CMMC Certified Professional™ (CCP™) and CMMC Certified Assessor™ (CCA™)

EXAM CANDIDATE GUIDE

CCP CMMC Certified Professional™
An ISACA® | CAICO® Certification

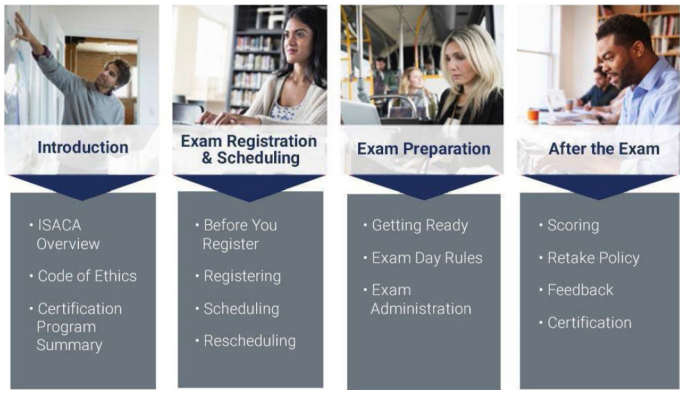
CCA CMMC Certified Assessor™
An ISACA® | CAICO® Certification

CONTENTS

CANDIDATE GUIDE OVERVIEW

Review this guide thoroughly. It contains important details ISACA exam candidates need to know before administration of the exam, including scheduling information, exam eligibility, and exam day rules.

This guide provides candidates with everything required to prepare for and take the CMMC Certified Professional (CCP) and CMMC Certified Assessor (CCA) exams and is separated into four (4) major sections:



Section I: Introduction

1.1 ISACA Overview and Code of Ethics

ISACA is a pace-setting global association that helps individuals and enterprises achieve the positive potential of technology.

ISACA equips professionals with knowledge, credentials, education, and community to advance their careers and transform their organizations.

ISACA leverages the expertise of its more than 185,000+ members who work in digital trust fields such as cybersecurity, governance, assurance, risk, privacy, and quality, as well as its enterprise performance subsidiary, CMMI® Institute, to help advance innovation through technology.

ISACA has a presence in 190 countries, including more than 230 chapters worldwide and offices in both the United States and China.

ISACA Products and Services

Membership

Being an ISACA member gives you access to exclusive member benefits, including savings on ISACA products like certification exams, conferences, and exam preparation materials.

Resources

Explore the latest research, guidance, and expert thinking on standards, best practices, and emerging trends.

Training

ISACA's globally respected training and certification programs inspire confidence that enables career progression and innovation in the workplace.

COBIT

COBIT is ISACA's legacy framework for customizing and right-sizing enterprise governance of information and technology

Certificate and Certification Programs

A full list of ISACA's certificate and certification programs can be found at: https://www.isaca.org/credentialing.

Code of Ethics

ISACA sets forth a Code of Professional Ethics to guide the professional and personal conduct of its members and/or certification holders.

- Members and those certified are required to abide by ISACA's Code of Professional Ethics.
- Failure to comply can result in an investigation and disciplinary measures, including but not limited to exam score nullification or certification revocation.

1.2 CCP and CCA Certification Program Summary

The table below provides a summary of the two ISACA certifications addressed in this guide.

	CCP CMMC Certified Professional An ISACA® | CAICO® Certification	CCA CMMC Certified Assessor An ISACA® | CAICO® Certification
Description	A CMMC Certified Professional (CCP) is the foundational certification for anyone seeking to work within the implementation and assessment ecosystem of the US Department of War's (DOW) Cybersecurity Maturity Model Certification (CMMC) program. It validates that a professional is ready to help organizations achieve assessment-ready cybersecurity programs or participate on a CMMC Assessment Team during official CMMC assessments.	A CMMC Certified Assessor (CCA) is the certification required to perform formal CMMC Level 2 assessments within the US DOW's cybersecurity ecosystem. A CCA equips experienced cybersecurity professionals with the advanced skills needed to evaluate evidence, validate security controls, conduct interviews, and determine whether organizations handling Controlled Unclassified Information (CUI) meet CMMC Level 2 requirements.
Experience Required	One of the following: • College degree in a cyber or information technical field, or • 2+ years of related education experience, or • 2+ years of related experience (including military) in a cyber, information technology, or assessment field	• Active CCP certification and 3+ years of cybersecurity experience • 1+ year of assessment or audit experience • One intermediate or advanced proficiency level for the Career Pathway Certified Assessor 612 from the DoD Manual 8140.3 Cyberspace Workforce Qualification and Management Program
Domain (%)	**Domain 1 -** CMMC Ecosystem (5%) **Domain 2 -** CMMC-AB Code of Professional Conduct (Ethics) (5%) **Domain 3 -** CMMC Governance and Source Documents (15%) **Domain 4 -** CMMC Model Construct and Implementation Evaluation (35%) **Domain 5 -** CMMC Assessment Process (CAP) (25%) **Domain 6 -** Scoping (15%)	**Domain 1 -** Evaluating Organizations Seeking Certification (OSC) Against CMMC Level 2 (15%) **Domain 2 -** CMMC Level 2 Assessment Scoping (20%) **Domain 3 -** CMMC Assessment Process (CAP) (25%) **Domain 4 -** Assessing CMMC Level 2 Practices (40%)
Exam Languages	English	English
Exam Length	3.5 hours (210 minutes); 170 multiple-choice questions	4 hours (240 minutes); 150 multiple-choice questions

Exam Fees

Exam registration fees are based on membership status at the time of exam registration:

- ISACA Member: US$575
- ISACA Nonmember: US$760

Exam registration fees are nonrefundable and nontransferable.

Resources

Below are some useful links and resources to help candidates learn more about the CCP and CCA certification exams.

CCP Certification

- CCP Exam Content Outline
- Prepare for the CCP Exam
- CCP Exam Information
- CCP Application Requirements
- CCP Maintenance Requirements

CCA Certification

- CCA Exam Content Outline
- Prepare for the CCA Exam
- CCA Exam Information
- CCA Application Requirements
- CCA Maintenance Requirements

Section II: Exam Registration and Scheduling

2.1 Before You Register

ISACA certification exams are computer-based and administered at authorized PSI testing centers globally or as remotely proctored exams. Exam registration is continuous, meaning candidates can register any time, with no restrictions. Candidates can schedule a testing appointment as early as 48 hours after payment of exam registration fees.

Upon registration, exam candidates have a six-month eligibility period. This means that from the date you register, you have six months to take the exam. It is important to note that the exam registration fee must be paid in full before you can schedule and take an exam.

If you need additional time to take the exam, you can purchase a six-month exam extension for US $75. The option to extend the exam eligibility will display on your dashboard 30 days before and after the expiration of your eligibility. When an exam is scheduled, the exam must be cancelled at least 48 hours prior to the exam date to extend the eligibility. There is a maximum of one extension on an exam.

Please be aware that the exam eligibility and registration fees will be forfeited in the event the candidate does not take the exam during the six-month eligibility period, if the testing appointment is missed, or if the candidate is more than 15 minutes late for a testing appointment.

2.2 Registering for the Exam

Exam registration must be completed online by following the steps below:

Step	Action
1.	Select your certification exam: CCP | CCA
2.	Log in or create an account. **Note**: If you are creating an account, please ensure your name is the same as what appears on your government-issued identification that you will present on exam day. See the 3.2 Exam Day Rules section for acceptable forms of ID. Before you register for the exam, it is important to verify there is a PSI test site with availability near you or have a compatible device for remote testing. To test your device, complete this compatibility check. If you are using a company device to take your exam, you may need your IT department's assistance or approval.
3.	Complete the registration process.

Please note: During the exam registration process, you will be required to accept ISACA's Terms of Use, section 16. Exams. Candidates must also accept the conditions set forth in this Candidate Guide, including those covering exam administration, certification rules, and the release of test results.

Candidates cannot schedule a testing appointment until exam registration fees are paid in full. Exam fees are **nonrefundable** and **nontransferable.**

Registration Acknowledgment

Candidates will receive a **Notification to Schedule** email within one (1) business day following registration and payment. This email provides information on 2.3 Scheduling the Exam Appointment.

Special Accommodations

Special testing accommodations must be requested during the registration process and approved by ISACA before scheduling the exam.

To request special testing accommodations, please follow the steps below:

Step	Action
1.	During the exam registration process, make sure to *check* the special accommodation requirement field.
2.	Print the Special Accommodation Request Form.
3.	Complete the Special Accommodation Request Form. **Note**: **This form must be completed by you and your healthcare professional.**
4.	Submit the form to ISACA at support.isaca.org.

Special accommodation requests will not be considered until exam registration fees are paid in full. All requests must be submitted to ISACA *no later than four (4) weeks* prior to your preferred exam date and are only valid for that one exam administration.

Registration Changes

There are three common registration changes that candidates request:

Type of Change	Steps
Name	The name on your ISACA account must match the name on the ID used to check in for your exam. To update your name: 1. Log in at www.isaca.org/myisaca. 2. Click on the red **MY ISACA PROFILE** button. 3. Make the necessary changes. 4. Click **Save.**
Exam Language	To change your preferred exam language: 1. Log in at https://www.isaca.org/myisaca/certifications. 2. Click the **Re-Schedule or Cancel Exam** link to proceed to PSI's scheduling page. 3. Follow the on-screen instructions to schedule your testing appointment. (The Scheduling Guide is available to help you schedule and reschedule.) **Note**: **If you need to change your exam language, you must also reschedule the testing appointment.** See Rescheduling an Exam for details.
Exam Type	To request a change to the exam type, contact ISACA Support immediately at support.isaca.org.

All change requests must be completed a minimum of 48 hours prior to your scheduled testing appointment.

2.3 Scheduling the Exam Appointment

Eligibility

Exam eligibility is required to schedule and take an exam. Eligibility is established at the time of exam registration and is good for six months.

Exam registration and payment are required before you can schedule and take an exam. Exam fees are nonrefundable and nontransferable.

You will forfeit your fees if you do not schedule and take the exam during your six-month eligibility period. No eligibility extensions are allowed without the purchase of an exam eligibility extension.

Exam Scheduling

There are five key steps to schedule an exam appointment:

Step	Action
1.	Log in to your ISACA account.
2.	Click **Certification & CPE Management**.
3.	Click **Schedule Your Exam** or **Visit Exam Website**. This will take you to the PSI dashboard.
4.	On the PSI dashboard, click **Schedule Exam.**
5.	Follow the step-by-step instructions in the Exam Scheduling Guide.

After scheduling the exam, you will receive a confirmation email from no-reply@psiexams.com confirming the exam appointment. Please view the Exam Scheduling Guide for additional assistance.

Exam appointments are only available 90 days in advance. If you do not see your exam site or date available more than 90 days in advance, please check back when it is closer to the desired exam date.

If you still do not see your desired exam site or date available, please verify that your exam eligibility has not expired by logging into your ISACA account and clicking the Certification & CPE Management tab.

Rescheduling an Exam

You can reschedule your exam any time during the eligibility period, without penalty, a minimum of 48 hours prior to the scheduled testing appointment. If you are within 48 hours of your scheduled testing appointment, you must take the exam or forfeit the registration fee. To reschedule an appointment, log into your ISACA account and follow the rescheduling steps outlined in the Exam Scheduling Guide.

Emergency Closing

Severe weather or an emergency could require canceling a scheduled exam. If this occurs, PSI will attempt to contact you by phone or email; however, ISACA suggests checking for test center closures by visiting www.psiexams.com. If the testing site is closed, the exam will be rescheduled at no additional charge.

Section III: Exam Preparation

3.1 Getting Ready for the Exam

Exam Questions

Exam questions are developed with the intent of measuring and testing practical knowledge and the application of general concepts and standards. All questions are designed with one best answer:

- Every question has a stem (question) and four options (answer choices).
- Choose the correct or best answer from the options.
- The stem may be in the form of a question or incomplete statement.

To learn more about the types of exam questions and how they are developed, review our Item Writing Requirements and Resources.

Exam Tips

- Read each question carefully. A question may require you to choose the answer based on a qualifier, such as MOST likely or BEST.
- Eliminate known incorrect answers and then make the best choice possible.
- A tutorial of the exam taking experience will be provided after logging onto the testing station before the start of the exam. Pay close attention to the tutorial so as not to miss important information.
- All questions should be answered.
- There are no penalties for incorrect answers. Grades are based solely on the total number of questions answered correctly, so do not leave any questions blank.

- Budget your time. Pace yourself to complete the entire exam. Candidates have 3.5 hours to complete the CCP exam and 4 hours to complete the CCA exam.

Exams at an In-Person Test Center

If your exam is scheduled at a test center, prepare before the day of the exam by:

- Locating the test center address and confirming the start time
- Mapping out your route to the testing center
- Planning to arrive at least 30 minutes prior to the exam start time
- Planning to store your personal belongings

See the 3.2 Exam Day Rules for more information.

Remotely Proctored Exams

For additional information about remotely proctored exams, download the Remote Proctoring Guide.

To test a device, complete the compatibility check prior to exam day. If you are using a company device to take the exam, you may need your IT department's assistance or approval to download the secure browser.

Identification Requirements

To enter the testing center or check in for your online exam, you must present an acceptable form of ID. An acceptable form of ID must be a current, valid, and original government-issued ID that contains:

- Candidate's name. The first and last name on the ID must match the name used to register for the exam, or you may not be permitted entry.
- Candidate's signature (driver's licenses issued in Japan without a signature are accepted)
- Candidate's photograph

All information must be demonstrated by a single form of ID (and cannot be a copy or handwritten). **Digital IDs and Military IDs are not accepted**. Any candidate who does not provide an acceptable form of ID will not be allowed to sit for the exam and will forfeit their registration fee.

Acceptable Forms of ID

Acceptable forms of ID include:

- Driver's license
- State ID card (nondriver's license)
- Passport
- Passport card
- Green card
- Alien registration
- Permanent resident card
- National ID card

The testing center reserves the right to ask for additional forms of ID for verification purposes. If there is any doubt surrounding your identity, you will be turned away from the test and ISACA will be notified. This will be considered a no-show, and you will forfeit your exam fees. To take the exam in the future, you will be required to register and pay the exam fee again.

3.2 Exam Day Rules

The exam rules are guidelines regarding what is acceptable during the exam. The exam rules apply for tests administered at PSI test center locations and remotely proctored exams. Upon registering for any ISACA exam, candidates must accept the Terms of Use. Per these terms, ISACA has the right to nullify exam scores if any unacceptable behaviors are identified.

Prohibited Items

During the exam, the candidate's workspace must be completely clear of all other items and materials. You will be required to face toward the screen for the duration of the exam so the proctors can properly monitor the exam session.

Candidates are prohibited from having the following items with them throughout the duration of the exam:

- Reference materials, study materials, paper, notes, notepads, language dictionaries, or other aids
- Calculators
- Multiple monitors
- Any type of communication, surveillance, or electronic/recording devices, including but not limited to:
  - Mobile phones
  - Tablets
  - Smart watches or glasses
  - Headphones/earbuds
- Baggage of any kind, including handbags, purses, or briefcases
- Weapons
- Tobacco products or vaping
- Food or beverages (this includes water and applies to both on-site and remotely proctored exams)
- Visitors

If candidates are seen with any such communication, surveillance, or electronic/recording devices during administration of the exam, their exam will be voided and they will be asked to immediately leave the exam site (if applicable). Candidates are not permitted to take screenshots or photos of any portion of the exam, including the exam results screen.

Storing Personal Items

Candidates should plan to store their personal items brought to the testing center in a locker or other designated area. You will not be able to access personal items until the exam is complete and submitted.

Unacceptable Behavior

Per the Terms of Use, the following activities are prohibited:

- Creating a disturbance
- Giving or receiving assistance using notes, papers, or other aids; use of unauthorized study materials
- Talking, reading the questions out loud, or moving your lips while reading silently
- Copying, photographing, recording, memorizing, or otherwise attempting to retain or recreate any exam content or assisting anyone in retaining, recreating, or reconstructing exam content for any purpose
- Attempting to take the exam for someone else or having someone else take the exam for you
- Possession of a communication, surveillance, or electronic/recording device, including but not limited to mobile devices, tablets, smart glasses, smart watches, etc.
- Attempting to sell, license, distribute, exchange, give away, share, comment on, disclose, or discuss, either directly or indirectly, any exam content to any person or entity before, during, or after the exam verbally, in writing, or through any other method of communication, including but not limited to the internet, email, or online forum
- Leaving the testing area without authorization. (These individuals will not be allowed to return to the testing room.) Two breaks, no longer than ten minutes each, are permitted with permission from your proctor. During the approved breaks, the exam will be paused, but the timer will not stop.
- Accessing items stored in the personal belongings area before the completion of the exam

Personal Hardship Guidelines

If you fail to arrive for a testing appointment due to a personal hardship, you may be able to reschedule without forfeiting the exam registration fee. To do this:

Step	Action
1.	Contact PSI no later than 72 hours following the scheduled appointment.
2.	Provide documentation to PSI to confirm the reason for your absence.

To contact PSI:

Step	Action
1.	Visit PSI Test Taker Support.
2.	Enter "ISACA" into the search field.
3.	Review and choose from the list of available contact numbers.

Examples of personal hardship include:

- Personal illness
    - Documentation such as a doctor's note, proof of an emergency room admittance, etc., is required:
        - Must be signed by a licensed doctor and include the date of the medical visit
        - Must include contact information for the licensed doctor
        - Does not need details about the illness or emergency
        - Should include indication from the doctor that the candidate should not take the exam due to the illness or emergency
- Death of an immediate family member, including a spouse, child/dependent, parent, grandparent, or sibling
    - Documentation must include the date of death, the deceased's name, and the candidate's relationship to the deceased
- Traffic accident
    - Documentation can include a police report or receipt from a mechanic or towing company, which includes the date and contact information

If a personal hardship request is denied, candidates are required to register and pay the full registration fee again.

Leaving the Testing Area

Candidates must gain authorization from the test proctor to leave the testing center. In the case of remotely proctored exams, they must gain authorization to leave the designated testing area. Leaving the testing center or area without authorization may result in your exam being terminated.

Two breaks are permitted with permission from your proctor. The exam will be paused, but the timer will not stop during the approved break.

Reason for Leaving	Directions
An emergency	• The exam will be paused temporarily. • Once it is confirmed as an emergency, the test will end.
To use the facilities	• You will be required to check out and check back in. • The exam time will not stop, and no extra time will be permitted. • Your breaks must be 10 minutes or less.

Consequences

If a candidate violates the Terms of Use or exam day rules or engages in any kind of misconduct, they will be subject to the following:

- Dismissal or disqualification
- Voiding of the exam
- Revocation of ISACA membership and any certifications currently held
- Banned from taking any ISACA exam

3.3 Exam Administration

The exam can be administered at a PSI testing center or remotely proctored.

PSI Testing Center

Your exam may be administered in a room with other test takers. Please note that some noise should be expected and is considered normal.

Here is a video of the PSI Test Center Experience.

3.4 Online Remote Proctoring

As mentioned, ISACA also offers the ability to take exams at home via online remote proctoring. Please review the Remote Proctoring Guide prior to taking an exam using this delivery modality.

Candidates can communicate with remote proctors in English using a live chat tool during the exam. Other languages are not available for communicating with remote proctors.

Here is a video of the PSI Online Remote Proctoring Experience.

Room Scan Instructions for Online Proctored Exams

Before your online proctored exam begins, you must complete a room scan as part of the check-in process. This step is mandatory and ensures compliance with exam security rules.

Here is what you will be asked to do:

- 360° room scan: Move your webcam to show all four walls of the room.
- Desk scan: Show your desk surface, including under your laptop or keyboard.
- Floor to ceiling scan: Starting from the floor beneath your test space, scan upwards to the ceiling.

For the room scan, you will have the following options:

1. External webcam scan
    - Connect an external webcam.
    - Move it around to show your room and desk as instructed by your check-in specialist.
2. Laptop camera with mirror scan
    - Use your laptop's built-in camera.
    - Hold a mirror (or use a mobile phone) to show the screen, keyboard, and all edges of your laptop.
    - The mirror check ensures that blind spots are visible to your check-in specialist.
    - If you use a mobile phone for this step, remove it from the testing area after the room scan check has been completed.
3. Mobile phone scan
    - You may use your mobile phone instead of a webcam.
    - Scan the QR code on your computer screen.
    - Allow camera access on your phone.
    - Follow your check-in specialist's instructions to show your room and desk.
    - Remove your phone from the testing area after the scan check has been completed.

Watch a short video explaining the online proctoring check-in process: PSI Check-In Process Video.

Exam Rules for Online Proctoring

The exam is online, closed book, and remotely proctored. The proctor will stop the exam if any of the exam rules are not followed. Any form of cheating will not be tolerated and will result in a voided exam without a refund.

More specifically, the following scenarios are NOT allowed during testing:

- Having someone else in the room during the exam, such as other people standing in, or walking through, the testing area
- Taking breaks, including stepping away without the proctor's permission
- Using a camera, recording device, or any other electronic device(s), including smart devices such as watches and glasses
- Taking screenshots of the computer screen and/or exam items
- Having reference materials present including papers, books, or notes in the workspace
- Using other programs or applications on your system, which includes viewing documents, browsing, remote access, or email access
- Reading exam questions out loud, talking to someone else in the room, or talking to yourself
- Copying or writing down exam content

- Covering the camera or moving away from the camera's view (please note that proctors will warn you if you make the slightest move out of camera view)
- Eating, drinking, or chewing gum
- Looking away from the computer screen

Note: Failure to comply with any of the above will result in your exam being voided and forfeiture of your exam fees. If you have any questions regarding these requirements, please contact the ISACA Customer Experience Center by visiting https://support.isaca.org.

ISACA will require a mirror check for each exam following a room scan. The purpose of the mirror check is to show the proctor the blind spots not captured during the room scan using a built-in webcam. A portable mirror or mobile phone may be used to complete the mirror check. During the mirror check, you will be required to hold the mirror up to the webcam and display the monitor/laptop screen, keyboard, and all four edges of the monitor/laptop screen. If you use a mobile phone, it will need to be placed out of reach of the room designated for testing after the mirror check is complete.

Section IV: After the Exam

This section covers exam scoring and applying for certification.

4.1 Exam Scoring

Receiving Your Score

Candidates will be able to view their preliminary passing status on screen immediately following the completion of the exam. You are not permitted to take screenshots or photos of any portion of the exam, including the exam results screen. The official score will be emailed and available online within ten (10) working days. If you have passed your exam, you will receive details on how to apply for certification.

- The email notification will be sent to the email address listed on your profile.
- Online results will be available on the MyISACA > Certifications & CPE Management page.
- Exam scores will not be provided by telephone or fax.
- Question-level results are not provided.

Scoring Criteria

Candidate scores are reported as a scaled score. A scaled score is a conversion of a candidate's raw score on an exam to a common scale. The purpose of a scaled score is to ensure that a standard way of reporting outcomes is used across disparate versions of the exam so that different versions are comparable and fair.

ISACA uses and reports scores on a common scale from 200 to 800. ISACA exams are comprised of scored items as well as pretest items. Pretest items are not used to calculate exam scores. Review the points below to identify the lowest, passing, and perfect scores:

- A score of 800 represents a perfect score with all questions answered correctly.
- A score of 200 represents the lowest score possible and signifies only a small number of questions were answered correctly.
- Candidates must receive a score of 450 or higher to pass the exam, which represents the minimum standard of knowledge.
- Domain-level results are provided for informational purposes only. Exam scores are based on the total number of exam items answered correctly, regardless of domain. Domain-specific percentages indicate the portion of the exam that reflects that domain content and are not used to calculate exam scores.
- A candidate who receives a passing score can apply for certification if all other requirements are met (see How to Become Certified for more details).

Requests for Rescoring

While ISACA is confident in the integrity and validity of our scoring procedures, you may request a rescore if you do not pass the exam. Rescores are performed by PSI.

Candidates must submit a rescore request in writing through the ISACA support page within 30 days following the release of the exam results:

- Requests for a rescore after 30 days will not be processed.
- All requests must include a candidate's name, ISACA ID number, and mailing address.
- A fee of US$75 must accompany each request.

4.2 Retake Policy

To protect the integrity of ISACA's certification exams, ISACA has implemented the following retake policy.

Individuals have four (4) attempts within a rolling 12-month period to pass the exam. Those that do not pass on their first attempt are allowed to retake the exam a total of three (3) more times within 12 months from the date of the first attempt. **Please note that candidates must pay the registration fee in full for each exam attempt.**

As an example, after taking and not passing the exam (attempt 1):

- Retake 1 (attempt 2): Candidates must wait 30 days from the date of the first attempt.
- Retake 2 (attempt 3): Candidates must wait 90 days after the date of the second attempt.
- Retake 3 (attempt 4): Candidates must wait 90 days after the date of the third attempt.

Individuals who pass the exam are restricted from taking the same exam within the application time period of one (1) year.

Certification holders are restricted from taking the same certification exam while they are certified.

4.3 Post-Exam Feedback

Candidates will have the opportunity to provide feedback after completing the exam via a post-exam survey. Your feedback is used to improve the testing experience and the quality of the exam questions.

Concerns About Exam Administration

Candidates may provide comments and concerns about the exam administration, including exam day issues, site conditions, or the content of the exam by contacting ISACA within 48 hours of the conclusion of the test. To submit comments:

Step	Action
1.	Contact ISACA support.
2.	Provide the following information in your comments: • ISACA ID number • Testing center location • Date and time tested • Any relevant details on the specific issue
3.	ISACA will review comments regarding exam day issues and site concerns prior to the release of the official score report.

ISACA does not reissue scores based on question updates. Our subject matter experts use these comments to improve future examinations.

4.4 Certification

How to Become Certified

Taking and passing an ISACA certification exam is only one part of becoming certified. To become certified, an individual must first meet the following requirements:

Step	Action
1.	Complete mandatory training from an approved training provider or ISACA.
2.	Successfully pass the certification exam.
3.	For CCP pay the US$200 application processing fee. For CCA pay the US$50 application processing fee.
4.	Submit an application to demonstrate the experience requirements.
5.	Hold at least one intermediate or advanced proficiency level for the Career Pathway Certified Assessor 612 from the DoD Manual 8140.3 Cyberspace Workforce Qualification and Management Program (CCA only).
6.	Have a Tier 3 determination from DOW.
7.	Adhere to the Code of Professional Ethics.
8.	Adhere to the Continuing Professional Education (CPE) Policy.

Candidates have one (1) year from passing the exam to apply for certification. Additional resources include:

- Pass the examination: CCP | CCA
- For CCP pay the US$200 application processing fee. For CCA pay the US$50 application processing fee.
- Submit the application for certification: CCP | CCA
- Adhere to ISACA's Code of Professional Ethics, Terms of Use, and Privacy Notice
- Adhere to the CPE Policy: CCP | CCA

ISO/IEC 17024:2012 Compliant

The ANSI National Accreditation Board (ANAB) has accredited the CCP and CCA certifications under ISO/IEC 17024:2012 *General Requirements for Bodies Operating Certification Systems of Persons*.

Accreditation by ANAB signifies that ISACA's procedures meet ISO's requirements for openness, balance, consensus, and due process.

The accreditation details are as follows:

ANAB Accredited Program

PERSONNEL CERTIFICATION #0694

ISO/IEC 17024:2012

CCP, CCA, CISA, CISM, CGEIT, and CRISC Program Accreditation

ANAB is a private, nonprofit organization that accredits other organizations to serve as third-party product, system, and personnel certifiers.

ISO/IEC 17024 specifies the requirements to be followed by organizations certifying individuals against specific requirements.

ANAB describes ISO/IEC 17024 as "expected to play a prominent role in facilitating global standardization of the certification community, increasing mobility among countries, enhancing public safety and protecting consumers."

Appendix A: CCP Examination Content

This exam will verify a candidate's knowledge of the CMMC, relevant supporting materials, and applicable legal and regulatory requirements to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). The exam will also assess the candidate's understanding of the CMMC ecosystem. A passing score on this exam is a prerequisite to Certified CMMC Assessor and Certified CMMC Instructor certifications. The Department of War (DOW) is the authoritative source for CMMC documentation, which can be found here: https://dodcio.defense.gov/CMMC/Documentation/.

Intended Audience

- Employees of organizations seeking CMMC 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

Exam Prerequisites

- College degree in a cyber or information technical 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
- Complete Certified CMMC Professional Class offered by an Approved Training Provider (ATP)

Exam Specifications

- Number of questions: 170
- Types of questions: Multiple choice
- Length: 3.5 hours
- Passing score: 450 points
- Not an open book exam

Domains

Upon successful completion of this exam, the candidate will be able to apply skills and knowledge to the below domains.

Domain	Exam Weight
1. CMMC Ecosystem	5%
2. CMMC-AB Code of Professional Conduct (Ethics)	5%
3. CMMC Governance and Sources Documents	15%
4. CMMC Model Construct and Implementation Evaluation	35%
5. CMMC Assessment Process (CAP)	25%
6. Scoping	15%

Domain 1: CMMC Ecosystem

Task 1. Identify and compare roles/responsibilities/requirements of authorities across the CMMC ecosystem.

1. Authorities

a) Office of the Undersecretary of Defense (OUSD)

1. Cybersecurity standards and best practices and knowledge of how to map these controls and processes across several levels that range from basic to advanced cyber hygiene

2. Regulation (DFARS 252.204-7012) that is based on trust by adding a verification component with respect to cybersecurity requirements

b) CMMC ecosystem (and the different types of entities participating in it)

1. Cybersecurity Maturity Model Certification Accreditation Body (CMMC-AB)

(a) Organizations

1. Organizations Seeking Certification (OSC)

1. Purpose, requirements, and benefits of OSC involvement in the ecosystem

2. CMMC Third-Party Assessment Organizations (C3PAO)

3. Registered Provider Organizations (RPO)

1. Requirements and benefits of RPO

(b) Individuals

1. Registered Practitioner (RP)

1. RPs in the CMMC ecosystem provide advice, consulting, and recommendations to their clients. They are the implementers and consultants, but do not participate in Certified CMMC Assessments.

2. CMMC Assessors and Instructors Certification Organization (CAICO)

a) Organizations

1. Licensed Partner Publishers (LPP)

1. Purpose, requirements, and benefits of LPPs

2. Licensed Training Providers (LTP)

1. Purpose, requirements, and benefits of LTPs

b) Individuals

1. Provisional Assessors (PA)

1. Purpose, requirements, and benefits of PAs

2. Timeline for sunsetting

2. Provisional Instructors (PI)

1. Purpose, requirements, and benefits of PIs

2. Timeline for sunsetting

3. Certified CMMC Professional (CCP)

1. Purpose, requirements, and benefits of CCPs active involvement in the ecosystem

2. Timeline for CCP certification and assessments

4. Certified CMMC Assessor (CCA)

1. Purpose, requirements, and benefits of CCAs active involvement in the ecosystem

2. Timeline for CCA certification and assessments

5. Certified CMMC Instructor (CCI)

1. Purpose, requirements, and benefits of CCIs active involvement in the ecosystem

2. Timeline for CCI certification and assessments

6. Assessment Team Member

1. CCP and CCA roles on the Assessment Team

7. CMMC Lead Assessor

1. Lead Assessor role on the Assessment Team

2. Timeline for Lead Assessor certification

Domain 2: CMMC-AB Code of Professional Conduct (Ethics)

Task 1. Identify and apply knowledge of the guiding principles and practices of the CMMC-AB Code of Professional Conduct (CoPC)/ISO/IEC/DOW requirements.

1. General Ethics Topics

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

3. ISO/IEC

4. Department of War (DOW) Requirements

5. Professionalism

6. Objectivity

7. Confidentiality

8. Proper Use of Methods

9. Information Integrity

10. Conflicts of Interest

11. Respect for Intellectual Property

12. Lawful and Ethical Practices

13. Contracts and Nondisclosure Agreements

Domain 3: CMMC Governance and Source Documents

Task 1. Demonstrate understanding of Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) in nonfederal unclassified networks.

1. Current Department of War (DOW) Defense Industrial Base (DIB) Cybersecurity Efforts, Regulations, and Executive Orders Pertaining to the CMMC Program

a) Part 32 of the Code of Federal Regulations (CFR)

b) Defense Federal Acquisition Regulation Supplement (DFARS) in Part 48 of the CFR

c) DFARS Clause 252.204-7012

1. National Institute of Standards and Technology (NIST) SP 800-171

2. Technical data (DFARS 252.227-7013)

3. FedRAMP

2. CMMC Framework Tenets

a) Key aspects of CMMC v.2.0 program requirements

1. Streamlined model

1. Focused on the most critical requirements

2. Aligned with widely accepted standards

2. Reliable assessments

1. Reduced assessment costs

2. Higher accountability

3. Flexible implementation

1. Spirit of collaboration

2. Added flexibility and speed

b) Rulemaking and timeline for CMMC v2.0

1. Incentives, assessments, and 9 to 24-month rulemaking

c) Levels of CMMC assessments and requirements

1. Foundational/Level 1 (same as previous CMMC v1.0 Level 1)

1. FAR Clause 52.204-21

1. Provide overview of the 17 basic safeguarding requirements and how procedures are applied within the CMMC Level 1/Level 2 practices/assessment framework.

2. Advanced/Level 2 (previous Level 3)

2. NIST SP 800-171 (requirements)

1. Provide overview of the 110 NIST SP 800-171 requirements and how they are applied within the CMMC Level 2 practices/assessment framework.

d) Self-assessments versus third-party assessments

1. Define different criteria for various assessment type under CMMC v2.0 framework.

3. Consequences of Noncompliance

a) Failure to receive an award of contract

b) Contractual liability

c) False Claims Act

1. US Department of Justice

1. Civil Cyber-Fraud Initiative

Task 2. Determine the appropriate roles/responsibilities/authority for FCI and CUI.

1. Importance of Data Classification, Collection, and Analysis

a) CUI basic versus specified

2. Contractor Sensitive Data Categories

a) Federal Contract Information (FCI)

1. Section 4.1901 of the Federal Acquisition Regulation (FAR)

b) Controlled Unclassified Information (CUI)

1. Part 2002 of Title 32 CFR, 2002.4(h)

3. Government Authority for Identifying and Marking CUI

a) Executive Order 13556

b) 32 Code of Federal Regulations, Part 2002 (Implementing Directive)

c) DoD Instruction (DoDI) 5200.48, Controlled Unclassified Information (CUI)

4. Contractor/Authorized Holders Responsibilities in Handling CUI

a) DoDI 5200.48

b) Part 2002 of Title 32 CFR

Task 3. Demonstrate understanding of the CMMC source and supplementary documents.

1. CMMC Source Documents

a) CMMC Model Overview

b) CMMC Level 1 Assessment Guide

c) CMMC Level 2 Assessment Guide

d) CMMC Level 1 Scoping Guidance

e) CMMC Level 2 Scoping Guidance

f) CMMC Assessment Process (CAP)

g) CMMC Glossary

h) CMMC Artifact Hashing Tool User Guide

2. Information Security Oversight Office (ISOO) CUI Registry

a) NARA administers the CUI Registry

1. Types of labeled information on documents such as:

1. Export Controlled (SP-EXPT)

2. Specified marking/labeling using NARA CUI Marking Handbook

3. DoD CUI Registry

a) Types of labeled information on documents such as:

1. Naval Nuclear Propulsion Information (NNPI)

2. NNPI marking/labeling using DoD CUI Marking Aid

Domain 4: CMMC Model Construct and Implementation Evaluation

Task 1. Given a scenario, apply the appropriate CMMC source documents as an aid to evaluate the implementation/ review of CMMC practices. (At a minimum CCP candidate must be evaluated on CMMC L1 Practices during CCP exam.)

1. Model Architecture

2. Model Levels

a) Cumulative nature

b) Characteristics

c) Levels required for specific contracts

1. Level 1

2. Level 2

3. Practices

a) Practice descriptions

1. Practice numbering scheme

2. Objectives

3. Assessment methods and objects

4. Domains

a) Access Control (AC)

1. AC.L1-3.1.1 Authorized Access Control

2. AC.L1-3.1.2 Transaction and Function Control

3. AC.L1-3.1.20 External Connections

4. AC.L1-3.1.22 Control Public Information

b) Audit and Accountability (AU)

c) Awareness and Training (AT)

d) Configuration Management (CM)

e) Identification and Authentication (IA)

1. IA.L1-3.5.1 Identification

2. IA.L1-3.5.2 Authentication

f) Incident Response (IR)

g) Maintenance (MA)

h) Media Protection (MP)

1. MP.L1-3.8.3 Media Disposal

i) Personnel Security (PS)

j) Physical Protection (PE)

1. PE.L1-3.10.1 Limit Physical Access

2. PE.L1-3.10.3 Escort Visitors

3. PE.L1-3.10.4 Physical Access Logs

4. PE.L1-3.10.5 Manage Physical Access

k) Risk Assessment (RA)

l) Security Assessment (CA)

m) System and Communications Protection (SC)

1. SC.L1-3.13.1 Boundary Protection

2. SC.L1-3.13.5 Public-Access System Separation

n) System and Information Integrity (SI)

1. SI.L1-3.14.1 Flaw Remediation

2. SI.L1-3.14.2 Malicious Code Protection

3. SI.L1-3.14.4 Update Malicious Code Protection

4. SI.L1-3.14.5 System and File Scanning

Task 2. Apply knowledge of the CMMC assessment criteria and methodology to the appropriate CMMC practices.

1. Practice Definitions

2. Assessment Objectives

3. Assessment Methods (Examine, Interview, and Test)

4. Information for Practice Discussion

5. Key References and Their Applicability to the Practices

a. Navigating and using the CMMC Assessment Guide(s) content

b. Determining the assessment method(s) that would be best for gathering sufficient and accurate evidence

Task 3. Analyze the adequacy/sufficiency around the location/collection/quality/usage of evidence.

1. Appraised Evidence

2. Measuring Evidence

Domain 5: CMMC Assessment Process

Task 1. Choose the appropriate roles of the CCP in the CMMC Assessment Process when developing the assessment plan (Phase 1 Plan and Prepare Assessment).

1. Validation criteria of OSC s assessment evidence

2. Analyzing the CMMC practice requirements

3. What needs to be included in a CMMC Assessment Plan

4. The CMMC Readiness Review Process

Task 2. Apply CMMC Assessment Process requirements pertaining to the role of the CCP as an Assessment Team Member while conducting a CMMC assessment (Phase 2 Conduct Assessment).

1. How to assist/support the Assessment Team during an assessment

2. The three possible assessment methods (Examine, Interview, and Test) and scoring evidence successfully for each practice

3. Communication skills to interview or observe tests/demonstrations for assessment practices

4. How Assessment Team Members rate practices and validate preliminary results

5. How Assessment Team Members assist in the preparation of final findings

6. How to score practices that are on a plan of action and milestone (POA&M)

Task 3. Demonstrate comprehension of the CCP role in the preparation of assessment report (Phase 3 Report Assessment Results).

1. The evidence presented for each practice

2. How Assessment Team Members score practices, validate, and deliver assessment preliminary results

3. How the Assessment Lead drafts and scores the final findings

4. How the final findings and associated information are incorporated into the Assessment Report

5. How the Lead Assessor submits the assessment report, including the review process, submitting to the C3PAO and the OSC

6. How to package and archive the assessment results for a record to support any future questions that maybe asked

Task 4. Demonstrate comprehension of the CCP role in the process of evaluating outstanding assessment issues on plan of action and milestones (POA&M) (Phase 4 Evaluation of Outstanding Assessment POA&M Items).

1. Evaluation of Assessment POA&M Items

a) DoD assessment methodology, POA&M scoring criteria

1. Minimum assessment score

2. Qualifying POA&M items

b) CMMC AG CA.L2-3.12.2, Plan of action objectives and requirements

Task 5. Given a scenario, determine the appropriate phases/steps to assist in the preparation/conducting/reporting on a CMMC Level 2 Assessment.

1. Plan and Prepare Assessments

a) CMMC CCP must be able to assist in analyzing requirements.

b) CMMC CCP must be able to assist in developing assessment plan.

c) CMMC CCP must be able to assist in verifying readiness to conduct assessment.

2. Conduct Assessment

a) CMMC CCP must be able to assist in collecting and examining evidence.

b) CMMC CCP must be able to assist in scoring practices and validating preliminary results.

c) CMMC CCP must be able to assist in generating final assessment results.

3. Report Recommended Assessment Results

a) CMMC CCP must be able to assist in delivering recommended assessment results.

4. Remediate Outstanding Assessment Issues

a) Awareness of the CCP s role in the POA&M process

Domain 6: Scoping

Task 1. Understand CMMC high-level scoping as described in the CMMC Assessment Process.

1. Defining Organizational Scoping

a) Organization

b) Host unit

c) Supporting units

Task 2. Given a scenario, analyze the organization environment to generate an appropriate scope for FCI Assets.

1. Defining FCI Data in the Form of Assets

a) Process

b) Store

c) Transmit

2. Out-of-Scope Assets

3. Specialized Assets

a) Government property

b) Internet of Things (IoT)/Industrial Internet of Things (IIoT)

c) Operational technology (OT)

d) Restricted information systems

e) Test Equipment

4. Scoping Activities

a) People

b) Technology

c) Facilities

d) External service providers (ESPs)

Appendix B: CCA Examination Content

This exam will verify a candidate's readiness to perform as an effective Certified Assessor of Organizations Seeking Certification (OSC) at CMMC Level 2. A passing score on this exam is a prerequisite to a CMMC Lead Assessor designation. The Department of War (DOW) is the authoritative source for CMMC documentation, which can be found here: The Department of War (DOW) is the authoritative source for CMMC documentation, which can be found here: https://dodcio.defense.gov/CMMC/Documentation/.

Intended Audience

- Certified CCPs seeking to advance to CCA
- Certified CCIs who wish to teach the CCA course

Exam Prerequisites

- College degree in a cyber or information technical 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
- Complete Certified CMMC Professional Class offered by an Approved Training Provider (ATP)

Exam Specifications

- Number of questions: 150
- Types of questions: Multiple choice
- Length: 4 hours
- Passing score: 450 points
- Not an open book exam

Domains

Upon successful completion of this exam, the candidate will be able to apply skills and knowledge to the below domains.

Domain	Exam Weight
1. Evaluating Organizations Seeking Certification (OSC) Against CMMC Level 2	15%
2. CMMC Level 2 Assessment Scoping	20%
3. CMMC Assessment Process (CAP)	25%
4. Assessing CMMC Level 2 Practices	40%

Domain 1: Evaluating Organizations Seeking Certification (OSC) Against CMMC Level 2

Task 1. Assess the various environmental considerations of Organizations Seeking Certification (OSCs) against CMMC Level 2 practices.

1. The Difference Between Logical (Virtual) and Physical Locations

2. The Difference Between Professional and Industrial Environments

3. Single and Multisite Environmental Constraints and Evidence Requirements

4. Cloud and Hybrid Environment Constraints and Evidence Requirements

5. On-Premises Environmental Constraints

6. Environmental Exclusions for a Level 2 CMMC Assessment

Domain 2: Scoping

Task 1. Analyze the CMMC assessment scope of Controlled Unclassified Information (CUI) assets as they pertain to a CMMC assessment using the five categories of CUI assets as defined in the CMMC Level 2 Assessment Scoping Guide.

1. Categorization of CUI Data in the Form of Assets in Scope

a) CUI assets

1. Process, store, or transmit CUI

b) Security protection assets

1. Assets that provide security functions and capabilities to contractor s CMMC assessment scope

c) Contractor risked managed assets

1. Assets that can, but are not intended to, process, store, or transmit CUI because of security policy, procedures, and practices in place

d) Specialized assets

1. Assets that may/may not process, store, or transmit CUI

2. Assets include government property, Internet of Things (IoT) devices, operational technology (OT), restricted information systems, and test equipment

e) Out-of-scope assets

1. Assets that cannot process, store, or transmit CUI

Task 2. Given a scenario, analyze the CMMC assessment scope based on the predetermined CUI categories within the CMMC Level 2 Assessment Scoping Guide.

1. CMMC Assessment Asset Categories (In-Scope)

a) CUI assets

b) Security protection assets

c) Contractor risked managed assets

d) Specialized assets

2. CMMC Assessment Asset Categories (Out-of-Scope)

3. Separation Techniques

a) Logical separation

1. Firewalls

2. Virtual local area networks (VLANs)

b) Physical separation

1. Gates

2. Locks

3. Badge access

4. Guards

Task 3. Evaluate the CMMC assessment scope considerations based on the CMMC Level 2 Assessment Scoping Guide.

1. FCI and CUI Within the Same Assessment Scope

a) Contractor defines FCI/CUI assets (in-scope); CMMC Assessor certifies implementation of Level 1 and 2 practices.

2. FCI and CUI Not Within the Same Assessment Scope

a) Contractor defines self-assessment of FCI assets (in-scope).

b) Contractor defines CUI assets (in-scope); CMMC Assessor certifies implementation of Level 1 and 2 practices.

3. External Services Providers

a) Evaluation of responsibility matrix

b) Nonduplication

c) Agreements, service level agreements (SLAs)

Domain 3: CMMC Assessment Process (CAP) v5.X

Task 1. Given a scenario, apply the appropriate phases and steps to plan, prepare, conduct, and report on a CMMC Level 2 Assessment.

1. Phase 1 Plan and Prepare Assessments

a) Analyze requirements.

b) Develop assessment plan.

c) Verify readiness to conduct assessment.

2. Phase 2 Conduct Assessment

a) Collect and examine evidence.

b) Score practices and validate preliminary results.

c) Generate final recommended assessment results.

3. Phase 3 Report Recommended Assessment Results

a) Deliver recommended assessment results.

Domain 4: CMMC Level 2 Practices

Task 1. Identify evidence verification/validation methods and objects for practices based on the CMMC Level 2 Assessment Guide and CMMC Assessment Process (CAP) documentation.

1. Methods and Objects for Determining Evidence

a) Examine

b) Interview

c) Test

2. Adequacy and Sufficiency Related to Evidence

a) Characteristics of acceptable evidence

b) Evidence of enabling persistent and habitual application of practices

1. Policy

2. Plan

3. Resourcing

4. Communication

5. Training

c) Characterization of evidence

1. Validation that evidence effectively meets intent of standard

2. An objective and systematic examination of evidence for the purpose of providing an independent assessment of the performance of CMMC

3. CMMC Level 2 Assessment Practice Objectives

a) Access Control (AC)

1. AC.L2-3.1.3 Control CUI Flow

2. AC.L2-3.1.4 Separation of Duties

3. AC.L2-3.1.5 Least Privilege

4. AC.L2-3.1.6 Nonprivileged Account Use

5. AC.L2-3.1.7 Privileged Functions

6. AC.L2-3.1.8 Unsuccessful Logon Attempts

7. AC.L2-3.1.9 Privacy and Security Notices

8. AC.L2-3.1.10 Session Lock

9. AC.L2-3.1.11 Session Termination

10. AC.L2-3.1.12 Control Remote Access

11. AC.L2-3.1.13 Remote Access Confidentiality

12. AC.L2-3.1.14 Remote Access Routing

13. AC.L2-3.1.15 Privileged Remote Access

14. AC.L2-3.1.16 Wireless Access Authorization

15. AC.L2-3.1.17 Wireless Access Protection

16. AC.L2-3.1.18 Mobile Device Connection

17. AC.L2-3.1.19 Encrypt CUI on Mobile

18. AC.L2-3.1.21 Portable Storage Use

b) Awareness and Training (AT)

1. AT.L2-3.2.1 Role-Based Risk Awareness

2. AT.L2-3.2.2 Role-Based Training

3. AT.L2-3.2.3 Insider Threat Awareness

c) Audit and Accountability (AU)

1. AU.L2-3.3.1 System Auditing

2. AU.L2-3.3.2 User Accountability

3. AU.L2-3.3.3 Event Review

4. AU.L2-3.3.4 Audit Failure Alerting

5. AU.L2-3.3.5 Audit Correlation

6. AU.L2-3.3.6 Reduction and Reporting

7. AU.L2-3.3.7 Authoritative Time Source

8. AU.L2-3.3.8 Audit Protection

9. AU.L2-3.3.9 Audit Management

d) Configuration Management (CM)

1. CM.L2-3.4.1 System Baselining

2. CM.L2-3.4.2 Security Configuration Enforcement

3. CM.L2-3.4.3 System Change Management

4. CM.L2-3.4.4 Security Impact Analysis

5. CM.L2-3.4.5 Access Restrictions for Change

6. CM.L2-3.4.6 Least Functionality

7. CM.L2-3.4.7 Nonessential Functionality

8. CM.L2-3.4.8 Application Execution Policy

9. CM.L2-3.4.9 User-Installed Software

e) Identification and Authentication (IA)

1. IA.L2-3.5.3 Multifactor Authentication

2. IA.L2-3.5.4 Replay-Resistant Authentication

3. IA.L2-3.5.5 Identifier Reuse

4. IA.L2-3.5.6 Identifier Handling

5. IA.L2-3.5.7 Password Complexity

6. IA.L2-3.5.8 Password Reuse

7. IA.L2-3.5.9 Temporary Passwords

8. IA.L2-3.5.10 Cryptographically-Protected Passwords

9. IA.L2-3.5.11 Obscure Feedback

f) Incident Response (IR)

1. IR.L2-3.6.1 Incident Handling

2. IR.L2-3.6.2 Incident Reporting

3. IR.L2-3.6.3 Incident Response Testing

g) Maintenance (MA)

1. MA.L2-3.7.1 Perform Maintenance

2. MA.L2-3.7.2 System Maintenance Control

3. MA.L2-3.7.3 Equipment Sanitization

4. MA.L2-3.7.4 Media Inspection

5. MA.L2-3.7.5 Nonlocal Maintenance

6. MA.L2-3.7.6 Maintenance Personnel

h) Media Protection (MP)

1. MP.L2-3.8.1 Media Protection

2. MP.L2-3.8.2 Media Access

3. MP.L2-3.8.4 Media Markings

4. MP.L2-3.8.5 Media Accountability

5. MP.L2-3.8.6 Portable Storage Encryption

6. MP.L2-3.8.7 Removeable Media

7. MP.L2-3.8.8 Shared Media

8. MP.L2-3.8.9 Protect Backups

i) Personnel Security (PS)

1. PS.L2-3.9.1 Screen Individuals

2. PS.L2-3.9.2 Personnel Actions

j) Physical Protection (PE)

1. PE.L2-3.10.2 Monitor Facility

2. PE.L2-3.10.6 Alternative Work Sites

k) Risk Assessment (RA)

1. RA.L2-3.11.1 Risk Assessments

2. RA.L2-3.11.2 Vulnerability Scan

3. RA.L2-3.11.3 Vulnerability Remediation

l) Security Assessment (CA)

1. CA.L2-3.12.1 Security Control Assessment

2. CA.L2-3.12.2 Plan of Action

3. CA.L2-3.12.3 Security Control Monitoring

4. CA.L2-3.12.4 System Security Plan

m) System and Communications Protection (SC)

1. SC.L2-3.13.2 Security Engineering

2. SC.L2-3.13.3 Role Separation

3. SC.L2-3.13.4 Shared Resource Control

4. SC.L2-3.13.6 Network Communication by Exception

5. SC.L2-3.13.7 Split Tunneling

6. SC.L2-3.13.8 Data in Transit

7. SC.L2-3.13.9 Connections Termination

8. SC.L2-3.13.10 Key Management

9. SC.L2-3.13.11 CUI Encryption

10. SC.L2-3.13.12 Collaborative Device Control

11. SC.L2-3.13.13 Mobile Code

12. SC.L2-3.13.14 Voice over Internet Protocol

13. SC.L2-3.13.15 Communications Authenticity

14. SC.L2-3.13.16 Data at Rest

n) System and Information Integrity (SI)

1. SI.L2-3.14.3 Security Alerts and Advisories

2. SI.L2-3.14.6 Monitor Communications for Attacks

3. SI.L2-3.14.7 Identify Unauthorized Use