Question #1 *Topic 1*

During an assessment, which phase of the process identifies conflicts of interest?

A. Analyze requirements.

B. Develop assessment plan.

C. Verify readiness to conduct assessment.

D. Generate final recommended assessment results.

Suggested Answer: *B*

Community vote distribution

C (100%)

578ae95 8 months, 3 weeks ago

Selected Answer: C

The correct answer is:

✅ C. Verify readiness to conduct assessment

Explanation:
The "Verify readiness to conduct assessment" phase is where the CMMC Assessment Team:

Confirms that all preconditions for the assessment are met.
Reviews the assessment scope and boundaries.
Identifies and addresses any conflicts of interest to ensure the integrity and impartiality of the assessment process.
This step is critical to maintaining the credibility and objectivity of the assessment.

Why the other options are incorrect:
A. Analyze requirements – Focuses on understanding the assessment objectives and applicable practices.
B. Develop assessment plan – Involves planning logistics, methods, and timelines, but not specifically conflict of interest checks.
D. Generate final recommended assessment results – Happens after the assessment is complete and does not involve conflict identification.

upvoted 4 times

Question #2 *Topic 1*

Which authority leads the CMMC direction, standards, best practices, and knowledge framework for how to map the controls and processes across different Levels that range from basic cyber hygiene to advanced cyber practices?

A. NIST

B. DoD CIO office

C. Federal CIO office

D. Defense Federal Acquisition Regulation Council

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #3 *Topic 1*

What is objectivity as it applies to activities with the CMMC-AB?

A. Ensuring full disclosure

B. Reporting results of CMMC services completely

C. Avoiding the appearance of, or actual, conflicts of interest

D. Demonstrating integrity in the use of materials as described in policy

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #4 *Topic 1*

What service is the MOST comprehensive that the RPO provides?

A. Training services

B. Education services

C. Consulting services

D. Assessment services

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 1*

The Assessment Team has completed Phase 2 of the Assessment Process. In conducting Phase 3 of the Assessment Process, the Assessment Team is reviewing evidence to address Limited Practice Deficiency Corrections. How should the team score practices in which the evidence shows the deficiencies have been corrected?

A. MET

B. POA&M

C. NOT MET

D. NOT APPLICABLE

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #6 *Topic 1*

A dedicated local printer is used to print out documents with FCI in an organization. This is considered an FCI Asset. Which function BEST describes what the printer does with the FCI?

A. Encrypt

B. Manage

C. Process

D. Distribute

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #7 *Topic 1*

What is the LAST step when developing an assessment plan for an OSC?

A. Verify the readiness to conduct the assessment.

B. Perform certification assessment readiness review.

C. Update the assessment plan and schedule as needed.

D. Obtain and record commitment to the assessment plan.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #8 *Topic 1*

Which domain has a practice requiring an organization to restrict, disable, or prevent the use of nonessential programs?

A. Access Control (AC)

B. Media Protection (MP)

C. Asset Management (AM)

D. Configuration Management (CM)

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #9

Topic 1

In preparation for a CMMC Level 1 Self-Assessment, the IT manager for a DIB organization is documenting asset types in the company's SSP. The manager determines that identified machine controllers and assembly machines should be documented as Specialized Assets. Which type of Specialized Assets has the manager identified and documented?

A. IoT

B. Restricted IS

C. Test equipment

D. Operational technology

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 1*

According to the Configuration Management (CM) domain, which principle is the basis for defining essential system capabilities?

A. Least privilege

B. Essential concern

C. Least functionality

D. Separation of duties

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 1*

What is DFARS clause 252.204-7012 required for?

A. All DoD solicitations and contracts

B. Solicitations and contracts that use FAR part 12 procedures

C. Procurements solely for the acquisition of commercial off-the-shelf

D. Commercial off-the-shelf sold in the marketplace without modifications

Suggested Answer: *A*

Community vote distribution

A (100%)

578ae95 8 months, 3 weeks ago

Selected Answer: A

The correct answer is: A. All DoD solicitations and contracts.

DFARS 252.204-7012, titled "Safeguarding Covered Defense Information and Cyber Incident Reporting," is a mandatory clause for all Department of Defense (DoD) contracts, except for those solely purchasing Commercial Off-The-Shelf (COTS) items. It requires contractors to implement NIST SP 800-171 security requirements to safeguard Covered Defense Information (CDI) and to report cyber incidents involving that data.

Let’s quickly run through the other options:

B: FAR Part 12 procedures cover commercial items, but DFARS 252.204-7012 extends beyond just those procurements.

C & D: COTS procurements are actually exempt from this clause, making those incorrect choices.

upvoted 1 times

Question #12 *Topic 1*

A contractor provides services and data to the DoD. The transactions that occur to handle FCI take place over the contractor’s business network, but the work is performed on contractor-owned systems, which must be configured based on government requirements and are used to support a contract. What type of Specialized Asset are these systems?

A. IoT

B. Restricted IS

C. Test equipment

D. Government property

Suggested Answer: *D*

Community vote distribution

B (100%)

578ae95 8 months, 3 weeks ago

Selected Answer: B

The correct answer is B. Restricted Information Systems (IS).

Here's why: These contractor-owned systems are configured to meet specific government security requirements and are used exclusively for performing work related to a DoD contract that involves handling Federal Contract Information (FCI). Even though the contractor owns them, the systems operate under strict limitations and are considered “restricted” due to their purpose and the sensitivity of the data they process.

Let’s break down the other options:

A. IoT (Internet of Things): Typically refers to networked devices like sensors, thermostats, cameras—not general-purpose systems used for contract work.

C. Test Equipment: This usually means devices used for measurement, diagnostics, or quality assurance—not systems used to handle FCI.

D. Government Property: These systems are contractor-owned, not provided by the government, so this doesn’t apply.

upvoted 4 times

Question #13 *Topic 1*

During a Level 2 Assessment, an OSC provides documentation that attests that they utilize multifactor authentication on nonlocal remote maintenance sessions. The OSC feels that they have met the controls for the Level 2 certification. What additional measures should the OSC perform to fully meet the maintenance requirement?

A. Connections for nonlocal maintenance sessions should be terminated when maintenance is complete.

B. Connections for nonlocal maintenance sessions should be unlimited to ensure maintenance is performed properly.

C. The nonlocal maintenance personnel complain that restrictions slow down their response time and should be removed.

D. The maintenance policy states multifactor authentication must have at least two factors applied for nonlocal maintenance sessions.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 1*

While developing an assessment plan for an OSC, it is discovered that the certified assessor will be interviewing a former college roommate. What is the MOST correct action to take?

A. Do not inform the OSC and the C3PAO of the possible conflict of interest, and continue as planned.

B. Inform the OSC and the C3PAO of the possible conflict of interest, and start the entire process over without the conflicted team member.

C. Inform the OSC and the C3PAO of the possible conflict of interest but since it has been an acceptable amount of time since college, no conflict of interest exists, and continue as planned.

D. Inform the OSC and the C3PAO of the possible conflict of interest, document the conflict and mitigation actions in the assessment plan, and if the mitigation actions are acceptable, continue with the assessment.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #15 *Topic 1*

Which words summarize categories of data disposal described in the NIST SP 800-88 Revision 1, Guidelines for Media Sanitation?

A. Clear, purge, destroy

B. Clear, redact, destroy

C. Clear, overwrite, purge

D. Clear, overwrite, destroy

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #16 *Topic 1*

The evidence needed for each practice and/or process is weight for:

A. adequacy and sufficiency.

B. adequacy and thoroughness.

C. sufficiency and thoroughness.

D. sufficiency and appropriateness.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #17 *Topic 1*

When assessing SI.L1-3.14.2: Provide protection from malicious code at appropriate locations within organizational information systems, evidence shows that all of the OSC's workstations and servers have antivirus software installed for malicious code protection. A centralized console for the antivirus software management is in place and records show that all devices have received the most updated antivirus patterns. What is the BEST determination that the Lead Assessor should reach regarding the evidence?

A. It is sufficient, and the audit finding can be rated as MET.

B. It is insufficient, and the audit finding can be rated NOT MET.

C. It is sufficient, and the Lead Assessor should seek more evidence.

D. It is insufficient, and the Lead Assessor should seek more evidence.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 1*

Which statement BEST describes the key references a Lead Assessor should refer to and use the:

A. DoD adequate security checklist for covered defense information.

B. CMMC Model Overview as it provides assessment methods and objects.

C. safeguarding requirements from FAR Clause 52.204-21 for a Level 2 Assessment.

D. published CMMC Assessment Guide practice descriptions for the desired certification level.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #19 *Topic 1*

As defined in the CMMC-AB Code of Professional Conduct, what term describes any contract between two legal entities?

A. Union

B. Accord

C. Alliance

D. Agreement

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #20 *Topic 1*

During a CMMC readiness review, the OSC proposes that an associated enclave should not be applicable in the scope. Who is responsible for verifying this request?

A. CCP

B. C3PAO

C. Lead Assessor

D. Advisory Board

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #21 *Topic 1*

What is the BEST description of the purpose of FAR clause 52.204-21?

A. It directs all covered contractors to install the cyber security systems listed in that clause.

B. It describes all of the safeguards that contractors must take to secure covered contractor IS.

C. It describes the minimum standard of care that contractors must take to secure covered contractor IS.

D. It directs covered contractors to obtain CMMC Certification at the level equal to the lowest requirement of their contracts.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 1*

Which principles are included in defining the CMMC-AB Code of Professional Conduct?

A. Objectivity, classification, and information accuracy

B. Objectivity, confidentiality, and information integrity

C. Responsibility, classification, and information accuracy

D. Responsibility, confidentiality, and information integrity

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #23

Topic 1

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. sufficient, and rate the audit finding as MET.

B. insufficient, and rate the audit finding as NOT MET.

C. sufficient, and re-rate the audit finding after a quarter two assessment report is examined.

D. insufficient, and re-rate the audit finding after a quarter two assessment report is examined.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #24 *Topic 1*

Which MINIMUM Level of certification must a contractor successfully achieve to receive a contract award requiring the handling of CUI?

A. Level 1

B. Level 2

C. Level 3

D. Any level

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #25 *Topic 1*

CA.L2-3.12.2: Plan of Action defines the clear goal or objective for the plan. What information is generally NOT a part of a plan of action?

A. Completion dates

B. Milestones to measure progress

C. Ownership of who is accountable for ensuring plan performance

D. Budget requirements to implement the plan’s remediation actions

Suggested Answer: *D*

leirbag 1 month, 2 weeks ago

Selected Answer: C

I am thinking C because in the CAP it says

2.4.1.3 Validate OSC POA&M

The Lead Assessor is solely responsible for reviewing and determining the legitimacy and validity of a POA&M at the time of the assessment closeout. A credible and effective POA&M should include, at a minimum, the following:
- The specific security weakness (see 2.1.5 Evidence Gaps) revealed in the Assessment and tied to specific practice;
- The severity of each weakness;
- The scope of each weakness with the assessed environment;
- The proposed mitigation approaches;
- The estimated costs for remediation;
- Documented records of mitigation status and delays; and
- A risk Assessment of the deficiency

upvoted 1 times

Question #26 *Topic 1*

Which code or clause requires that a contractor is meeting the basic safeguarding requirements for FCI during a Level 1 Self-Assessment?

A. FAR 52.204-21

B. 22 CFR 120-130

C. DFARS 252.204-7011

D. DFARS 252.204-7021

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #27 *Topic 1*

How does the CMMC define a practice?

A. A business transaction

B. A condition arrived at by experience or exercise

C. A series of changes taking place in a defined manner

D. An activity or activities performed to meet defined CMMC objectives

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #28 *Topic 1*

The Lead Assessor interviews a network security specialist of an OSC. The incident monitoring report for the month shows that no security incidents were reported from OSC's external SOC service provider. This is provided as evidence for RA.L2-3.11.2: Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. Based on this information, the Lead Assessor should conclude that the evidence is:

A. inadequate because it is irrelevant to the practice.

B. adequate because it fits well for expected artifacts.

C. adequate because no security incidents were reported.

D. inadequate because the OSC's service provider should be interviewed.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #29 *Topic 1*

While determining the scope for a company's CMMC Level 1 Self-Assessment, the contract administrator includes the hosting providers that manage their IT infrastructure. Which asset type BEST describes the third-party organization?

A. ESPs

B. People

C. Facilities

D. Technology

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #30 *Topic 1*

When are contractors required to achieve a CMMC certificate at the Level specified in the solicitation?

A. At the time of award

B. Upon solicitation submission

C. Thirty days from the award date

D. Before the due date of submission

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #31 *Topic 1*

Which example represents a Specialized Asset?

A. SOCs

B. Hosted VPN services

C. Consultants who provide cybersecurity services

D. All property owned or leased by the government

Suggested Answer: *D*

Community vote distribution

A (100%)

⊟ **fifunmitimothy** 4 days, 11 hours ago

Selected Answer: D

Because Specialized Assets include categories such as:
Government Property
Operational Technology (OT)
Internet of Things (IoT)
Industrial Control Systems (ICS)
Test equipment
Restricted Information Systems

upvoted 1 times

⊟ **578ae95** 8 months, 3 weeks ago

Selected Answer: A

The correct answer is: A. SOCs

Explanation: A Specialized Asset refers to a unique or specific resource that plays a critical role in an organization's operations or security infrastructure. Security Operations Centers (SOCs) are considered specialized assets because they are dedicated facilities or teams focused on monitoring, detecting, and responding to cybersecurity threats. They are integral to an organization's security posture and are not general-purpose assets.

Let's analyze the other options:

B. Hosted VPN services: While important, hosted VPN services are not considered specialized assets as they are typically general-purpose tools used for secure remote access.

C. Consultants who provide cybersecurity services: Consultants are external resources, not assets owned or controlled by the organization.

D. All property owned or leased by the government: This is too broad and does not align with the definition of a specialized asset.

upvoted 2 times

Question #32 *Topic 1*

When assessing an OSC for CMMC, the Lead Assessor should use the information from the Discussion and Further Discussion sections in each practice because it:

A. is normative for an OSC to follow.

B. contains examples that an OSC must implement.

C. is mandatory and aligns with FAR Clause 52.204-21.

D. provides additional information to facilitate the assessment of the practice.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #33 *Topic 1*

An OSC has requested a C3PAO to conduct a Level 2 Assessment. The C3PAO has agreed, and the two organizations have collaborated to develop the Assessment Plan. Who agrees to and signs off on the Assessment Plan?

A. OSC and Sponsor

B. OSC and CMMC-AB

C. Lead Assessor and C3PAO

D. C3PAO and Assessment Official

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #34 *Topic 1*

Which regulation allows for whistleblowers to sue on behalf of the federal government?

A. NIST SP 800-53

B. NIST SP 800-171

C. False Claims Act

D. Code of Professional Conduct

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #35 *Topic 1*

Within how many days from the Assessment Final Recommended Findings Brief should the Lead Assessor and Assessment Team Members, if necessary, review the accuracy and validity of the OSC’s updated POA&M with any accompanying evidence or scheduled collections?

A. 90 days

B. 180 days

C. 270 days

D. 360 days

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #36 *Topic 1*

Ethics is a shared responsibility between:

A. DoD and CMMC-AB.

B. OSC and sponsors.

C. CMMC-AB and members of the CMMC Ecosystem.

D. members of the CMMC Ecosystem and Lead Assessors.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #37 *Topic 1*

Which phase of the CMMC Assessment Process includes developing the assessment plan?

A. Phase 1

B. Phase 2

C. Phase 3

D. Phase 4

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #38 *Topic 1*

During Phase 4 of the Assessment process, what MUST the Lead Assessor determine and recommend to the C3PAO concerning the OSC?

A. Ability

B. Eligibility

C. Capability

D. Suitability

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #39 *Topic 1*

The CMMC Level 2 assessment methods include examination and can include:

A. documents, mechanisms, or activities.

B. specific hardware, software, or firmware safeguards employed within a system.

C. policies, procedures, security plans, penetration tests, and security requirements.

D. observation of system backup operations, exercising a contingency plan, and monitoring network traffic.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #40 *Topic 1*

Who is responsible for ensuring that subcontractors have a valid CMMC Certification?

A. CMMC-AB

B. OUSD A&S

C. DoD agency or client

D. Contractor organization

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #41 *Topic 1*

When are data and documents with legacy markings from or for the DoD required to be re-marked or redacted?

A. When under the control of the DoD

B. When the document is considered secret

C. When a document is being shared outside of the organization

D. When a derivative document's original information is not CUI

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #42 *Topic 1*

An Assessment Team is reviewing a practice that is documented and being checked monthly. When reviewing the logs, the practice is only being completed quarterly. During the interviews, the team members say they perform the practice monthly but only document quarterly. Is this sufficient to pass the practice?

A. No, the work is not being done as stated.

B. Yes, the practice is being done as documented.

C. No, all three assessment methods must be met to pass.

D. Yes, the interview process is enough to pass a practice.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #43 *Topic 1*

Which phase of the CMMC Assessment Process includes the task to identify, obtain inventory, and verify evidence?

A. Phase 1: Plan and Prepare Assessment

B. Phase 2: Conduct Assessment

C. Phase 3: Report Recommended Assessment Results

D. Phase 4: Remediation of Outstanding Assessment Issues

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #44 *Topic 1*

What is the MOST common purpose of assessment procedures?

A. Obtain evidence.

B. Define level of effort.

C. Determine information flow.

D. Determine value of hardware and software.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #45 *Topic 1*

What are CUI protection responsibilities?

A. Shielding

B. Governing

C. Correcting

D. Safeguarding

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #46

Topic 1

An Assessment Team is conducting a Level 2 Assessment at the request of an OSC. The team has begun to score practices based on the evidence provided. At a MINIMUM, what is required of the Assessment Team to determine if a practice is scored as MET?

A. All three types of evidence are documented for every control.

B. Examine and accept evidence from one of the three evidence types.

C. Complete one of the following: examine two artifacts, either observe a satisfactory demonstration of one control or receive one affirmation from the OSC personnel.

D. Complete two of the following: examine one artifact, either observe a satisfactory demonstration of one control or receive one affirmation from the OSC personnel.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #47

Topic 1

When assessing SI.L2-3.14.6: Monitor communications for attack, the CCA interviews the person responsible for the intrusion detection system and examines relevant policies and procedures for monitoring organizational systems. What would be a possible next step the CCA could conduct to gather sufficient evidence?

A. Conduct a penetration test.

B. Interview the intrusion detection system’s supplier.

C. Upload known malicious code and observe the system response.

D. Review an artifact to check key references for the configuration of the IDS or IPS practice for additional guidance on intrusion detection and prevention systems.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #48 *Topic 1*

An OSC needs to be assessed on RA.L2-3.11.1: Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. What is in scope for a Level 2 assessment of RA.L2-3.11.1?

A. IT systems

B. Enterprise systems

C. CUI Marking processes

D. Processes, people, physical entities, and IT systems in which CUI processed, stored, or transmitted

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #49 *Topic 1*

Which term describes the process of granting or denying specific requests to obtain and use information, related information processing services, and enter specific physical facilities?

A. Access control

B. Physical access control

C. Mandatory access control

D. Discretionary access control

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #50 *Topic 1*

A client uses an external cloud-based service to store, process, or transmit data that is reasonably believed to qualify as CUI. According to DFARS clause 252.204-7012, what set of established security requirements MUST that cloud provider meet?

A. FedRAMP Low

B. FedRAMP Moderate

C. FedRAMP High

D. FedRAMP Secure

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #51 *Topic 1*

A CCP is working as an Assessment Team Member on a CMMC Level 2 Assessment. The Lead Assessor has assigned the CCP to assess the OSC's Configuration Management (CM) domain. The CCP's first interview is with a subject-matter expert for user-installed software. With respect to user-installed software, what facet should the CCP's interview focus on?

A. Controlled and monitored

B. Removed from the system

C. Scanned for malicious code

D. Limited to mission-essential use only

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #52 *Topic 1*

During the planning phase of a CMMC Level 2 Assessment, the Lead Assessor is considering what would constitute the right evidence for each practice. What is the Assessor attempting to verify?

A. Adequacy

B. Sufficiency

C. Process mapping

D. Assessment scope

Suggested Answer: *B*

fifunmitimothy 4 days, 7 hours ago

Selected Answer: A

Adequacy = Is the evidence appropriate and relevant to the practice?

Sufficiency = Is there enough evidence to support a conclusion?

Since the question focuses on what would constitute the right evidence (not the amount of evidence), the assessor is verifying adequacy.

upvoted 1 times

Question #53 Topic 1

Within the CMMC Ecosystem, which organization ultimately will manage and oversee the training, testing, authorization, and certification of candidate assessors and instructors?

A. DoD OUSD

B. DIB Collaborative Information Sharing Environment

C. Committee on National Security Systems Instructions

D. CMMC Assessors and Instructors Certification Organization

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #54 *Topic 1*

Which statement BEST describes an assessor's evidence gathering activities?

A. Use interviews for assessing a Level 2 practice.

B. Test all practices or objectives for a Level 2 practice.

C. Test certain assessment objectives to determine findings.

D. Use examinations, interviews, and tests to gather sufficient evidence.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #55 *Topic 1*

A C3PAO Assessment Plan document captures the names of the interviewees, the facilities that will utilized, along with estimated costs and schedule of the assessment. What part of the assessment plan is this?

A. Identify resources and schedule.

B. Select Assessment Team members.

C. Identify and manage assessment risks.

D. Select and develop the evidence collection approach.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #56 *Topic 1*

A CCP is on their first assessment for CMMC Level 2 with an Assessment Team and is reviewing the CMMC Assessment Process to understand their responsibilities. Which method gathers information from the subject matter experts to facilitate understanding and achieve clarification?

A. Test

B. Examine

C. Interview

D. Assessment

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #57 *Topic 1*

What is a PRIMARY activity that is performed while conducting an assessment?

A. Develop assessment plan.

B. Collect and examine evidence.

C. Verify readiness to conduct assessment.

D. Deliver recommended assessment results.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #58 Topic 1

CMMC scoping covers the CUI environment encompassing the systems, applications, and services that focus on where CUI is:

A. received and transferred.

B. stored, processed, and transmitted.

C. entered, edited, manipulated, printed, and viewed.

D. located on electronic media, on system component memory, and on paper.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #59 *Topic 1*

An assessor is collecting affirmations. So far, the assessor has collected interviews, demonstrations, emails, messaging, and presentations. Are these appropriate approaches to collecting affirmations?

A. No, emails are not appropriate affirmations.

B. No, messaging is not an appropriate affirmation.

C. Yes, the affirmations collected by the assessor are all appropriate.

D. Yes, the affirmations collected by the assessor are all appropriate, as are screenshots.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #60 *Topic 1*

Prior to conducting a CMMC Assessment, the contractor must specify the CMMC Assessment scope by categorizing all assets. Which two asset categories are always assessed against CMMC practices?

A. CUI Assets and Specialized Assets

B. Security Protection Assets and CUI Assets

C. Specialized Assets and Contractor Risk Managed Assets

D. Security Protection Assets and Contractor Risk Managed Assets

Suggested Answer: *A*

Community vote distribution

B (100%)

fifunmitimothy 4 days, 7 hours ago

Selected Answer: B

Level 2 scoping highlight CUI Assets and SPA

upvoted 1 times

DSPKills 2 months, 2 weeks ago

Selected Answer: B

According to the level 2 scoping table CUI Assets and Security Protection Assets are the only two that are assessed against all level 2 controls.

upvoted 1 times

Question #61

Topic 1

While conducting a CMMC Assessment, a Lead Assessor is given documentation attesting to Level 1 identification and authentication practices by the OSC. The Lead Assessor asks the CCP to review the documentation to determine if identification and authentication controls are met. Which documentation BEST satisfies the requirements of IA.L1-3.5.1: Identify system users, processes acting on behalf of users, and devices?

A. Procedures for implementing access control lists

B. List of unauthorized users that identifies their identities and roles

C. User names associated with system accounts assigned to those individuals

D. Physical access policy that states, “All non-employees must wear a special visitor pass or be escorted.”

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #62 *Topic 1*

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. CDI

B. CTI

C. CUI

D. FCI

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #63 *Topic 1*

Which document BEST determines the existence of FCI and/or CUI in scoping an assessment with an OSC?

A. OSC SSP

B. OSC POA&M

C. OSC Evidence

D. OSC Contract with DoD

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #64 *Topic 1*

Which term describes the prevention of damage to, protection of, and restoration of computers and electronic communications systems/services, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation?

A. Cybersecurity

B. Data security

C. Network security

D. Information security

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #65 *Topic 1*

Which organization is the governmental authority responsible for identifying and marking CUI?

A. NARA

B. NIST

C. CMMC-AB

D. Department of Homeland Security

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #66 *Topic 1*

On a Level 2 Assessment Team, what are the roles of the CCP and the CCA?

A. The CCP leads the Level 2 Assessment Team, which consists of one or more CCAs.

B. The CCA leads the Level 2 Assessment Team, which can include a CCP with US Citizenship.

C. The CCA leads the Level 2 Assessment Team, which can include a CCP regardless of citizenship.

D. The CCP leads the Level 2 Assessment Team, which can include a CCA, regardless of citizenship.

Suggested Answer: *B*

Community vote distribution

B (100%)

88cfdd0 3 months ago

Selected Answer: B

IN order for a CCP to be active on an assessment, they must be a U.S. citizen.

upvoted 1 times

578ae95 8 months, 3 weeks ago

Selected Answer: B

The correct answer is:

B. The CCA leads the Level 2 Assessment Team, which can include a CCP with US Citizenship.

Here's why:
According to the CMMC Assessment Process (CAP) v5.6.1, the Certified CMMC Assessor (CCA) is designated as the Lead Assessor for a Level 2 assessment. The Lead Assessor is responsible for:

Overseeing and managing the assessment team
Making final determinations on practice scores
Ensuring the assessment is conducted in accordance with CMMC procedures
The Certified CMMC Professional (CCP) may participate on the assessment team but cannot lead a Level 2 assessment. Additionally, U.S. citizenship is a requirement for participation in Level 2 assessments due to the handling of Controlled Unclassified Information (CUI).

upvoted 2 times

Shacla6457 8 months, 3 weeks ago

Selected Answer: B

Ccp can't lead an assessment

upvoted 4 times

Question #67 *Topic 1*

A CCP is part of a CMMC Assessment Team interviewing a subject-matter expert on Access Control (AC) within an OSC. During the interview process, what will the CCP ensure about the information exchanged during the interview?

A. Performed in groups for more efficient use of resources

B. Recorded for inclusion in the Final Recommended Findings report

C. Confidential and non-attributable so interviewees can speak without fear of reprisal

D. Mapped to specific CMMC practices to clearly delineate which practice is being evaluated

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #68 *Topic 1*

The facilities manager for a company has procured a Wi-Fi enabled, mobile application-controlled thermostat for the server room, citing concerns over the inability to remotely gauge and control the temperature of the room. Because the thermostat is connected to the company's FCI network, should it be assessed as part of the CMMC Level 1 Self-Assessment Scope?

A. No, because it is OT

B. No, because it is an IoT device

C. Yes, because it is a restricted IS

D. Yes, because it is government property

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #69 *Topic 1*

A company is about to conduct a press release. According to AC.L1-3.1.22: Control information posted or processed on publicly accessible systems, what is the MOST important factor to consider when addressing CMMC requirements?

A. That the information is correct

B. That the CEO approved the message

C. That the company has to safeguard the release of FCI

D. That so long as the information is only FCI, it can be released

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #70 *Topic 1*

In performing scoping, what should the assessor ensure that the scope of the assessment covers?

A. All assets documented in the business plan

B. All assets regardless if they do or do not process, store, or transmit FCI/CUI

C. All entities, regardless of the line of business, associated with the organization

D. All assets processing, storing, or transmitting FCI/CUI and security protection assets

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #71 *Topic 1*

Where can a listing of all federal agencies' CUI indices and categories be found?

A. 32 CFR Section 2002

B. Official CUI Registry

C. Executive Order 13556

D. Official CMMC Registry

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #72 *Topic 1*

What is the primary intent of the verify evidence and record gaps activity?

A. Map test and demonstration responses to CMMC practices.

B. Conduct interviews to test process implementation knowledge.

C. Determine the one-to-one relationship between a practice and an assessment object.

D. Identify and describe differences between what the Assessment Team required and the evidence collected.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #73 *Topic 1*

How are the Final Recommended Assessment Findings BEST presented?

A. Using the CMMC Findings Brief template

B. Using a C3PAO-provided template that is preferred by the OSC

C. Using a C3PAO-branded version of the CMMC Findings Brief template

D. Using the proprietary template created by the Lead Assessor after approval from the C3PAO

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #74 *Topic 1*

A Level 2 Assessment was conducted for an OSC, and the results are ready to be submitted. Prior to uploading the assessment results, what step MUST the C3PAO complete?

A. Pay an assessment submission fee.

B. Complete an internal review of the results.

C. Notify the CMMC-AB that submission is forthcoming.

D. Coordinate a final briefing between the Lead Assessor and the OSC.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #75 *Topic 1*

Which term describes “the protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information”?

A. Adopted security

B. Adaptive security

C. Adequate security

D. Advanced security

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #76 *Topic 1*

A Level 2 Assessment of an OSC is winding down and the final results are being prepared to present to the OSC. When should the final results be delivered to the OSC?

A. At the end of every day of the assessment

B. Daily and during a final separately scheduled review

C. Either at the final Daily Checkpoint, or during a separately scheduled findings and recommendation review

D. Either after approval from the C3PAO, or during a separately scheduled final recommended findings review

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #77 *Topic 1*

Which document is the BEST source for determining the sources of evidence for a given practice?

A. NIST SP 800-53

B. NIST SP 800-53A

C. CMMC Assessment Scope

D. CMMC Assessment Guide

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #78 *Topic 1*

Who will verify the adequacy and sufficiency of evidence to determine whether the practices and related components for each in-scope Host Unit, Supporting Organization/Unit, or enclave has been met?

A. OSC

B. Assessment Team

C. Authorizing official

D. Assessment official

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #79 *Topic 1*

A Lead Assessor is performing a CMMC readiness review. The Lead Assessor has already recorded the assessment risk status and the overall assessment feasibility. At MINIMUM, what remaining readiness review criteria should be verified?

A. Determine the practice pass/fail results.

B. Determine the preliminary recommended findings.

C. Determine the initial model practice ratings and record them.

D. Determine the logistics, Assessment Team, and the evidence readiness.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #80 *Topic 1*

As part of CMMC 2.0, the change to Level 1 Self-Assessments supports “reduced assessment costs” allows all companies at Level 1 (Foundational) to:

A. conduct self-assessments.

B. opt out of CMMC Assessments.

C. have assessment costs reimbursed by the DoD.

D. pay no more than $500.00 for their annual assessment.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #81 *Topic 1*

At which CMMC Level do the Security Assessment (CA) practices begin?

A. Level 1

B. Level 2

C. Level 3

D. Level 4

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #82 *Topic 1*

A machining company has been awarded a contract with the DoD to build specialized parts. Testing of the parts will be done by the company using in-house staff and equipment. For a Level 1 Self-Assessment, what type of asset is this?

A. CUI Asset

B. In-scope Asset

C. Specialized Asset

D. Contractor Risk Managed Asset

Suggested Answer: *C*

Community vote distribution

B (50%) D (50%)

88cfdd0 3 months ago

Selected Answer: D

What information is being processed, stored, or transmitted by the machining process? How can this be an in-scope asset?

upvoted 1 times

578ae95 8 months, 3 weeks ago

Selected Answer: B

The correct answer is: B. In-scope Asset

Here's why:
For a CMMC Level 1 Self-Assessment, the focus is on protecting Federal Contract Information (FCI), not Controlled Unclassified Information (CUI). The types of assets considered during a Level 1 assessment are those that:

Process, store, or transmit FCI
Are used to support the contract (e.g., systems, equipment, personnel)
In this scenario:

The machining company is performing in-house testing using its own staff and equipment.
These assets are directly involved in fulfilling the DoD contract.
Therefore, they are considered in-scope assets for the assessment, as they are part of the environment that supports the contract and may handle FCI.

upvoted 1 times

Question #83 *Topic 1*

Two network administrators are working together to determine a network configuration in preparation for CMMC. The administrators find that they disagree on a couple of small items. Which solution is the BEST way to ensure compliance with CMMC?

A. Consult with the CEO of the company.

B. Consult the CMMC Assessment Guides and NIST SP 800-171.

C. Go with the network administrator’s ideas with the least stringent controls.

D. Go with the network administrator’s ideas with the most stringent controls.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #84 *Topic 1*

Which statement BEST describes an LTP?

A. Creates DoD-licensed training

B. Instructs a curriculum approved by CMMC-AB

C. May market itself as a CMMC-AB Licensed Provider for testing

D. Delivers training using some CMMC body of knowledge objectives

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #85 *Topic 1*

Prior to initiating an OSC's CMMC Assessment, the Lead Assessor briefed the team on the most important requirements of the assessment. The assessor also insisted that the same results of the findings summary, practice ratings, and Level recommendations must be submitted to the C3PAO for initial processes and review. After several weeks of assessment, the C3PAO completes the internal review, the recommended results are then submitted through the C3PAO for final quality review and rating approval. Which document stipulates these reporting requirements?

A. CMMC Assessment reporting requirements

B. DFARS 52.204-21 assessment reporting requirements

C. NIST SP 800-171 Revision 2 assessment reporting requirements

D. DFARS clause 252.204-7012 assessment reporting requirements

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!