM) system to secure documents movement
B. Conduct a security audit of the document management system's infrastructure
C. Perform interviews with employees to gather detailed user requirements
D. Identify how information moves through the document management system, highlighting major inputs and outputs for each module

2. During a CMMC Level 3 assessment, a CCA will evaluate whether the organization meets the requirement to Implement multi-factor authentication (MFA) for all network access to privileged accounts. Which assessment procedure would the CCA most likely use to evaluate this requirement?

A. Observe users logging into the network with privileged accounts
B. Review training documentation on multi-factor authentication practices
C. Examine system logs and configuration files that confirm the use of multiple authentication factors for privileged accounts
D. Interview personnel responsible for managing network access to privileged accounts

3. As a CCA performing a CMMC compliance assessment, you need to verify that an organization's training practices align with cybersecurity policies in practice AC.L2-3.1.2.4. Which type of document would be the most appropriate to examine for this purpose?

A. Staff compliance acknowledgments
B. Training completion records
C. Access logs
D. Policy dissemination records

4. While assessing a financial services company for CMMC compliance, you note that they have an advanced monitoring system logging diverse transaction anomalies and access attempts. However, the company does not have a documented process for regularly reviewing its logging policies. Interviews with their cybersecurity team reveal that they revisit the system occasionally without a predefined schedule or criteria. What is the primary benefit of implementing CMMC guidelines for regular event log review in this context?

A. It ensures all transaction anomalies are reviewed and analyzed thoroughly.
B. It streamlines the process of investigating fraudulent activities.
C. It guarantees the logged events remain relevant and sufficient for detecting threats.
D. It simplifies the configuration of the monitoring system for logging events.

5. You are evaluating a company's compliance with audit logging protection using FIPS-validated encryption to meet Level 2 requirements of the CMMC standards. What documentation cannot be provided as valid evidence of compliance?

A. Specifications of the FIPS-validated encryption mechanisms used, including references.
B. Evidence of FIPS validation, such as validation certificates or references to validated encryption modules.
C. Audit log configuration files demonstrating encryption settings.
D. Network topology diagrams

6. You are evaluating Zentech Corp, a company that operates a cloud services platform handling sensitive data for numerous clients. During your review, you discover that marketing employees were able to access protected client data files. The access logs show unusual activity from multiple accounts in the "Marketing_Team" group accessing data intended only for the "IT_Security" group. Which error likely led to this unauthorized access?

A. Integration with third-party apps without proper vetting
B. Misconfigured role group policies
C. Weak network encryption settings
D. Insufficient employee training on data classification

7. You are tasked to assess a private aerospace company looking to secure CMMC certification for their work related to satellite systems. The company handles sensitive communication technologies and has implemented significant measures to mitigate insider threats. During your assessment, you learn that the company tracks anomalies such as attempts to access restricted communication channels, sudden changes in financial status among personnel, and behavioral shifts indicating potential exploitation vulnerabilities. They conduct quarterly security awareness sessions and use biometric monitoring in high-security zones. Employees with access to highly sensitive channels receive intensive insider threat awareness training. After conducting interviews with the company's CIO, who confirms the full implementation of CMMC practice AT.L2-3.2.3-Insider Threat Awareness, how would you score their program for compliance?

A. +1
B. 0
C. +5
D. Not Met

8. You are conducting a CMMC assessment for a contractor responsible for maintaining a critical supply chain network for the DoD. During the assessment of the Media Protection (MP) domain, you request a review of the contractor's access control documentation, focusing on the management of encryption and decryption keys. The contractor employs a Data Custodian role to manage these keys. However, during interviews, you discover that the Data Analysts and IT Support roles also have access to certain key management functions. When questioned about this practice, the contractor's security team explains that these roles need access for operational continuity and data processing efficiency. Based on this scenario, how would you assess the contractor's compliance with CMMC practice MP.L2-3.8.2-Key Management?

A. Partially Met - While only the Data Custodian role should have access, current roles need better definition.
B. Not Applicable - This practice does not apply to the contractor's operational environment.
C. Not Met - The contractor allows multiple roles access to key management functions, violating the restriction to a limited subset of defined privileged users.
D. Met - The contractor has defined roles for key management as required by CMMC.

9. In the realm of cloud-security, organizations increasingly rely on cloud-based systems for storing and processing sensitive data. To comply with CMMC standards when using these systems, a contractor must ensure that any identifiers used are robust, consistent, and facilitate tracking within the cloud environment. As a CMMC Assessor, you are tasked with evaluating an organization's cloud security practices, specifically concerned with identifier usage for accessing cloud services. What is the primary consideration for a contractor when selecting an identifier for these cloud-based systems?

A. Selecting easily guessable identifiers to facilitate quick user access.
B. Assigning identifiers based on the time of system access to differentiate sessions.
C. Using identifiers that change frequently to keep users engaged.
D. Choosing an identifier that ensures traceability and consistency for all users across the cloud environment.

10. A small healthcare facility recently experienced a series of cybersecurity incidents related to unauthorized data access during system upgrade activities. The organization's IT team has been using unapproved software tools, leading to potential data breaches. As a certified CMMC assessor, you have been asked to provide a recommendation to help them meet CMMC practices, specifically regarding system maintenance control. What action should the facility take to comply with CMMC practice MA.L2-3.7.2?

A. Implement basic antivirus measures but allow IT staff discretion on software and tools used for maintenance.
B. Develop and strictly enforce policies and procedures for reviewing, approving, and monitoring all maintenance activities and the tools used.
C. Outsource the IT department completely to an external managed service provider to handle all upgrades and maintenance activities.
D. Grant unrestricted access to the hospital's IT system for maintenance to all IT staff to ensure quick resolution of incidents.

11. An organization's incident response policy requires all security incidents to be logged within 24 hours of detection. However, a recent audit reveals that incidents are logged on average 48 hours post-detection, and some critical incidents took over 72 hours to be addressed. Based on this information, how would you score the organization's implementation of the IR domain requirement on Logging and Tracking Security Incidents?

A. Not Met (-1 point)
B. Met (+5 points)
C. Met (+1 point)
D. Not Met (-5 points)

12. A financial services firm is preparing for a CMMC assessment, implementing a well-defined Risk Management Framework (RMF) and utilizing continuous monitoring tools. Their policies include comprehensive data classification procedures and regular security awareness training. An independent audit verifies the existence of a regularly updated risk register and a detailed policy on accepting risks. Considering this information, how would you evaluate the firm's compliance with RM.L2-3.11.2-Risk Management practice?

A. Met (+5 points)
B. Not Met (-5 points)
C. Not Met (-1 point)
D. Met (+1 point)

13. In assessing an organization's incident response plan, you evaluate their list of actions upon detecting a security breach. Which of the following actions would you NOT expect to find included in the organization's immediate response protocol?

A. Immediate lockout of affected user accounts
B. Activation of incident response team
C. Pre-approved access for new software installations
D. Escalation of alerts to security team

14. You are performing a cybersecurity assessment for a financial services company. They have quarterly audits of their applications to identify vulnerabilities but do not include source code analysis due to workflow integration challenges. Despite strong external application firewalls and regular security updates, internal reports show unresolved application layer vulnerabilities. Which of the following would be the most appropriate compensating control or mitigation for the absence of source code analysis?

A. Strengthen existing external application firewalls
B. Conduct regular manual code reviews and application penetration testing
C. Activate additional external monitoring with Intrusion Detection Systems (IDS)
D. Increase the frequency of security audits by an external firm

15. A contractor is implementing a cybersecurity strategy to protect sensitive data during transmission over networks to meet CMMC compliance. The contractor has implemented several techniques, including network segmentation, secure communication protocols, and data encryption in transit. To adhere to the requirements of protecting data in transit, which strategy should the contractor NOT consider?

A. Data encryption using secure protocols like TLS or SSL
B. Implementing Virtual Private Networks (VPNs)
C. Utilizing strong authentication mechanisms for network access
D. Encrypting data at rest

16. During a company's CMMC self-assessment, a formal risk management strategy is presented, outlining identified threats and appropriate responses. However, upon interviewing the personnel responsible for executing this strategy, it becomes clear that the actions required to mitigate these threats are either not being taken or improperly implemented. What assessment objective has the company failed to implement from CMMC practice CA.L2.3.15.3-Risk Management Strategy?

A. Develop a formal risk management strategy
B. Conduct regular reviews of the risk management strategy
C. Effectively execute the risk management strategy to mitigate identified threats.
D. Identify the potential threats and risks

17. You are assessing SecureSoft Inc., a company that specializes in security software development. During your audit, you notice that certain employees have accessed a secure customer database without authorization. Upon reviewing access logs, it's evident that these unauthorized attempts weren't flagged nor reviewed by the security team. How should SecureSoft Inc. address this issue to align with AC.L2-3.1.7-Privileged Functions?

A. Implement alerts for unauthorized access attempts and ensure logs are reviewed by the security team.
B. Automatically deny access and notify all users via email.
C. Implement session timeouts after unauthorized access attempts.
D. Restrict database access to business hours only.

18. You are conducting a CMMC Level 3 assessment for a defense contractor. Upon reviewing their subcontracted services, you find that an IT vendor is responsible for key network security functions. What should you verify about this vendor? Vendor Type Vendor Certification Level IT Vendor for Network Security None Bookkeeping Service Level 2 IT Vendor for Web Hosting Level 1

A. Advise the contractor to substitute the IT vendor with another vendor
B. Confirm the IT vendor has a CMMC Level 3 or higher certification
C. Accept the contractor's use of the vendor with any CMMC certification
D. Ask for a self-assessment from the IT vendor

19. An organization is preparing its documentation for a CMMC Level 3 assessment. As an assessor, you need to determine which of the following documents is not a requirement under the CMMC Model for risk-managed assets. Which document should NOT be included?

A. Penetration Test Report
B. Business Impact Analysis
C. Asset inventory
D. Network diagram

20. In a healthcare organization, an IT Security Specialist is responsible for overseeing data encryption processes that secure Protected Health Information (PHI) as it moves between internal databases and external partners. All PHI is stored in a cloud environment and accessed via secure remote applications. What type of asset is the IT Security Specialist?

A. Security Protection Asset (SPA)
B. Healthcare Compliance Asset (HCA)
C. Encryption Managed Asset (EMA)
D. Cloud Technological Asset (CTA)

21. While conducting a remote assessment session, a supplier requests the Lead Assessor to provide evidence of their CMMC training completion before proceeding to exchange sensitive documents for evaluation. What should the Lead Assessor do?

A. Decline to proceed with the assessment until the supplier agrees to waive this requirement.
B. Provide the necessary evidence of CMMC training completion, ensuring confidentiality of the material.
C. Inform the supplier that such evidence is unnecessary, as the Cyber AB credentials suffice.
D. Explain that the requirement of providing CMMC training evidence is against the Cyber AB guidelines.

22. An aerospace manufacturer is undergoing a CMMC Level 3 assessment. As the Lead Assessor, you request access to the manufacturer's Incident Response Plan (IRP) as part of the initial objective evidence for validating the scope. Which of the following is true about the aerospace manufacturer's obligations in honoring the request?

A. The aerospace manufacturer can choose to provide a summary of the IRP, omitting detailed action steps.
B. The aerospace manufacturer is not obligated to provide the IRP until a cybersecurity incident occurs during the assessment.
C. The aerospace manufacturer can refuse to provide the IRP if they consider it sensitive and confidential.
D. The aerospace manufacturer must furnish the Lead Assessor with the IRP.

23. During your CMMC assessment of an organization, you find that they have effectively implemented the marking and labeling of their digital assets, but their documented guidelines do not reflect this practice. What should the organization do in this situation with respect to potential discrepancies in practice documentation?

A. Track it under the Limited Practice Deficiency Correction (LPDC) program and correct it within 5 days.

B. Negotiate with the CCA to ignore the documentation issue and promise to update it in the future.

C. Replace the asset management team immediately to ensure procedures match the current documentation.

D. Track it under the Limited Practice Deficiency Correction (LPDC) program and correct it within 90 days.

24. As a CMMC Assessor conducting an evaluation, you encounter an organization that showcases its adherence to the NIST Cybersecurity Framework (NIST CSF) in its cybersecurity processes. The organization seeks to utilize this certification to expedite its CMMC certification process. How should you, as the assessor, proceed with this request?

A. Inform the organization that NIST CSF cannot be considered as part of the CMMC certification due to different evaluating bodies.

B. Derive a parallel assessment method combining aspects of both NIST CSF and CMMC without further verification.

C. Verify the alignment of the organization's NIST CSF adherence with the specific requirements of the CMMC Assessment Process before considering any acknowledgment.

D. Approve the request, as NIST CSF is closely aligned with many CMMC controls, granting a significant head start.

25. While conducting an assessment, a CCA uncovers a significant cybersecurity vulnerability in a client's internal network that might lead to potential data breaches. The vulnerability falls outside the immediate authority of the CCA to address. What is the appropriate initial course of action for the CCA?

A. Attempt to fix the vulnerability independently and then report to the company

B. Keep a record of the finding and address it in the final assessment report without notifying the client

C. Ignore the issue since it falls outside the scope of the CCA's authority

D. Notify the client's cybersecurity officer or a designated authority for further assessment and resolution

26. As a CCA, you are organizing a seminar for organizations interested in understanding CMMC requirements. You plan to distribute flyers containing the CMMC logo to attract more participants. According to the provisions of the CMMC Code of Professional Conduct (CoPC), how should you proceed?

A. Include the logo without permissions to expedite promotion
B. Modify the logo slightly to avoid needing permission
C. Use the logo only on internal materials where it won't be publicly seen
D. First, seek authorization from Cyber AB to use their intellectual property

27. As a CMMC Assessor, you are evaluating an organization's compliance to the Data Protection standards. During the assessment, you find they conduct Data Protection Impact Assessments (DPIAs) whenever significant changes in data processing activities occur. However, the personnel confirm that there is a documented procedure for conducting DPIAs before implementing such changes. Where should you find this information?

A. In their cybersecurity risk assessment report.
B. In the organization's data audit reports.
C. In their Data Protection Policy.
D. In the organization's incident response plan.

28. As a CCA, during an assessment of an organization's cybersecurity practices, you receive an email containing critical company passwords shared through an unsecured email channel by the organization's security officer. What principle of the CMMC Code of Professional Conduct is violated by this action?

A. Information integrity
B. Confidentiality
C. Availability
D. Proper use of methods

29. A healthcare organization is planning to adopt a new cybersecurity framework. Which of the following factors should NOT be considered when selecting this framework?

A. The framework's compliance with healthcare regulations.
B. The framework's ability to protect patient data privacy.
C. The ease of integration with existing hospital IT systems.
D. The popularity of the framework in the tech industry.

30. A company is preparing for certification by the Cyber AB to meet CMMC standards. Before submitting their application for assessment, they need to conduct an initial evaluation of their cybersecurity policies and processes. Who is primarily responsible for conducting this evaluation?

A. Cyber AB
B. Both the Cyber AB and the Company's Internal Cybersecurity Team jointly.
C. The Company's Internal Cybersecurity Team
D. The CMMC Third-Party Assessment Organization (C3PAO)

Answer Key & Explanations

1. D — Identify how information moves through the document management system, highlighting major inputs and outputs for each module
Answer: Identify how information moves through the document management system, highlighting major inputs and outputs for each module The first step in constructing an information flow diagram for the document management system is to identify and document the major inputs and outputs associated with each module. This foundational step enables the development of a comprehensive diagram that visually represents the information flow within the system, which is essential for CMMC assessment readiness.

2. C — Examine system logs and configuration files that confirm the use of multiple authentication factors for privileged accounts
To evaluate the implementation of MFA, the primary assessment procedure for the CCA is to examine system logs and configuration files that confirm MFA use. While interviewing personnel or observing users may provide context, these methods do not conclusively determine MFA implementation. Examining logs and configuration files ensures the control is actively implemented.

3. A — Staff compliance acknowledgments
The correct answer is Staff compliance acknowledgments. To assess whether training practices are aligned with cybersecurity policies under practice AC.L2-3.1.2.4, the Certified CMMC Assessor would examine staff compliance acknowledgments. These records indicate that employees have read and understood the policies, supporting the alignment between training content and policy requirements. Other options, such as training completion records and policy dissemination records, do not confirm direct acknowledgment and understanding of specific policies.

4. C — It guarantees the logged events remain relevant and sufficient for detecting threats.
Regular review of logged events as per CMMC guidelines ensures that logging policies remain effective for the company's current and emerging threat landscape. Without scheduled reviews, certain relevant event types may be overlooked, thereby weakening the system's ability to detect threats promptly.

5. D — Network topology diagrams
Answer: Network topology diagrams To demonstrate FIPS validation for audit logging encryption, one must cite evidence like specifications of the encryption mechanisms, validation certificates, and encryption settings documentation. Network topology diagrams do not demonstrate adherence to FIPS encryption requirements.

6. B — Misconfigured role group policies
Misconfigured role group policies led to the marketing employees gaining access to data reserved for the IT security team. Such an error indicates improper separation between role permissions, allowing crossover of access rights that violate least privilege principles. Correctly categorizing and assigning permissions is crucial to preventing unauthorized data access.

7. A — +1
The company has effectively implemented the required measures, meeting the CMMC practice standards,

thus a score of +1 is warranted, indicating that the practice is MET.

8. C — Not Met - The contractor allows multiple roles access to key management functions, violating the restriction to a limited subset of defined privileged users.
Answer: Not Met - The contractor grants access to key management functions across various roles, contravening the CMMC requirement to restrict this access to a narrowly defined subset of privileged users. The contractor should limit key management access only to the Data Custodian to comply with CMMC practice MP.L2-3.8.2.

9. D — Choosing an identifier that ensures traceability and consistency for all users across the cloud environment.
The correct choice emphasizes traceability and consistency, which are key in ensuring secure and compliant access to cloud-based systems. The CMMC standards highlight the need for identifiers to be robust and uniform to track, manage, and control access across multiple users in a cloud environment.

10. B — Develop and strictly enforce policies and procedures for reviewing, approving, and monitoring all maintenance activities and the tools used.
The correct action involves establishing and enforcing comprehensive policies and procedures to control and monitor maintenance processes. This helps ensure that all tools and techniques used are approved and do not expose the organization to unnecessary risk, thereby aligning with CMMC practice MA.L2-3.7.2 requirements.

11. A — Not Met (-1 point)
Answer: Not Met (-1 point) The audit reveals that the organization fails to log security incidents within the 24-hour timeframe stipulated by their policy, leading to delays in threat response. This non-compliance indicates that the organization does not meet the CMMC requirements for efficient logging and tracking of security incidents, crucial for timely incident response and mitigation.

12. A — Met (+5 points)
Answer: Met (+5 points) The firm meets the requirements for CMMC RM.L2-3.11.2-Risk Management through its established RMF, continuous monitoring, regular trainings, and updated risk register, indicating a comprehensive risk management process.

13. C — Pre-approved access for new software installations
Answer: Pre-approved access for new software installations Immediate response protocols are designed to contain and mitigate the impact of a security breach. They typically involve actions like alert escalation, affected account lockout, and incident response team activation. Pre-approved access for new software installations is unrelated to immediate threat response and would not typically be part of such protocols.

14. B — Conduct regular manual code reviews and application penetration testing
The lack of source code analysis can be mitigated by conducting regular manual code reviews and application penetration testing. This ensures that vulnerabilities in the application layer are identified and addressed, compensating for the absence of automated code scans. Strengthening external defenses and increasing audit frequency are beneficial but do not directly address code vulnerabilities. Similarly, enhancing external monitoring helps identify attacks but doesn't identify code-level flaws.

15. D — Encrypting data at rest
Answer: Encrypting data at rest While implementing data encryption is crucial, the requirement here is

specifically to protect data during transmission. Encrypting data at rest is concerned with data storage but does not protect data when it's being transmitted. CMMC compliance requires strategies like TLS or SSL for data encryption during transit.

16. C — Effectively execute the risk management strategy to mitigate identified threats.
Answer: Effectively execute the risk management strategy to mitigate identified threats. While the company has identified threats and developed a risk management strategy, the failure lies in the effective execution of this strategy to mitigate the identified threats, as evidenced by the interviews.

17. A — Implement alerts for unauthorized access attempts and ensure logs are reviewed by the security team.
To comply with CMMC standards, SecureSoft Inc. should ensure that unauthorized access attempts generate alerts and logs are comprehensively reviewed by designated security personnel. This aligns with the principle of monitoring and managing privileged functions effectively.

18. B — Confirm the IT vendor has a CMMC Level 3 or higher certification
In CMMC assessments, vendors providing critical services like network security must have a certification level equal to or higher than that sought by the organization. For a Level 3 target, the IT vendor should have CMMC Level 3 or higher.

19. B — Business Impact Analysis
Answer: Business Impact Analysis The Business Impact Analysis is not typically required as part of the documentation for CMMC compliance, whereas asset inventory, network diagram, and penetration test report are required.

20. A — Security Protection Asset (SPA)
The correct answer is Security Protection Asset (SPA). The IT Security Specialist's role in managing the encryption process is a security function aimed at protecting healthcare data. As such, they are considered a Security Protection Asset (SPA).

21. B — Provide the necessary evidence of CMMC training completion, ensuring confidentiality of the material.
Answer: Provide the necessary evidence of CMMC training completion, ensuring confidentiality of the material. In CMMC assessments, transparency and mutual agreements facilitate smooth operations. If a supplier requests proof of relevant certification, accommodating such requests showcases professionalism and trust, vital for working with sensitive information. The Lead Assessor should provide appropriate evidence demonstrating their competencies, respecting any conditions around confidentiality.

22. D — The aerospace manufacturer must furnish the Lead Assessor with the IRP.
Answer: The aerospace manufacturer must furnish the Lead Assessor with the IRP. Organizations seeking CMMC Level 3 compliance must provide initial objective evidence, including an IRP, which helps establish and verify the assessment scope. Providing such documents is crucial for a comprehensive evaluation.

23. A — Track it under the Limited Practice Deficiency Correction (LPDC) program and correct it within 5 days.
Answer: Track it under the Limited Practice Deficiency Correction (LPDC) program and correct it within 5 days. The LPDC program allows for minor documentation updates if the practice evidence shows it has been effectively implemented. Both criteria must be met, and corrections are typically required within 5 business

days from the Final Findings Briefing or by a determined alternative date not exceeding 5 days before the Final Findings Report is submitted to CMMC eMASS.

24. C — Verify the alignment of the organization's NIST CSF adherence with the specific requirements of the CMMC Assessment Process before considering any acknowledgment.
Answer: Verify the alignment of the organization's NIST CSF adherence with the specific requirements of the CMMC Assessment Process before considering any acknowledgment. While NIST CSF is an established framework, it is crucial to evaluate its alignment with specific CMMC requirements to ensure compliance. The assessor must verify the validity and authenticity of the alternative cybersecurity framework against CMMC requirements.

25. D — Notify the client's cybersecurity officer or a designated authority for further assessment and resolution
The CCA should notify the client's cybersecurity officer or a relevant authority who has the proper scope and resources to evaluate and resolve the vulnerability. This ensures that the client's cybersecurity posture is maintained and potential breaches are prevented.

26. D — First, seek authorization from Cyber AB to use their intellectual property
Answer: First, seek authorization from Cyber AB to use their intellectual property It is essential to seek explicit and written permission from Cyber AB before using their logos or trademarks, according to the CMMC Code of Professional Conduct. Failing to do so could violate the intellectual property guidelines set forth by the CMMC.

27. C — In their Data Protection Policy.
Answer: In their Data Protection Policy. An organization's approach to DPIAs must be documented in their Data Protection Policy. Specific processes and procedures for conducting DPIAs are typically detailed within this policy to ensure compliance with data protection standards.

28. B — Confidentiality
The correct answer is Confidentiality. Disseminating sensitive information such as company passwords via an unsecured email channel breaches confidentiality obligations by potentially exposing it to unauthorized access.

29. D — The popularity of the framework in the tech industry.
While the popularity of a cybersecurity framework can be an indicator of widespread use or potential community support, it is not a primary factor that should guide decisions in highly regulated sectors like healthcare. Instead, considerations should focus on compliance with specific healthcare regulations, the framework’s ability to safeguard sensitive patient data, and its compatibility with existing technological infrastructures in the organization.

30. C — The Company's Internal Cybersecurity Team
Answer: The Company's Internal Cybersecurity Team. Before a company applies for the CMMC assessment, it is the responsibility of its internal cybersecurity team to evaluate current cybersecurity policies and processes. They identify and document their strengths and weaknesses in a self-assessment report to ensure thorough preparation for the official assessment.

Ready to pass?

Unlock the full Certified CMMC Assessor (CCA) Exam bank, every explanation, and unlimited timed mock exams.

Scan to start practising
https://certs.theorypractice.app/cca

Also on iOS & Android — search your exam name on the App Store or Google Play