Cyber AB CCP - Quiz Questions with Answers

1. CMMC Ecosystem

1.

If a prime contractor engages the services of a subcontractor to deliver on the contract, whose responsibility is it to ensure contract adherence and flow down of requirements?

The prime contractor

The Department of Defense

Both the prime contractor and subcontractor equally

The subcontractor

DFARS clause 252.204-7012 flows down to subcontractors without alteration, except to identify the parties, when performance will involve operationally critical support or covered defense information. Per 252.204-7012(m)(1), the prime contractor shall determine if the information required for subcontractor performance retains its identity as covered defense information, thus necessitating flow-down of the clause. The contractor should consult with the contracting office if clarification is required. The Department's emphasis is on the deliberate management of information requiring protection. Prime contractors should minimize the flow-down of information requiring protection. Flow down is a requirement of the terms of the contract with the Government, which should be enforced by the prime contractor because of compliance with these terms. If a subcontractor does not agree to comply with the terms of DFARS Clause 252.204–7012, then covered defense information shall not be on that subcontractor's information system.

2.

Jane has one year of experience and an associate's degree in cybersecurity. She is interested in eventually becoming a Certified CMMC Assessor (CCA) but wants to start with the Certified CMMC Professional (CCP). What are Jane's options for gaining the experience required for the CCP?

Continue building her work experience and consider additional certifications.

Complete the CCP certification without additional work experience, as the associate's degree in cybersecurity may fulfill the requirements.

Wait until she has the required five years of experience before considering the CCP certification

Focus solely on obtaining the Certified CMMC Assessor (CCA) certification without pursuing the CCP

Jane should continue building her work experience, pursue relevant roles as a cybersecurity assessor, engage in professional development, and consider additional certifications, until she has more years of experience to pursue the CCP and then the CCA certification.

3.

How does CMMC differ from cybersecurity guidelines within FISMA (Federal Information Security Modernization Act)?

Companies cannot certify compliance themselves

CMMC emphasizes self-certification for compliance.

FISMA mandates third-party assessments for compliance.

CMMC and FISMA have no significant differences.

CMMC builds on cybersecurity guidelines within FISMA but with one major difference: companies cannot certify compliance on their own. Instead, companies that need CMMC accreditation must be assessed by a third-party assessor known as a C3PAO - CMMC Third Party Assessment Organization

4.

To become a CMMC Third Party Assessment Organization an organization must be which one of the following to qualify?

It must be 100% U.S. Citizen owned

It must be a registered business located in any of the (North Atlantic Treaty Organization) NATO countries.

There are no specific requirements for C3PAOs. Any organization can become a C3PAO

It must have been in business for a minimum of five years

For an entity to be approved to act as a C3PAO, it must be 100% U.S. Citizen owned and successfully pass a Foreign Ownership, Control or Influence (FOCI) and SF-328 review to be eligible. No foreign owned businesses are currently admitted

5.

Which of the following institutions was involved in the development of the Cybersecurity Maturity Model Certification (CMMC)?

Carnegie Mellon University

Harvard University

Massachusetts Institute of Technology (MIT)

University of California, Berkeley

The Office of the Under Secretary of Defense, Acquisition & Sustainment (OUSD) (A&S)) engaged the researchers at the Carnegie Mellon University Software Engineering Institute (SEI) and The Johns Hopkins Applied Physics Laboratory (APL) to develop the CMMC to prevent loss of Intellectual Property and Controlled Unclassified Information (CUI), and bolster the Defense Industrial Base (DIB) sector's cybersecurity posture.

6.

Which of the following actions would be considered a violation of the Code of Professional Conduct (CoPC) for Certified CMMC Professionals (CCPs)?

Soliciting business based on promises of guaranteed certification outcomes

Maintaining confidentiality of assessment results and findings

Continuing professional development and staying current with CMMC requirements

Disclosing any conflicts of interest before starting an assessment

---

Correct answer: Soliciting business based on promises of guaranteed certification outcomes

The Code of Professional Conduct for Certified CMMC Professionals outlines ethical guidelines and standards of behavior expected from professionals involved in the CMMC assessment and certification process. Key points include:

- *Maintaining Confidentiality: Professionals must protect the confidentiality of assessment results and findings.*
- *No Guarantees: It is unethical and a violation to promise guaranteed certification outcomes to solicit business.*
- *Professional Development: Professionals should engage in continuous learning and stay updated with the latest CMMC requirements.*
- *Conflict of Interest: It is important to disclose any potential conflicts of interest before beginning an assessment to ensure impartiality.*

Soliciting business by guaranteeing certification outcomes undermines the integrity and objectivity of the assessment process, thus violating the Code of Professional Conduct.

7.

Which of the following best describes the CMMC Professional (CCP) certification path?

Application, Training, Exam, Certification

Training, Exam, Application, Certification

Training, Application, Certification, Exam

Application, Training, Certification, Exam

Complete CCP Application Online on the Cyber AB website (www.cyberab.org). After that, the applicant should complete an approved training program from a Licensed Training Provider (LTP). They should then demonstrate some basic understanding of CMMC. Only then can they complete a CCP certification test.

8.

Who provides targeted support to top-tier Defense Industrial Base (DIB) companies categorized as critical infrastructure?

National Security Agency (NSA)

DoD Chief Information Officer (CIO)

Defense Counterintelligence and Security Agency (DCSA)

Department of Defense Cyber Crime Center (DC3)

NSA shares "left of boom" products and tools with DIB to prevent bad events from occuring and are responsible for providing targeted support to DIB companies categorized as critical infrastructure.

9.

Which organization is responsible for curriculum development?

LPP

LTP

RPO

OSC

Licensed Partner Publishers (LPPs) are responsible for developing educational content and curriculum that map to the Cyber AB certification exams. Licensed Training Providers (LTPs) are entities that use the authorized curriculum to deliver training to individuals. Registered Practitioner Organizations (RPOs) are organizations that provide advice, consulting, and recommendations to help Organizations Seeking Certification (OSCs) create cybersecurity programs in preparation to meet or exceed CMMC assessment requirements

10.

Which of the following is NOT a prerequisite for the CMMC Professional (CCP) exam?

CompTIA Security+ certification

CompTIA A+ or equivalent knowledge/experience

Passing DoD CUI Awareness Training

2+ years of IT experience

The Certified CMMC Professional (CCP) Test Blueprint defines the exam prerequisites as: A College degree in a cyber or information technology field or 2+ years of related experience or education; or 2+ years of equivalent experience (including military) in a cyber, information technology, or assessment field; and • Suggested CompTIA A+ or equivalent knowledge/experience; and • Complete Certified CMMC Professional Class offered by a Licensed Training Provider (LTP); and • Pass DOD CUI Awareness Training no earlier than three months prior to the exam

11.

This regulation requires DIB suppliers to implement a set of basic security controls from NIST SP800-171 for contractor information systems upon which this information resides and specifies cyber incident reporting.

DFARS 252.204-7012

FAR 52.204-21

Federal Risk and Authorization Management Program (FedRAMP)

Federal Information Security Modernization Act (FISMA)

DFARS 252.204-7012 requires DIB suppliers to implement a set of basic security controls from NIST SP 800-171 for contractor information systems upon which this information resides and specifies cyber incident reporting.

12.

As an active Certified CMMC Professional (CCP), is there a platform where I can list my qualifications and promote myself?

Cyber AB Marketplace

Cybersecurity Job Boards

Department of Defense Personnel Directory

National Cybersecurity Registry

After successfully completing your Certified CMMC Professional (CCP) certification, it will become active once you have completed all required steps, such as signing the Code of Professional Conduct, at that point the CCP will be listed in the CMMC Marketplace that is managed by the Cyber AB.

13.

How often does the CMMC Professional (CCP) need to renew their certification?

Annually

Every 6 months

Every 2 years

It does not need renewal

Once certified, a CCP needs to renew their certification each year, which is currently a $250 fee. However, if they earn the Certified CMMC Assessor (CCA) certification, they will only be required to renew the CCA certification, which is a $500 annual maintenance fee.

14.

What can a Registered Practitioner (RP) do to assist the members of an Organization Seeking Certification (OSC) in achieving CMMC compliance faster?

RPs can offer CMMC training to OSC members to expedite compliance efforts

RPs are responsible for compliance, and training is not within their scope.

RPs can provide CMMC training, but it doesn't contribute to faster compliance

RPs are not allowed to offer CMMC training to OSC members

While they may be equipped and knowledgeable enough to offer CMMC training to OSCs, RPs and Registered Practioner Organizations (RPOs) can only provide advice, consulting, general training, and recommendations. They cannot legally conduct Certified CMMC Assessments or Certified Training. RPs are the "implementers" and consultants and are not certified by Cyber AB.

15.

CMMC framework was developed to be a unifying cybersecurity standard for the Department of Defense (DoD) and improve security within the Defense Industrial Base. Which organization developed it?

The Office of the Undersecretary of Defense (OUSD)

The Cyber Accreditation Body (Cyber AB)

Deparment of Homeland Security (DHS)

Department of Defense (DoD)

The OUSD oversees the security of the Defense Industrial Base (DIB). They developed the CMMC Framework to improve security of the DIB and become a unifying cybersecurity standard for DoD acquisitions to reduce exfiltration of CUI from the DIB

16.

Which is not a requirement to become a CCP:

Obtain a Top-Secret Clearance

Pass the CCP exam

Pass a commercial background check

Complete CCP training with a CMMC Licensed Training Provider (LTP)

Some of the requirement to become a CCP include: completing the CCP application, completing CCP training with an LTP, passing the CCP exam, passing a commercial background check, and signing the Code of Professional Conduct (CoPC) to name a few. You are not required to obtain a Top-Secret Clearance as part of the certification process.

17.

Who holds the final interpretation authority for CMMC Assessment findings if there is no dispute?

The Lead Assessor

The C3PAO

The Assessment Team

The OSC Sponsor

The Lead Assessor holds the final interpretation authority for the recommended practice ratings and their related findings.

18.

Which executive order directed the Defense Secretary to assess risks and make recommendations to support the defense industrial base?

Executive Order 13806

Executive Order 13800

Executive Order 13805

Executive Order 13556

Executive Order 13806 specifically directs the Defense Secretary to assess risks, impacts, and make recommendations in support of the defense industrial base.

19.

The Cyber Accreditation Body (AB) is the sole official accreditation body of the Cybersecurity Maturity Model Certification (CMMC) Ecosystem and the sole authorized non-governmental partner of the U.S. Department of Defense in implementing and overseeing the CMMC conformance regime. The primary mission of The Cyber AB is to authorize and accredit the CMMC Third-Party Assessment Organizations (C3PAOs) that conduct CMMC Assessments of companies within the Defense Industrial Base (DIB). What is the main requirement before the Cyber AB can accredit a candidate C3PAO?

The candidate C3PAO must achieve and maintain ISO/IEC 17011 accreditation standard

The candidate C3PAO must be DFARS 252.204-7012 compliant.

The candidate C3PAO must be compliant at a FISMA moderate level.

The candidate C3PAO must be certified at CMMC Level 1.

Trained CMMC ecosystem, Cyber AB is required to achieve compliance with the ISO/IEC 17011 Conformity Assessment. This assessment will be the certification that Cyber AB provides consistent application of its accreditations. It will also apply impartial attestations of those certified using international consensus-based standards. One condition of the ISO 17011 certification is that it prevents the accrediting body from also controlling the accreditation training program designed.

20.

Susan recently completed a Certified CMMC Professional (CCP) course from a Licensed Training Provider (LTP). What should she do next to complete the process of becoming a CCP?

Apply to obtain a CMMC Professional Number (CPN), send her CPN to the LTP to submit her successful training completion, and sign up for and successfully complete the CCP exam

Begin accumulating the required five years of work experience before taking any further steps

Pursue additional certifications to enhance her qualifications in cloud security

Wait for the certification to be automatically issued, as passing the exam is sufficient for certification

---

To be come a CCP, one must apply to obtain a CMMC Professional Number (CPN), send the CPN to the LTP to submit the successful training completion, and sign up for and successfully complete the CCP exam. Upon successful completion of the process, all candidates will be presented with additional information to include the authorized use of digital credentials in business materials, listing in the CMMC Central Marketplace and access to the Cyber AB's community updates. CCPs, however, cannot participate in CMMC Level 2 assessments, even as an Assessment Team Member. A CCP participating as a CMMC Assessment Team Member on Level 1 or 2 Assessments should be a U.S. Person defined under ITAR Part 120.15 and EAR Part 772.

21.

What prerequisite training must a Certified CMMC Professional (CCP) candidate complete before taking the CCP exam?

DOD CUI Awareness Training

Cybersecurity Basics Course

C3PAO Certification Workshop

NIST Risk Management Fundamentals

A CCP candidate must complete DOD CUI Awareness Training before taking the exam.

22.

Jameson Inc. is looking to contract Beta Systems, an Registered Practitioner Organizations (RPO), for recommendations, advice, and consulting to help them improve their cybersecurity posture due to an upcoming CMMC assessment. Unfortunately, there are many organizations out there proclaiming to be RPOs. Hence, Jameson Inc. must thoroughly vet Beta Systems before contracting them. Which of the following is the most important step that Jameson Inc. must do to ensure Beta Systems is a legitimate RPO?

Jameson must ensure that Beta System has a current (within 1 year) registration with the Cyber AB as an RPO.

Jameson Inc. must have a DUNS number, a proof that they have passed the basic organizational background check via data provided by Dun & Bradstreet

Jameson Inc. must check the Beta System's staff, to confirm there is a member who is a Registered Practitioner at all times.

Jameson Inc. must check to ensure that Beta Systems maintains insurance minimums and provide verification of General Liability, Errors and Omissions, and Cybersecurity Liability insurance

---

RPs and Registered Practitioner Organizations (RPOs) are authorized to represent the organization as familiar with the basic constructs of the CMMC Standard with a Cyber AB provided logo. Individuals holding any level of an RP designation can provide CMMC implementation consulting services to assist in identifying gaps and providing mitigation strategies for an OSC preparing for an assessment. RPs work for Registered Practitioner Organizations (RPO) but can also be contracted as individuals. These professionals bring their experience as well as their CMMC Registered Practitioner (RP) training knowledge to the Organizations Seeking Certification (OSC) as part of contract engagement.

23.

What is the annual maintenance fee to retain your CMMC Professional (CCP) certification and after how long does this start?

$250 and it starts one year after you become certified.

$200, One and a half years after certification.

$25, limmediately after you register for the CCP examination

There is no annual fee to maintain the CCP certification.

It costs $250 and starts one year after the certification

24.

Who is responsible for building, accrediting, certifying, and managing the CMMC ecosystem?

Cyber AB

The Department of Defense

C3PAOs

NARA

The Cyber AB is the sole, authorized accreditation and certification partner of DoD in its CMMC program. All other organizations, are not officially endorsed CMMC entities and do not operate under contract with DoD in support of the CMMC initiative.

25.

_____ is an experienced individual who is authorized to assist an assessor.

Certified CMMC Professional

Certified CMMC Assessor

Registered Practitioner

Assessment Team Member

Certified CMMC Professionals are authorized to participate as assessment team members under the supervision of a Certified CMMC Assessor on CMMC Level 2 Assessments.

26.

Patrick is an independent consultant of a small sized information security consulting firm. He wants to expand his services to include consulting and advisory services to Organizations Seeking Certification (OSCs). After a little research, Patrick learns that to offer such a service, he first must become a CMMC Registered Practitioner (RP). Once he becomes an RP, Patrick wants to be able to work with multiple Registered Practitioner Organizations (RPOs). Can Patrick work with multiple RPOs?

Yes, Patrick can work with a single or multiple RPOs although by mutual consent

Yes, Patrick can work with multiple RPOs but he must be the only Registered Practioner on contract with the RPO

No, Patrick cannot work with multiple RPOs, until his contract with the first RPO expires.

No, Patrick cannot work with multiple RPOs, because he signed an exclusivity agreement with the Cyber AB

Yes, Patrick can work with a single or multiple RPOs although by mutual consent. However, as things are currently, an RP can only be associated with one RPO in the CMMC Marketplace. If an RP's Marketplace affiliation changes from one RPO to another RPO, that change will need to be reflected in the system

27.

What role can a Registered Practitioner (RP) play during an actual CMMC Certification Assessment based on their training?

RPs are not allowed to participate in CMMC Certified Assessments.

RPs can provide certified advice on what is and is not acceptable during the assessment.

RPs are limited to documenting assessment outcomes and cannot offer advice.

Only Certified CMMC Professionals (CCP) can provide advisory services during assessments.

Only Certified CMMC Professionals or Assessors (CCPs/CCAs) can perform CMMC Certification Assessments. During the assessment, no advice can be provided. Prior to the certification assessment, RPs can deliver non-certified advisory services informed by basic training on the CMMC standard.

28.

Halcyon Technologies is a Cloud Service Provider (CSP) that is bidding for a contract to provide sovereign cloud services to a Department of Defense (DoD) prime contractor. The prime deals with Defense Research & Development (R&D) dealing with submarine sonar systems. Understanding that CMMC compliance is a prerequisite to the award of this contract, Halcyon invites a CMMC Third Party Assessment Organization (C3PAO) to conduct an assessment. a) What must Halcyon Technologies do first? b) What will the C3PAO ask for before starting the assessment?

Halcyon should identify the appropriate CMMC Level based on the type of information that will be processed while working for the prime. The C3PAO will ask Halcyon for their System Security Plan (SSP)

Halcyon should develop a System Security Plan (SSP) and Plan of Action & Milestones (POA&M). The C3PAO will ask Halcyon for their Configuration Management Plan (CMP)

Halcyon should seek the expertise of a qualified consulting partner to help with developing their policies and procedures. The C3PAO will ask Halcyon for their Incident Response Plan (IRP)

Halcyon should work with a Certified CMMC Assessor (CCA) to verify that they are ready for the CMMC assessment. The C3PAO will ask Halcyon for their System Security Plan (SSP)

Before contacting the C3PAO, Halcyon should identify the appropriate CMMC level based on the type of information that will be handled on the contract with the Prime. However, prior to making this identification, Halycyon should evaluate their current cybersecurity posture against the requirements of their target CMMC level to identify areas of improvement. This step is known as a Gap Analysis, following which Halcyon should outline the steps needed to address the identified gaps and establish a timeline for implementation. They can seek the expertise of a qualified consulting partner to assist with the process to ensure practices are implemented appropriately producing the desired outcome. During the process, the contractor should update its policies, procedures, and technologies to meet the required CMMC requirements. They are also required to develop a System Security Plan (SSP) and Plan of Action & Milestones (POA&M) that details their current and planned posture. Finally, they can engage the services of a contultant to perform a self-assessment to verify that they are ready for the CMMC Assessment. When the C3PAO engages with a contractor to begin the assessment process, the main document that is requested is the SSP. Additionally the POA&M and Policies & Procedures can be requested for ahead of

the assessment. They request for the Incident Response Plan (IRP) or Configuration Management Plan will happen further along the way, they are not the first set of documents that are typically requested.

29.

Rita has been a Certified Information Systems Auditor (CISA) for 8 years and has performed many cybersecurity audits and risk assessments for her consulting firm's clients. Her firm wants to offer CMMC assessment services. What credentials does Sara need to lead CMMC assessments?

Attend CCP Training from a Licensed Training Provider (LTP), take and pass the CCP exam to earn the CCP certification, complete and submit DoD Suitability Application, train for the Certified CMMC Assessor (CCA), take and pass the CCA exam to earn the CCA certification then participate on three Level 2 assessments only assessing Level 1 practices, take the Lead Assessor training from the Cyber AB when it becomes available and then leverage her existing experience in cybersecurity audits.

Continue leading assessments based on her CISA certification without additional Cyber AB credentials

Enroll in any cybersecurity training program to gain CMMC assessment credentials

Wait for the firm to provide specific guidance on leading CMMC assessments without seeking additional credentials

---

To be come a Lead Assessor, one must attend CCP Training from a Licensed Training Provider (LTP), take and pass the CCP exam to earn the CCP certification, complete and submit DoD Suitability Application, train for the Certified CMMC Assessor (CCA), take and pass the CCA exam to earn the CCA certification then participate on three Level 2 assessments only assessing Level 1 practices, take the Lead Assessor training from the Cyber AB when it becomes available and then leverage her existing experience in cybersecurity audits. Upon successful completion of the process, all candidates will be presented with additional information to include the authorized use of digital credentials in business materials, listing in the CMMC Central Marketplace and access to the Cyber AB's community updates.

30.

What is the minimum passing score on the CMMC Professional (CCP) exam?

0.7

0.6

0.75

0.77

The passing score for the CCP exam is 500/800, which is equivalent to 62.5%. However, candidates can earn a 200-point bonus for showing up, which means the passing score with the bonus is 700/1000, or 70%.

31.

A CMMC Third-Party Assessment Organization (C3PAO) is mandated with all the following, EXCEPT?

Fine an Organization Seeking Ceritification (OSC) for its non-compliance, errors, or omissions

Hire and Train Certified CMMC Assessors To perform CMMC Assessments supported by CCPs

Manage and deliver certification assessments to contracted clients and provide advisory services to other OSCs

Contract with OSCs Looking to achieve a certain CMMC Certification Level

---

C3PAOs have several key responsibilities, including to: i. Contract with OSCs Looking to achieve a certain CMMC Certification Level ii. Hire and Train Certified Assessors To perform CMMC Assessments supported by CCPs iii. Perform Readiness Assessments for OSCs seeking CMMC certification when contacted on the Marketplace iv. Manage and deliver certification assessments to contracted clients and provide advisory services to other OSCs However, C3PAOs are not an enforcement organization within the CMMC ecosystem. Thus, they cannot issue fines for non-compliance.

32.

Which of the following is not an assessment provider?

C3PO

Certified CMMC Professional

Certified CMMC Assessor

C3PAO

CMMC Third-party Assessment Organizations (C3PAOs), Certified CMMC Assessors (CCAs), and Certified CMMC Professionals (CCPs) all provide assessment services. C3PO is not a designation that exists within the CMMC Ecosystem.

33.

Registered Provider Organizations (RPO) can provide which of the following service(s)?

Readiness Assessments

CMMC Assessments

Level 1 Self-Assessments

Certification Assessments

Registered Practitioners (RPs) are the "implementers" and consultants in Certified CMMC Assessments. They do not participate in Certified CMMC Assessments as "Assessment Team Members." RPs deliver a non-certified advisory service informed by basic training on the CMMC standard. By contrast, a Certified CMMC Professional (CCP) or Certified CMMC Assessor (CCA) delivers advice that is based on their rigorous training on what is and is not acceptable during an actual CMMC Certified Assessment. RPs are consultants, employed by or through RPOs, who help OSCs design and implement practices and create processes and process documentation consistent with the CMMC requirements. RPs are authorized to represent themselves as familiar with the basic constructs of the CMMC Standard with a Cyber AB provided logo.

34.

ACME Manufacturing is considering some of their employees for roles supporting their CMMC Level 3 efforts. Which of the following would be the best candidate?

Priya, a Software Developer

Stephen, their HR Manager

Tom, the Accounting Controller

Sarah, the Marketing Director

Priya's software development background makes her the best candidate to support ACME's CMMC Level 3 efforts. Her experience working on systems security and technical skills related to access control, system auditing, and configuration management will be directly relevant to meeting CMMC requirements. Priya's knowledge of secure software development principles and hands-on tech experience also aligns closely with the technical aspects of CMMC Level 3. Her qualifications make Priya well-positioned (compared to others on the list to ensure ACME's systems and software practices meet CMMC standards

35.

ABC Co. is a C3PAO that only has a single Certified CMMC Assessor (CCA), who dissociated himself from the organization on January 15, 2023. By which date is ABC Co. required to associate itself with another CCA?

2/14/2023

1/31/2023

2/28/2023

3/15/2023

C3PAOs are given a 30-day grace period to maintain association with at least one Certified CMMC Professional (CCP), Provisional Assessor (PA), or Certified CMMC A ssessor (CCA).

36.

Which of the following is NOT the responsibility of CMMC Assessors and Instructors Certification Organization (CAICO)?

Certifying Third Party Assessment Organizations

Certifying Assessors; Certifying Third Party Assessment Organizations

Certifying Assessors

Overseeing Training

CAICO is responsible for training and certifying assessors and ensuring assessors are prepared and ready to conduct assessments. They are not responsible for certifying C3PAOs.

37.

What entity approves and authorizes organization's known as CMMC Licensed Training Providers?

The Cyber Accreditation Body (Cyber AB)

The Department of Defense

Cybersecurity Training and Education Consortium

National Institute of Standards and Technology (NIST)

The Cyber Accreditation Body (AB) is the sole official accreditation body of the Cybersecurity Maturity Model Certification (CMMC) Ecosystem and the sole authorized non-governmental partner of the U.S. Department of Defense in implementing and overseeing the CMMC conformance regime. The primary mission of The Cyber AB is to authorize and accredit the CMMC Third-Party Assessment Organizations (C3PAOs) that conduct CMMC Assessments of companies within the Defense Industrial Base (DIB). Currently, The Cyber AB also manages the professional certification and training aspects of the CMMC Ecosystem and authorizes organizations that qualify as Licensed Publishing Partners and Licensed Training Providers, and work with their partners to develop the curricula and examination protocols for CMMC Assessors and CMMC Instructors. This responsibility, however, will soon be "spun-out" from The Cyber AB as the Cybersecurity Assessor and Instructor Certification Organization (CAICO), which will become a its own separate legal entity.

38.

Which is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services?

FedRAMP

FISMA

ISO 27002

CMMC

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

39.

Which of the following is NOT a primary source of CMMC cybersecurity practices?

NIST SP 800-88

48 CFR 52.204-21

DFARS 252.204-7012

NIST SP 800-171 Rev 2

CMMC level 1 fully relies on requirements of 48 CFR 52.204-21 while DFARS 252.204-7012, NIST SP 800-171 Rev 2, and NIST SP 800-172 are the sources from which the 110+ CMMC practices are based on. Therefore, NIST SP 800-88 (Guidelines for Media Sanitization) is the only publication or clause that is not a primary source.

40.

What does the CMMC Professional (CCP) credential allow you to do?

Demonstrate knowledge and understanding of the CMMC Framework.

To perform CMMC Certification Assessments independently.

To become a Certified CMMC Assessor (CCA).

To earn other cybersecurity certifications.

While the CCP credential alone does not specifically allow you to perform CMMC assessments independently or become a certified CMMC assessor, you can work on Level 1 assessments or participate in an Assessment Team Reviewing Level 1 Controls Only. To work on these, you need not be a U.S. citizen. However, working on Level 2 Assessment Teams requires the Team Member to be a Citizen. Those roles typically require other certifications and qualifications, such as the Certified CMMC Assessor (CCA) certification for assessors.

41.

Which of the following is not a pillar of the Office of the Undersecretary of Defense (OUSD) acquisition process?

Professionally trained personnel

Schedule

Cost

Cybersecurity

Recognizing that the three pillars of the OUSD acquisition process (cost, schedule, and performance) can only be effective in a secure environment, the DoD added cybersecurity as the fourth pillar.

42.

What must a contractor do to maintain their CMMC 2.0 expert level certification?

Triennial Government-led assessments by the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC)

Quarterly internal audits with annual self-attestations

Continuous monitoring by the Department of Defense

Biennial reviews by the Cyber Accreditation Body

To maintain an expert (level 3) CMMC certification, a contractor needs triennial Government-led assessment. This level also requires implementation of 110 practices from NIST SP 800-171 and practices from NIST SP 800-172.

43.

Which domain makes up the largest percentage of the CMMC Professional (CCP) exam?

The CMMC Model Construct and Implementation Evaluation

The CMMC Governance and Source Documents

The CMMC Code of Professional Conduct

The CMMC Ecosystem

As a CCP, you are required to understand all levels of the CMMC Model, its underlying regulatory requirements, and its unique implementation requirements, all of which are contained within the "CMMC Model Construct and Implementation Evaluation" domain and is 35% of the exam. The other domains are weighted as follows on the CCP exam: The CMMC Governance and Sources Documents - 15% The CMMC Code of Professional Conduct (Ethics) - 5% The CMMC Ecosystem - 5% The CMMC Assessment Process (CAP) - 25% Scoping - 15%

44.

What evaluation requirements apply to a CMMC Third-Party Assessment Organization (C3PAO) under the CMMC framework?

C3PAOs must undergo evaluation under a specific CMMC assessment level

C3PAOs are evaluated based on their previous cybersecurity certifications

Evaluation requirements for C3PAOs are determined by the DOD

C3PAOs can self-evaluate their compliance without external scrutiny

---

Entities seeking to become a C3PAO must pass a CMMC Level 2 assessment performed by the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) and obtain a CMMC Level 2 Certification and pass a Foreign Ownership, Control or Influence (FOCI) and SF-328 review to be eligible

45.

_____ are consultants, employed by or through RPOs, who help OSCs design and implement practices and create processes and process documentation consistent with the CMMC requirements.

Registered Practitioners

Certified CMMC Professionals

Certified CMMC Assessors

Assessment Team Members

Registered Practitioners (RPs) are consultants, employed by or through Registered Practitioner Organizations (RPOs), who help OSCs design and implement practices and create processes and process documentation consistent with the CMMC requirements.

46.

In CMMC 2.0 there are significant changes compared to the previous version 1.0. Which of the following is not true?

CMMC 2.0 places a lot of effort on maturity processes unlike in CMMC 1.0

There are 14 domains in CMMC 2.0 compared to the 17 in CMMC version 1.0

There are 3 maturity levels in CMMC 2.0 unlike CMMC 1.0 that had 5 levels

CMMC 1.0 had a total of 171 practices compared to CMMC 2.0's 110+.

Unlike CMMC 1.0 that had five maturity levels, CMMC 2.0 has only three (foundational, advanced, and expert). Further, while CMMC 1.0 had 17 cyber domains, the 2.0 framework has 14. Domains are distinct groups of cybersecurity practices with similar characteristics that are critical for protecting controlled unclassified information and federal contract information either separately or together. Within the 2.0 framework, 110 practices associated with the various domains are identified at level 2, which is equivalent to level 3, and a reduction from the 130 practices for CUI protection under CMMC 1.0). Currently, at level 1, 17 practices apply for the basic security of covered information systems for the protection of federal contract information, which is similar to CMMC 1.0. Additional practices for level 3 from NIST SP 800-172 have not yet been agreed upon.

47.

What is the length of the CMMC Professional (CCP) exam?

3.5 hours

3 hours

2.5 Hours

4 Hours

The Certified CMMC Professional (CCP) Test Blueprint defines the length of the CCP exam as 3.5 hours maximum.

48.

The single clearinghouse for classified incident reports is:

Defense Counterintelligence and Security Agency (DCSA)

Defense Contract Management Agency (DCMA)

Department of Defense Cyber Crime Center (DC3)

National Security Agency (NSA)

The Defense Counterintelligence and Security Agency (DCSA) ensures companies are taking necessary measures to protect their facilities, personnel, and associated IT systems against vulnerabilities and potential attacks.

49.

Minimum threshold and requirements for CMMC certification, C3PAO ownership and assessor certification is set by:

DoD

OUSD(A&S)

NIST

NARA

The DoD owns and controls the CMMC Model and related documentation.

50.

Which of the following is NOT a responsibility of the Cyber AB?

Setting threshold and requirements for CMMC certification

Managing the CMMC ecosystem

Providing feedback to DoD on the CMMC Model implementation

Creating minimum education and service requirements for service providers

---

The Cyber AB is the official accreditation body of the Cybersecurity Maturity Model Certification (CMMC) Ecosystem and the sole authorized non-governmental partner of the U.S. Department of Defense in implementing and overseeing the CMMC conformance regime. It exists to further the successful implementation of CMMC within the Defense Industrial Base in order to reduce digital risk to DoD's supply chains and contractor support infrastructure. The primary mission of The Cyber AB is to authorize and accredit the CMMC Third-Party Assessment Organizations (C3PAOs) that conduct CMMC Assessments of companies within the Defense Industrial Base (DIB). Currently, The Cyber AB also manages the professional certification and training aspects of the CMMC Ecosystem, working with their partners to develop the curricula and examination protocols for CMMC Assessors and CMMC Instructors. This responsibility, however, will soon be "spun-out" from The Cyber AB as the Cybersecurity Assessor and Instructor Certification Organization (CAICO), which will become a its own separate legal entity.

51.

Which of the following is NOT the role of a Certified CMMC Assessor (CCA) as an assessment team member?

Identifying methods, techniques, and responsibilities, for collecting, managing and reviewing evidence.

Mapping responses from interviewees to CMMC practices to evaluate and aid in determining and supporting the rating of that practice.

Updating and reviewing the assessment requirements and plan for the assessment continuously as more information is gathered.

Recording draft assessment requirements and interviewing the POCs within the OSC to understand the nature of the OSC's business.

As an assessment team member, the CCA continuously reviews and updates the assessment requirements and plan for the assessment as more information is gathered. They also record draft assessment requirements and interview the POCs within the OSC to understand the nature of the OSC's business and the configuration of their systems and processes. The CCA maps responses from interviewees to CMMC practices to evaluate and aid in determining and supporting the rating of that practice. They also record any in-scope practices determined to be fully compliant. They also identify, describe, and record any gaps in CMMC practices or processes and present the results of each day to the OSC during a daily checkpoint meeting.

52.

Which of the following were not involved in developing the CMMC?

NASA Jet Propulsion Laboratory (JPL)

The Office of the Undersecretary of Defense for Acquisition and Sustainment (OUSD (A&S))

Carnegie Mellon University Software Engineering Institute (SEI)

The Johns Hopkins Applied Physics Laboratory (APL)

In 2019, to bolster the cybersecurity posture of the DIB sector and prevent losses of intellectual property and CUI, the Office of the Undersecretary of Defense for Acquisition and Sustainment (OUSD(A&S)) engaged the researchers at the Carnegie Mellon University Software Engineering Institute (SEI) and The Johns Hopkins Applied Physics Laboratory (APL) to develop the CMMC.

53.

Which of the following best describes the target audience for the Certified CMMC Professional (CCP) certification exam?

A wide range of professionals, including IT, cybersecurity, compliance, legal, management, and more.

Only cybersecurity professionals

Only those who want to become Certified CMMC Assessors

Only those with prior cybersecurity experience

The Certified CMMC Professional (CCP) Test Blueprint defines the intended audience as: - Employees of Organizations Seeking Certification (OSC), Information Technology (IT) and Cybersecurity Professionals, Regulatory Compliance Officers, Legal and Contract Compliance Professionals, Management Professionals - Cybersecurity and Technology Consultants - Federal Employees - Candidate CMMC Assessment Team Members

2. CMMC-AB Code of Professional Conduct (Ethics)

54.

The CMMC Code of Professional Conduct (CoPC) applies to the following individuals and entities, EXCEPT

Company Chief Information Security Officers (CISOs)

Certified CMMC Professional (CCP) Certified CMMC Assessor (CCA) Certified CMMC Instructor (CCI) Certified CMMC Master Instructor (CCMI) CMMC Quality Assurance Professional (CQAP)

CMMC Third Party Assessment Organization (C3PAO)

Registered Practitioners (RPs) Registered Practitioner Advanced (RPA) Registered Practitioner Organization (RPO) Licensed Publishing Partner (LPP) Licensed Training Provider (LTP)

CoPC applies to credentialed individuals and those applying to the Cyber AB to be credentialed as either a Certified CMMC Professional (CCP), a Certified CMMC Assessor (CCA), a Certified CMMC Instructor (CCI), a Certified CMMC Master Instructor (CCMI), or a CMMC Quality Assurance Professional (CQAP). It is also a requirement for the entities that provide training materials for Certified Assessors or Certified Professionals (i.e., Licensed Training Partners (LTPs) and Licensed Publishing Partners (LPPs)). It also applies to the entities accredited by the Cyber AB to employ or engage Credentialed Individuals to conduct assessments, and entities applying for accreditation and to those individuals and entities that register for inclusion in the Cyber AB's directory of Credentialed Individuals and Accredited entities. However, company CISOs are not bound to the CMMC CoPC

55.

In terms of CoPC violations, an appeal against Cyber AB corrective actions may be filed within how many days?

30 days

60 days

90 days

15 days

If you have been subject to a corrective action and wish to appeal the outcome with the Cyber AB, you may request a review within 30 days of termination notice.

56.

Which of the following organizations reserves the right to investigate CMMC Credentialed, Registered, and Accredited persons or entities for potential violations arising from unusual behavior?

The Cyber AB

The CAICO

The DoD

The ISO/IEC

The Cyber AB monitors the CMMC-related activity of all CMMC Credentialed, Registered, and Accredited roles and reserves the right to investigate any potential violations that arise from unusual behavior.

57.

What document provides the performance standards by which the roles of the CMMC Ecosystem will be held accountable?

The Code of Professional Conduct (CoPC)

The CMMC Model

The CMMC Assessment Process

The CMMC Scoping Guide

The Code of Professional Conduct (CoPC) sets expectations for those CMMC-AB credentialed individuals and entities that are authorized to deliver CMMC services under license from the CMMC Accreditation Body (CMMC-AB). It also sets expectations for those Registered Practitioners (RPs) and Registered Provider Organizations (RPOs) that deliver unlicensed non-certified services that choose to register with the CMMC-AB, and other individuals and entities with a relationship to the CMMC-AB. This CoPC represents the performance standards by which the roles of the CMMC eco-system will be held accountable, and the procedures for addressing violations of those performance standards.

58.

Mr. XYZ has been convicted for stealing cash from a store. Mr. XYZ does not report this conviction to the Cyber AB as he thinks that this matter does not directly link to his role as a CMMC Assessor. Is Mr. XYZ correct in not disclosing his conviction, and how soon after, if necessary, should he disclose his conviction?

No, 30 days after

Yes, 15 days after

Yes, 30 days after

No, 15 days after

Mr. XYZ is not correct in not disclosing his conviction to the Cyber AB. Consequently, he needs to report to the Cyber AB within 30 days of conviction, whether or not in connection with activities that relate to his role in the CMMC ecosystem. Negligence to disclose a conviction can be perceived as an infringement of the Cyber AB's code of conduct, which can lead to disciplinary consequences.

59.

What sets the expectations for accredited and credentialed entities authorized to deliver CMMC services under Cyber AB licensing?

CMMC Code of Professional Conduct

CMMC Code of Ethical Conduct

Code of Practical Conduct

CMMC Professional Conduct Guidelines

The Code of Professional Conduct (CoPC) sets expectations for credentialed individuals and accredited entities that are authorized to deliver CMMC services under license from the Cyber AB. CoPC sets expectations for RPs and RPOs that deliver unlicensed noncertified services that choose to register with the Cyber AB, and other individuals and entities with a relationship to the Cyber AB.

60.

Which organization initiates an investigation if a violation of the code is reported?

Cyber AB

NARA

OUSD (A&S)

DoD

The Cyber AB may initiate an investigation based on a complaint or on information received or observed relating to a violation by a person or organization.

61.

Which of the following activities is NOT prohibited behavior for CMMC Assessors?

Fulfilling all commitments as defined in the contract or registration agreement

Providing a guarantee of the assessment results

Soliciting business from customers either for themselves or their organization

None of the above

CoPC practices include professionalism that discourages dishonesty in all dealings including misleading or exaggerating services you accredited.

62.

If an investigation finds that the CoPC has been violated. Corrective actions may include: warning, remediation, suspension, _____ , as well as temporary or permanent loss of eligibility for such credentials.

Denial or termination of CMMC Credentials, Registration, or Accreditation

A Warning

Temporary or permanent loss of eligibility for credentials

A Financial Penalty

Corrective actions may include warning, remediation, suspension, denial or termination of CMMC Credentials, Registration, or Accreditation, as well as temporary or permanent loss of eligibility for such credentials.

63.

Which of the following applies if a member of the CMMC ecosystem witnesses a violation of the Code of Professional Conduct (CoPC)?

They should report ethical violations, misconduct, or professional breaches to the CMMC Accreditation Body within 30 days, regardless of whether they try to personally resolve the situation or not

They should report to the Department of Justice's False Claims Act team for the violating party to be arrested

They should escalate the issue to the International Standards Organization (ISO), for there to be an investigation

They should talk with the violating party and settle the underlying issues

---

If a member of the CMMC ecosystem violates the Code of Professional Conduct (CoPC), they should not just try to privately settle the issues with the aggrieved party. According to the CoPC, individuals who participate in the CMMC ecosystem have an obligation to report ethical violations, misconduct, or professional breaches to the CMMC Accreditation Body within 30 days, regardless of whether they try to personally resolve the situation. Violations of the CoPC can undermine the integrity and trustworthiness of the entire CMMC framework, so handling them as internal matters between two parties is insufficient. Formal reporting enables oversight bodies to conduct proper investigations and enforce standards consistently across the ecosystem. Trying to quietly settle CoPC violations without external awareness risks enabling unethical or unprofessional actions to continue. For the good of the ecosystem, violations must be reported

64.

The investigation of a violation may result in findings and recommendations for _____.

Corrective Action

The C3PAO

Certification

A Different Maturity Level

Corrective action is taken depending on the nature of the violation and the policies. The investigation manages the issue and dissuades it from reoccurring. Corrective actions may include remedial action or revocation of license.

65.

A CMMC implementation consultant has been asked to conduct a certified assessment. Which of the following should the consultant do?

Decline the assignment

Accept the assignment

Provide a disclaimer to management before accepting the audit

None of the above

Under no circumstances are credentialed or registered individuals permitted to conduct a certified assessment, or participate on a certified assessment team, if they have also served as a consultant to prepare the organization for that assessment. Consulting is defined as "providing direct assistance to the creation of processes, training, and technology required to meet the intent of CMMC controls and processes."

66.

Which of the following designations is not permitted by the Cyber AB to participate in a CMMC certification assessment?

Registered Practitioner

Certified CMMC Professional

Certified CMMC Assessor

Provisional Assessor

Registered Practitioners (RPs) are the "implementers" and consultants in Certified CMMC Assessments. They do not participate in Certified CMMC Assessments as "Assessment Team Members." RPs deliver a non-certified advisory service informed by basic training on the CMMC standard. By contrast, a Certified CMMC Professional (CCP) or Certified CMMC Assessor (CCA) delivers advice that is based on their rigorous training on what is and is not acceptable during an actual CMMC Certified Assessment. RPs are consultants, employed by or through RPOs, who help OSCs design and implement practices and create processes and process documentation consistent with the CMMC requirements. RPs are authorized to represent themselves as familiar with the basic constructs of the CMMC Standard with a Cyber AB provided logo.

67.

The practices in the CMMC Code of Professional Conduct (CoPC) are mandatory expectations for any member of the CMMC ecosystem. Which of the following is NOT a repercussion of failure to comply with or violating the CoPC practices?

$1000 fine per violation

A warning

Temporary suspension

Permanent revocation of credentials

Violating the CMMC CoPC practices may result in sanctions, up to and including denial or revocation of a Credential, Registration, or Accreditation. This encompasses a warning, suspension, and permanent revocation.

68.

Which of the following is not true about the Confidentiality principle of the CMMC Code of Professional Conduct (CoPC)?

If revealing the confidential customer or government data is beneficial to an entity or member of the CMMC, or an OSC's compliance efforts the entity is authorized to release it.

Members of the CMMC ecosystem should treat confidential information with utmost care

Entities and individuals within the CMMC ecosystem should ensure the confidentiality of government and customer data.

CMMC ecosystem members should never reveal information learned during the delivery of a CMMC service to any entity unless that entity is expressly authorized to view it

---

The CMMC ecosystem members should maintain the confidentiality of customer and government data. They should treat confidential information with the utmost care, and under no circumstances reveal whatever they learn during the delivery of CMMC services to anyone who is not expressly authorized to view it.

69.

Assisting the client in rectifying an anomaly, so that it is not reported, is a violation of which of the following?

Information Integrity; Proper Use of Methods; Professionalism & Objectivity

Information Integrity

Proper Use of Methods

Professionalism & Objectivity

Assisting a client in rectifying an anomaly threatens the integrity of the process and compromises the objectivity of the client. This opposes information integrity, proper use of methods, professionalism, and objectivity. Essentially, honesty and transparency is needed in the relationship between clients and stakeholders.

70.

Jane is a Certified CMMC Assessor (CCA) for a leading CMMC Third Party Assessment Organization (C3PAO). The C3PAO has selected a team of four led by James to assess how Micron Inc., an Organization Seeking Certification (OSC), has implemented the requirements for a level 2 certification. However, she witnesses James and Micron's Chief Information Security Officer (CISO) strike a deal to manipulate some findings to ensure the OSC is certified. What should Jane do?

When observing colleagues making choices that are in violation of the CoPC, you should privately request clarification or offer to help rectify the violation. Thereafter, you should report the ethical violation, misconduct, or professional breach to the CMMC Accreditation Body within 30 days.

She should report to the Department of Justice's False Claims Act team for James and the CISO to be arrested

She should escalate the issue to the Department of Defense's investigation team for them to initiate an investigation

She should talk with both James and the CISO and tell them to self-report or she will escalate the matter to the Cyber AB

When observing colleagues making choices that are in violation of the CoPC, you should privately request clarification or offer to help rectify the violation.

71.

In a situation where the first assessor concludes there are gaps requiring addressing before certification, and the Organization Seeking Certification (OSC) contracts with a second assessor who finds adequate implementation of the practices, can the first assessor release their findings to challenge the second assessor's certification?

No, releasing findings would violate the non-disclosure agreement (NDA) and the Code of Professional Conduct

No, as it goes against the principles of fairness and impartiality in assessments.

Yes, but only if the OSC requests the first assessor to do so.

Yes, the first assessor can release their findings to present an alternative perspective.

No. Any member of the CMMC ecosystem be it consultants, assessors, trainers, or even OSCs should always portray a professional business posture. Therefore, the assessor should respect the Non-Disclosure Agreements (NDAs), remain objective to avoid any conflict of interests, and ensure confidentiality of whatever information they come across during the assessments.

72.

The Cyber AB can initiate an investigation into an accredited, registered, or credentialed members of the CMMC ecosystem based on which of the following?

Complaint or on information received or observed relating to a violation

None of the above

Evidence of an entity like a C3PAO or CCA unfairly competing with others

Social media posts that an entity may be involved in a violation

---

Cyber AB may initiate an investigation based on a complaint or on information received or observed relating to a violation by a person or organization covered by CoPC

73.

Violation of the Code of Professional Conduct practices may result in:

Denial or revocation of a Credential, Registration, or Accreditation; Loss of eligibility to hold a Credential, Registration, or Accreditation

Denial or revocation of a Credential, Registration, or Accreditation

Loss of eligibility to hold a Credential, Registration, or Accreditation

A Financial Penalty

Violation of the CoPC may lead to corrective actions that include warning, remediation, suspension, denial or termination of CMMC Credentials, Registration, or Accreditation, as well as temporary or permanent loss of eligibility for such credentials.

74.

The CoPC guiding principle that says to treat confidential information with the utmost care, and under no circumstances reveal information learned during the delivery of CMMC services to anyone who is not expressly authorized to view it is:

Confidentiality

Information Integrity

Objectivity

Availability

Confidentiality exercises due care to ensure that confidential or privileged information gathered during assessments or consulting remains so, even after a work engagement has ended.

75.

When a CMMC Assessor discovers an anomaly, which of the following is the most appropriate action to take?

Document the results

Inform Client's Senior Management of the potential issue

Request client to rectify the issue

All of the above

Documenting and describing the anomaly to all affected parties is essential to secure an agreement to continue.

76.

Which of the following documents should be referred to when a Cyber AB member faces a situation that may result in the compromise of integrity?

Code of Professional Conduct

ISO/IEC Code of Ethics

FISMA

NIST SP 800-37

According to the CoPC Guiding Principles, it said, "Demonstrate integrity in the use of materials and methods as they are described by the Cyber AB in policies, methodologies, and training materials. "

77.

The entities or individuals in the CMMC ecosystem should do all the following, EXCEPT?

Work with your company to suppress any evidence of conflict of interest.

Complete Conflict of Interest Declaration as required by the agreement

Avoid the appearance of, or actual, conflicts of interest where possible

Comply fully with Conflict-of-Interest policies that may be signed as part of license agreements

---

The CoPC requires that entities and individuals transparently disclose conflicts to affected stakeholders, including your own organization and your customer, when they are unavoidable.

78.

Educavo is an accredited Licensed Training Provider (LTP) that delivers training services through Cyber-AB certified individuals. The same individuals also participate in certified assessment teams. Which practice of the CMMC Code of Professional Conduct (CoPC) is violated here?

Professionalism

Confidentiality

Lawful and ethical practices

Objectivity

Under no circumstances are credentialed or registered individuals permitted to conduct a certified assessment, or participate on a certified assessment team, if they have also served as a consultant to prepare the organization for that assessment. Consulting is defined as "providing direct assistance to the creation of processes, training, and technology required to meet the intent of CMMC controls and processes.

79.

Which of the following activities would constitute a breach of the confidentiality principle?

Inability to exercise due care in ensuring privacy of clients' data; Disclosing clients' information to a third party without explicit consent from client

Inability to exercise due care in ensuring privacy of clients' data

Disclosing information to government agency (when required by law) without explicit consent from client

Disclosing clients' information to a third party without explicit consent from client

---

Confidentiality protects identifiable and confidential customer data from unauthorized disclosure, unless permitted in writing by the Cyber AB or from a legal obligation.

80.

You are a Certified CMMC Assessor (CCA) for a large CMMC Third Party Assessment Organization (C3PAO) and have been tasked with assessing the cybersecurity posture of an Organization Seeking Certification (OSC) looking to be CMMC certified at level 2. Which CMMC Code of Professional Conduct should you follow to ensure information integrity of the OSC?

Ensure authenticity and accuracy of the information received or discovered during the delivery of CMMC services

Ensure information is securely copied and retained by the Assessment Team after the Assessment concludes

Accurately disseminate all the information received or discovered during the delivery of CMMC services to the CyberAB

Ensure that you fill out the evaluation materials on the OSC's behalf

---

To ensure information integrity, you should report results and data from Assessments and Training objectively, clearly, accurately, and completely. Further, you must ascertain that the information presented is authentic and accurate. Your actions should also ensure the security of all information discovered or received while delivering CMMC services. Members of the CMMC ecosystem should never cheat, assist another in cheating, or allow cheating on examinations. Cheating includes unauthorized reproducing, distributing, displaying, discussing, sharing or otherwise misusing test questions or any part of test questions before, during or after an examination. They should never use deceptive means, including submitting to the Cyber AB or a C3PAO any document or testimony that contains a misstatement of fact or omits a fact to obtain, attempt to obtain or assist others in obtaining or maintaining a CMMC Credential, Accreditation, or Registration.

81.

Which of the following entities is responsible for initiating investigations for potential CoPC violations?

The CyberAB

The DoD

CMMC Third Party Assessment Organizations (C3PAOs)

CMMC Assessors and Instructors Certification Organization (CAICO)

The Cyber AB may initiate an investigation based on a complaint or on information received or observed relating to a violation by a person or organization covered by this Code. The Cyber AB has sole authority to determine the action to be taken.

82.

When a CMMC-AB member is not representing themselves in a way that is in line with the certification, this represents a lack of _____.

Professionalism

Integrity

Objectivity

Proper Use of Methods

Under the CoPC, professionalism is defined as "Always maintain a professional business posture. Never represent yourself or your company in a way that is not aligned with your certification, Non-Disclosure Agreement (NDA), or authorization by the AB."

83.

Under what circumstances is the CMMC Assessor authorized to disclose a client's confidential information?

When explicitly authorized by the client; When required by law

Under no circumstances

When explicitly authorized by the client

When required by law

Protect identifiable and confidential customer data from unauthorized disclosure, unless permitted in writing by the Cyber AB or from a legal obligation to disclose the information.

84.

Which CMMC Code of Professional Conduct practice requires that due care is taken to ensure that confidential or privileged information gathered during assessments or consulting remains so, even after a work engagement has ended.

Confidentiality

Professionalism

Information Integrity

Lawful and Ethical Practices

Confidentiality requires that you protect identifiable and confidential customer data from unauthorized disclosure, unless permitted in writing by Cyber AB or from a legal obligation to disclose the information. Entities and individuals must also take due care to ensure that confidential or privileged information gathered during assessments or consulting remains so, even after a work engagement has ended. Additionally, you should not share working group materials or conversations outside of the working group. Do not post working group decisions or conversations on social media.

85.

What actions are allowed for a Certified CMMC Assessor (CCA) or a CMMC Third-Party Assessment Organization (C3PAO) after a CMMC Assessment to influence the certification of an Organization Seeking Certification (OSC) ahead of contract award?

To maintain integrity, tweaking findings to expedite certification during or after an assessment is strictly prohibited

The OSC has the sole authority to adjust findings after a CMMC Assessment.

CCAs and C3PAOs can tweak findings but only with explicit approval from the Cyber AB

CCAs and C3PAOs can adjust findings to expedite certification with proper justification

---

The Assessors are bound by CMMC Code of Professional Conduct that demands they ensure information integrity. Hence, they should report the results of the assessments fully, accurately, and with integrity as required by their certification or licensing agreements. No actions are allowed after a CMMC Assessment.

86.

A Certified CMMC Assessor has been assigned a job that may create a "Conflict of Interest" issue. Which of the following should the Certified CMMC Assessor do?

Provide a disclaimer of the conflict of interest to management before accepting the audit.

Accept the assignment

Provide a disclaimer of the conflict of interest to the assessment team lead before accepting the audit

Decline the assignment

Under the guiding principle of Objectivity, the CoPC requires the CCA to document and describe the conflict of interest to all affected parties and secure agreement to continue when a perceived or actual conflict may be present.

87.

Which of the following statements BEST describes why ethics in cybersecurity are important?

Humans are involved with everyday decisions that impact the safety of systems and data.

The laws that govern cybersecurity require ethical behavior.

Ethics are required by the CMMC Code of Professional Conduct (CoPC).

Ethics and cybersecurity are not related.

Cybersecurity is a blend of ethics and technical complexity. Since humans are involved with decisions that affect the data and systems safety, ethics certainly are critical. This is because one wrong decision exposes systems and data to malicious actors such as ransomware groups, hackers, among others.

88.

Which of the following is not a principle of the CoPC?

Stubbornness

Professionalism

Objectivity

Confidentiality

Stubbornness is not a principle of the Code of Professional Conduct (CoPC) of the Cyber AB because it refuses to compromise and ignores others' ideas. Open-mindedness is a foundation for assessors to build effective relationships with their clients.

89.

What is meant by Information Integrity?

Retaining accuracy and authenticity of information received from client

Using consistent testing/assessment approach to preserve the integrity of CMMC service delivery

Offering guaranteed assessment results

Fulfilling all commitments as defined by the contract or registration agreement.

Information integrity is defined as the trustworthiness and reliability of information including its accurateness, coherence, and credibility.

90.

Using "Undercutting" to get a client, is a violation of which of the following?

Professionalism

Objectivity

Proper Use of Methods

Professionalism; Proper Use of Methods; Objectivity

Professionalism requires honesty in all dealings and delivers CMMC services according to the agreements with customers and Cyber AB. Additionally, it does not misrepresent your organization, such as selling services that are not accredited to deliver, falsifying records or experience, or proposing fees that are far below the level of effort that is required.

91.

This is a contract by which one or more parties agree not to disclose confidential information that they have shared with each other as a necessary part of doing business together.

Non-disclosure Agreement

Intellectual Property Agreement

Secrecy Agreement

Memorandum of Understanding

Non-disclosure Agreement is binding and prevents sensitive information from being shared with others.

92.

As the lead assessor for Organization Seeking Certification (OSC) Matrix Technologies CMMC Certification Assessment, Bauer has scheduled a site visit, and his team has made travel arrangements. His team has organized several interviews and demonstrations with Felicity, Matrix Technologies' system administrator, who is responsible for executing various security tasks on their network. On the first day of the site visit, the CEO of Matrix Technologies informs Bauer that Felicity has fallen seriously ill and has been hospitalized. Consequently, she will not be available for the assessment. The CEO offers to be interviewed by Bauer about Felicity's responsibilities, despite not being directly involved in her work. Bauer agrees to the CEO's proposal out of concern for Felicity and to ensure that the assessment can proceed smoothly without causing any frustration for the CEO. Should Bauer have agreed to let the CEO substitute Felicity?

No, the CEO is not the implementer of those practices and will have limited knowledge of how they operate

Yes, Bauer has accepted to be the lead assessor, a role he has always wanted and he does not want to disappoint his manager

Yes, Bauer as the lead assessor, knows this is an important opportunity for his company and he wants to make sure everything goes smoothly

No, he and Felicity are past co-workers and had agreed privately to collaborate on the assessment so that Matrix Technologies will pass their assessment

---

The CMMC Assessment Process and Assessment Guides explicitly stipulate interviews and demonstrations should involve the individual(s) responsible for executing the tasks. Bauer should inquire whether there is someone else tasked with performing Felicity's responsibilities during her absence. This violates the proper use of methods principle.

93.

Which CoPC practice requires that due care is taken to ensure that confidential or privileged information gathered during assessments or consulting remains so, even after a work engagement has ended?

Confidentiality

Information Integrity

Lawful and Ethical Practices

Professionalism

Confidentiality exercises due care to ensure that confidential or privileged information gathered during assessments or consulting remains so, even after a work engagement has ended.

94.

Which CMMC Code of Professional Conduct principle involves avoiding any actual or perceived conflicts of interest?

Objectivity

Professionalism

Confidentiality

Information Integrity

Members of the CMMC ecosystem should remain objective. They should avoid the appearance of, or actual, conflicts of interest where possible, and full compliance with Conflict-of-Interest policies that may be signed as part of license agreements. In the case where a perceived or actual management conflict may be present, they must document and describe the conflict to all affected parties and secure agreement to continue

95.

Which of the following is the most effective way to restrict the disclosure of sensitive information?

Signing a Non-Disclosure Agreement

All of the above

Explicitly providing the name of parties with whom sensitive information may be shared

Limiting the provision of sensitive information

A Non-Disclosure Agreement (NDA) is a contract by which one or more parties agree not to disclose confidential information that they have shared as a necessary part of doing business together. Additionally, it is binding and prevents sensitive information from being shared with others.

96.

How many days do you have to appeal the outcome of a corrective action?

- **30**
- 90
- 60
- 45

If you have been subject to a corrective action and wish to appeal the outcome with the Cyber AB, you may request a review within 30 days of termination notice.

97.

Can any party within the CMMC ecosystem terminate their agreements at any time for whatever reason without any explanations?

Yes, but termination requires written notice with reasons provided

No, termination is not allowed within the CMMC ecosystem

Yes, any party can terminate agreements unilaterally

No, only the Cyber AB has the authority to terminate agreements

---

Any party (CMMC Accredited Organization, CMMC Credentialed Individuals) may terminate their agreements at any time, with or without cause, with thirty (30) calendar days written notice to the other party, prior to the date specified in such notice

98.

A member of the CMMC ecosystem should do the following under the code of professional conduct to ensure confidentiality, except?

Posting working group decisions or discussions on social media for more publicity.

Protecting the confidential and identifiable customer data from unauthorized disclosure

Never copying tools or materials from external entities with no explicit permissions to.

Ensure that privileged information gathered during consulting remains as such.

Working group materials or conversations should not be shared outside of the working group. Therefore, it is obvious that they should not be posted on social media.