Cyber AB
CMMC-CCA
Certified CMMC Assessor (CCA) Exam

For More Information – Visit link below:

https://www.examsempire.com/

Product Version

1. **Up to Date products, reliable and verified.**
2. **Questions and Answers in PDF Format.**

Latest Version: 9.0

Question: 1

While assessing a company, the CCA is determining whether the company controls and manages connections between its corporate network and all external networks. The company has: (1) a strict employee policy prohibiting personal Internet use and personal email on company computers, and (2) firewalls plus a connection allow-list so only authorized external networks can connect to the company network. Are these safeguards sufficient to meet the applicable CMMC requirement?

A. Yes. The company's strict employee policy is the best practice for meeting the requirement.
B. No. The company must isolate its system from all external connections to meet the requirement.
C. Yes. The company's firewalls and connection allow-lists are appropriate technical controls to meet the requirement.
D. No. The company needs full control over all external systems it interfaces with to meet the requirement.

Answer: C

Explanation:
Applicable CMMC/NIST Requirement: AC.L2-3.1.20 — "Verify and control/limit connections to and use of external systems."
Isolation Not Required (refutes B): The requirement acknowledges that individuals using external systems (e.g., contractors, partners) may need to access organizational systems. In such cases, organizations must ensure those connections do not compromise or harm organizational systems. Therefore, complete isolation from all external systems is not mandated.
Policy Alone is Insufficient (refutes A): Assessment guidance requires mechanisms that technically enforce terms and conditions for use of external systems. A written employee policy by itself does not satisfy the requirement unless paired with technical enforcement (e.g., firewalls, connection rules).
Allow-lists & Firewalls are Best Practice (supports C): Assessment considerations specify that organizations should restrict external systems to an approved list, such as by using firewalls, VPNs, IP restrictions, or certificates. The company's use of firewalls and a connection allow-list directly addresses this requirement.
Full Control of External Systems Not Required (refutes D): The definition of "external systems" clarifies that organizations typically do not have direct supervision or authority over those systems. The requirement is to limit and control connections to such systems, not to own or fully manage them.
Assessment Objectives for AC.L2-3.1.20 (from NIST SP 800-171A):
Connections to external systems are identified.
Use of external systems is identified.
Connections to external systems are verified.
Use of external systems is verified.
Connections to external systems are controlled/limited.

Use of external systems is controlled/limited.
Firewalls and allow-lists satisfy these verification and limitation requirements, enabling a CCA to mark the practice MET if evidence is present.
Reference (CCA Official Sources):
NIST SP 800-171 Rev. 2 — §3.1.20 (Discussion)
NIST SP 800-171A — §3.1.20 (Assessment Objectives & Methods)
CMMC Assessment Guide – Level 2, Version 2.13 — AC.L2-3.1.20 (External Connections [CUI Data], including "Potential Assessment Considerations")

Question: 2

The OSC has assembled its documentation relating to how it controls remote access for assessment. The Lead Assessor compared this documentation to the provided topology map and noted several indications of external connections with External Service Providers (ESPs). Which document is MOST LIKELY to show acceptable evidence of the security controls related to the interface between the OSC and the ESP?

A. OSC's access control policy
B. Interconnection agreement with ESPs
C. Technical design of the security of the available VPN
D. Instructions provided to the OSC from the ESP to implement remote access

Answer: B

Explanation:
Applicable Requirement (CMMC/NIST): Multiple practices may apply (e.g., AC.L2-3.1.14 "Control remote access sessions" and CA.L2-3.12.4 "Develop, document, and periodically update system security plans"). However, when an OSC uses an External Service Provider (ESP), the key control is the documented agreement defining the terms, conditions, and responsibilities between the OSC and the ESP.
Why Interconnection Agreement is Correct (supports B):
According to the CMMC Assessment Guide (Level 2), acceptable evidence for external connections with ESPs includes "interconnection security agreements, memoranda of understanding, or contracts that define the security requirements governing the connection."
These agreements document controls at the interface boundary and ensure both parties understand their responsibilities for protecting CUI.
Why Other Options Are Insufficient:
A . OSC's access control policy — An internal policy outlines organizational expectations, but it does not constitute binding evidence of controls at the boundary with an ESP.
C . Technical design of VPN security — Technical configurations demonstrate how connections are secured, but they do not formally document agreed security requirements between OSC and ESP.
D . Instructions from ESP — ESP-provided setup instructions are not evidence of the OSC's validated control implementation or responsibility-sharing agreement.
Assessment Process Alignment:
The CMMC Assessment Process (CAP) requires assessors to confirm not only technical implementations but also documented agreements that establish accountability for safeguarding

CUI.
Evidence such as interconnection agreements is specifically highlighted as objective evidence that the OSC has verified and controlled external system interfaces.
Reference (CCA Official Sources):
CMMC Assessment Guide – Level 2, Version 2.13 — External Service Providers and Evidence Requirements for External Connections
NIST SP 800-171 Rev. 2 — §3.1.20 and §3.13.6 (discussions on external system connections and interconnection agreements)
NIST SP 800-171A — Assessment Methods for verifying security of external system interfaces

Question: 3

The assessment team has divided responsibilities to review portions of the OSC's scope, including the Host Unit, the specific enclave, and supporting teams such as a Managed Security Service Provider (MSSP). During evidence review, the team notices that MSSP personnel answered interview questions somewhat differently than OSC personnel. To clarify this inconsistency, the Lead Assessor decides to take all the following steps EXCEPT:

A. Review the network diagrams.
B. Review the agreement with the MSSP.
C. Review the notes to determine what was different.
D. Review interview questionnaire consistency.

Answer: D

Explanation:
Applicable Requirement (CMMC Assessment Process): The CMMC Assessment Process (CAP) requires assessors to collect, analyze, and reconcile evidence using triangulation (examine, interview, test) to confirm whether requirements are MET or NOT MET. When inconsistencies arise, the assessor must go back to objective evidence such as diagrams, contracts, and notes.
Why Reviewing Network Diagrams Helps (supports A): Network diagrams provide authoritative evidence of scope, data flows, and system boundaries, which helps clarify whether the MSSP's services were accurately described.
Why Reviewing MSSP Agreements Helps (supports B): Agreements (such as interconnection security agreements or service-level agreements) define shared responsibilities and confirm how the MSSP supports security controls. This evidence is critical to resolving inconsistent testimony.
Why Reviewing Notes Helps (supports C): Notes from previous interviews allow the team to pinpoint where answers diverged. This is a valid method of evidence review and aligns with CAP guidance on documenting interviews.
Why Interview Questionnaire Consistency is NOT the Correct Step (refutes D): The CAP emphasizes resolving inconsistencies through additional evidence, not by adjusting or re-checking the questionnaire itself. The consistency of the questionnaire is irrelevant — what matters is reconciling the evidence provided by both the OSC and MSSP. Thus, this is the action the Lead Assessor would NOT take.
Assessment Guidance Extract (CAP):
"When conflicting evidence is observed, the assessment team must review technical documentation,

agreements, and notes to identify the root cause and determine whether additional clarification is required."
"The interview instrument itself is not a tool for reconciling inconsistencies; rather, objective evidence must be used."
Reference (CCA Official Sources):
CMMC Assessment Process (CAP) v1.0 — Section 3: Conducting the Assessment (Interview, Evidence, Triangulation, and Conflict Resolution)
CMMC Assessment Guide – Level 2, Version 2.13 — Guidance on the role of External Service Providers (MSSPs) and use of documented agreements as evidence
NIST SP 800-171A — General assessment methodology: reconcile evidence using examine, interview, and test methods

Question: 4

During an assessment interview, the interviewee states that anyone can connect to the company Wi-Fi without prior approval. Within which domains is the Wi-Fi configuration covered?

A. Media Protection (MP), Access Control (AC), and Physical Protection (PE)
B. Identification and Authentication (IA), Media Protection (MP), and System and Information Integrity (SI)
C. Access Control (AC), Identification and Authentication (IA), and System and Communications Protection (SC)
D. System and Communications Protection (SC), System and Information Integrity (SI), and Physical Protection (PE)

Answer: C

Explanation:
Access Control (AC): Wi-Fi access must be restricted to authorized users and devices. CMMC Level 2 incorporates NIST SP 800-171 AC requirements to limit and control access to systems and resources.
Identification and Authentication (IA): Wireless access requires authentication to ensure only authorized individuals/devices can connect (e.g., WPA2-Enterprise, certificates, or strong passwords).
System and Communications Protection (SC): Wi-Fi encryption and secure configuration protect datain-transit from interception or unauthorized disclosure.
Why Other Options Are Incorrect:
A (MP, AC, PE): Media protection and physical protection are not primary domains for Wi-Fi configuration.
B (IA, MP, SI): Media protection and system/information integrity do not directly address Wi-Fi security.
D (SC, SI, PE): Physical and integrity controls are not central to wireless access security.
Reference (CCA Official Sources):
CMMC Model v2.0 — Domains AC, IA, SC
NIST SP 800-171 Rev. 2 — AC.L2-3.1.1, IA.L2-3.5.3, SC.L2-3.13.8 (wireless access, identification/authentication, protection of communications)
NIST SP 800-171A — Associated assessment objectives verifying Wi-Fi control and encryption

==========

Question: 5

An assessor is reviewing whether an organization appropriately analyzed the security impact of a new release of an application. Which of the following documents is MOST useful for the assessor to review?

A. A description of the change from the software vendor
B. Change Control Board (CCB) meeting minutes and supporting documents
C. System audit logs showing that the change occurred, when, and by whom
D. A log of security incidents/issues after the change was implemented

Answer: B

Explanation:
Applicable Requirement: CM.L2-3.4.3 — "Track, review, approve/disapprove, and audit changes to organizational systems."
Why CCB Minutes Are Correct (supports B):
Change Control Board (CCB) documentation includes impact analyses, approvals, disapprovals, and justification for system changes.
The CMMC Assessment Guide explicitly identifies CCB minutes and supporting records as primary evidence of compliance with change management practices.
Why Other Options Are Insufficient:
A (Vendor description): Provides information on the update, but does not show organizational review or approval.
C (Audit logs): Show when a change occurred, but not whether it was analyzed and approved beforehand.
D (Incident logs): Reflects results after implementation, but not the review/approval process.
Assessment Guidance Extract (NIST SP 800-171A, CM.L2-3.4.3):
Objectives include verifying that system changes are:
Documented,
Reviewed,
Approved/disapproved, and
Audited.
Evidence such as CCB minutes and approval records directly satisfies these objectives.
Reference (CCA Official Sources):
NIST SP 800-171 Rev. 2 — CM.L2-3.4.3 (Change Management)
NIST SP 800-171A — Assessment Objectives for CM.L2-3.4.3
CMMC Assessment Guide – Level 2, Version 2.13 — Change Management evidence expectations

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/