GUIDE

Redspin®
A Division of Clearwater

# Preparing for Your CMMC Interview: Commonly Asked Questions – Maintenance Edition

This domain focuses on the health and servicing of our critical systems, much like a routine health check-up or scheduled car service. It requires consistent upkeep, servicing, and updating of an organization's systems, hardware, and software to ensure optimal functionality. This regular maintenance can help to detect and resolve minor issues before they escalate, and is performed through periodic assessment and updating of systems, such as patching vulnerabilities, such that the organization may guard against exploitation of known or emerging vulnerabilities.

# TABLE OF CONTENTS

**Key**

- ● Domain Family
- ● Identifier
- ◐ Basic | Derived
- ● Security Requirement

## Security Requirement Table of Contents

## Maintenance

As you prepare for your organization's assessment, it's important to understand what to expect during the interview process. Individuals can anticipate a range of questions that will be both comprehensive and reflective of several key areas intended to assure that the controls are implemented correctly and performing as expected. Interview sessions typically follow a basic pattern to help inform this decision. Below is an example interview session construct. Though not all inclusive these guides provide typical questions asked during an assessment.

**Typical Question Format:**

**Policy and Procedures:**

- How does your organization's security policy address the encryption of Controlled Unclassified Information (CUI) on mobile devices and platforms?
- Can you provide documentation or guidelines that mandate encryption on mobile devices and platforms when handling CUI?

**Implementation:**

- What encryption standards or protocols does your organization use for CUI on mobile devices?
- Are there specific mobile device management (MDM) or mobile application management (MAM) tools in place to enforce encryption on mobile devices and platforms?
- How do you ensure that all mobile devices used within the organization have encryption enabled?

**Monitoring and Auditing:**

- How do you monitor and verify that CUI remains encrypted on mobile devices and platforms?
- Are there any auditing mechanisms in place to check for devices that might have encryption disabled or bypassed?
- Can you provide recent audit logs or reports showing encryption checks for mobile devices?

**Incident Handling:**

- Have there been any incidents where CUI was found unencrypted on a mobile device? If so, how was it handled?
- What are the consequences or actions taken against users who fail to encrypt CUI on their mobile devices?

**Training and Awareness:**

- How are employees made aware of the importance of encrypting CUI on mobile devices?
- Is there a specific training module or awareness campaign focused on mobile device encryption?

**Technical:**

- Can you demonstrate the encryption settings on a sample mobile device used within the organization?
- Are there any exceptions or scenarios where CUI might not be encrypted on mobile devices, and how are these exceptions handled?

**Third-party and BYOD:**

- How does your organization ensure that third-party vendors or contractors adhere to this encryption requirement when accessing CUI on mobile devices?
- If you have a Bring Your Own Device (BYOD) policy, how do you ensure that personal devices encrypt CUI?

## Maintenance

## MA.L2-3.7.1

## Basic

## Perform maintenance on organizational systems.

- How frequently do you perform system maintenance?
- Describe the process for scheduling and announcing planned maintenance activities.
- What tools or platforms do you use for system maintenance?
- How do you ensure that maintenance activities do not inadvertently introduce vulnerabilities?
- How do you manage and track third-party vendors or contractors involved in system maintenance?
- Are there specific protocols or procedures for maintenance on critical or high-security systems?
- How do you handle unscheduled or emergency maintenance requirements?
- How do you test systems post-maintenance to ensure their functionality and security?
- What documentation or logging is generated for each maintenance activity, and how is it stored?
- How do you manage system backups or data integrity during maintenance activities?
- What training or certification do maintenance personnel undergo to ensure they adhere to security standards?
- How do you integrate system maintenance with other security protocols, like vulnerability management or incident response?
- Describe any challenges or issues you've faced during system maintenance and how they were addressed.
- How do you notify stakeholders or users about maintenance activities, especially if there might be system downtime?
- How do you ensure that third-party software or tools used during maintenance are secure and compliant with organizational standards?
- Are there automated mechanisms in place to monitor and report on system health and potential maintenance needs?
- How do you validate the success and effectiveness of maintenance activities?
- How do you review and refine maintenance protocols based on feedback or post-maintenance assessments?
- Are there periodic security audits or assessments specifically targeting maintenance activities and their impact on system security?
- How do you ensure that the approach to system maintenance aligns with NIST guidelines and broader cybersecurity objectives?

## Maintenance

## MA.L2-3.7.2

## Basic

## Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

- What controls are in place to ensure only authorized tools are used for system maintenance?
- How do you vet and approve techniques or mechanisms employed during system maintenance?
- Describe the authentication and authorization processes in place for personnel conducting system maintenance.
- How do you ensure that third-party maintenance tools adhere to your organization's security controls?
- What logging or auditing capabilities are in place to track system maintenance activities?
- How do you control and monitor remote system maintenance activities?
- Are there specific protocols or controls for maintenance activities on critical or sensitive systems?
- How do you ensure the timely patching or updating of maintenance tools to address known vulnerabilities?
- Describe any encryption or security measures employed during data transfer for maintenance activities.
- How do you handle the storage and disposal of data or logs generated during system maintenance?
- How do you train and educate maintenance personnel on security best practices and protocols?
- Are there periodic security assessments or audits to validate the controls on system maintenance tools and techniques?
- How do you handle exceptions or emergency maintenance requirements in terms of security controls?
- How do you ensure that maintenance activities do not inadvertently introduce new vulnerabilities or risks?
- What controls are in place to restrict or monitor the installation of third-party or unauthorized software during maintenance?
- How do you manage feedback or concerns related to system maintenance from other departments or stakeholders?
- How do you stay updated on industry best practices or recommendations related to secure system maintenance?
- Describe any challenges or issues you've faced related to controlling system maintenance activities and how they were addressed.
- How do you ensure that third-party vendors or partners adhere to your organization's maintenance control standards?

- How do you ensure that the approach to controlling system maintenance activities aligns with NIST guidelines and broader cybersecurity objectives?

## Maintenance

## MA.L2-3.7.3

## Derived

## Ensure equipment removed for off-site maintenance is sanitized of any CUI.

- How do you identify equipment that contains or has accessed CUI before it's sent off-site for maintenance?
- Describe the process used to sanitize equipment of CUI prior to off-site maintenance.
- What tools or software are used to ensure complete sanitization of CUI from the equipment?
- How do you verify or validate that the sanitization process has been effective in removing all traces of CUI?
- What protocols are in place for handling equipment that cannot be adequately sanitized before off-site maintenance?
- How do you maintain a chain of custody or track equipment that is sent off-site for maintenance?
- Are there specific agreements or contracts with maintenance vendors regarding the handling and protection of CUI?
- How do you handle the potential backup or retention of CUI during the sanitization process?
- Describe any training or awareness programs in place for personnel responsible for sanitizing equipment of CUI.
- How do you address situations where equipment containing CUI is sent off-site for emergency maintenance or repairs?
- Are there automated tools or alerts in place to detect CUI on equipment designated for off-site maintenance?
- How do you handle potential data remnants or hidden storage areas on equipment that might contain CUI?
- Describe any challenges or issues you've faced related to sanitizing equipment of CUI and how they were addressed.
- How do you ensure the recovery or restoration of non-CUI data on equipment after the sanitization process?
- Are there periodic audits or assessments to verify the effectiveness of CUI sanitization procedures for off-site maintenance?

- How do you handle feedback or concerns related to the sanitization of equipment containing CUI?
- How do you collaborate with external entities, industry peers, or security experts to enhance your sanitization practices for CUI?
- Are there specific protocols or considerations for different types of equipment, such as servers, workstations, mobile devices, or storage devices?
- How do you ensure that the sanitization process adheres to NIST guidelines and other relevant standards?
- How do you document and maintain records of sanitization processes and verifications for equipment sent off-site?

## Maintenance

## MA.L2-3.7.4

Derived

## Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.

- What procedures are in place to check media with diagnostic and test programs for malicious code?
- How do you ensure that all media, regardless of its source, undergoes this checking process before use?
- Describe the tools or software you use for scanning and detecting malicious code on such media.
- How frequently are these scanning tools or software updated to detect the latest threats?
- How do you handle media that is found to contain malicious code?
- What protocols are in place for reporting and addressing incidents related to malicious code detection?
- How do you ensure that third-party or externally sourced diagnostic/test media is checked for malicious code before use?
- Are there any exceptions or scenarios where media might bypass this checking process? If so, how are they justified or managed?
- How do you train and educate relevant personnel about the importance of checking media for malicious code?
- Are there automated alerts or mechanisms in place to detect unauthorized or unchecked media usage within organizational systems?
- How do you verify the integrity and authenticity of diagnostic and test programs on the media?
- Describe any challenges or issues you've faced related to checking media for malicious code and how they were addressed.
- How do you ensure that the checking process doesn't inadvertently affect the functionality of legitimate diagnostic and test programs?

- How do you handle media that is reused or repurposed for diagnostic and test purposes?
- How do you collaborate with external entities, industry peers, or security experts to stay updated on best practices for media checking?
- Are there periodic security audits or assessments to verify the consistent application of malicious code checking on all media?
- How do you manage feedback or concerns related to the media checking process?
- How do you balance the need for rapid diagnostics or testing with the time required for thorough malicious code checks?
- How do you stay updated on emerging threats or attack vectors that might bypass traditional media checking mechanisms?
- How do you ensure that the approach to checking media for malicious code aligns with NIST guidelines and broader cybersecurity objectives?

## Maintenance

## MA.L2-3.7.5

Derived

### Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.

- How does your organization implement multifactor authentication for nonlocal maintenance sessions?
- What factors or methods are used as part of your MFA process for nonlocal maintenance?
- Describe the tools or platforms used to enforce MFA for these sessions.
- How do you ensure that nonlocal maintenance sessions are terminated upon completion?
- Are there any automated mechanisms in place to detect and terminate inactive nonlocal maintenance sessions?
- How do you handle exceptions or scenarios where MFA might be bypassed or not possible?
- How do you train and educate relevant personnel about the importance of MFA for nonlocal maintenance sessions?
- What measures are in place to protect against potential MFA bypass or spoofing attempts?
- How do you verify the identity and authenticity of external entities initiating nonlocal maintenance sessions?
- How do you log and monitor nonlocal maintenance sessions, especially those requiring MFA?
- Describe any challenges or issues you've encountered related to MFA for nonlocal maintenance and how they were addressed.

- How do you integrate MFA enforcement with other security systems or protocols?
- How frequently do you review and update your MFA mechanisms and policies for nonlocal maintenance sessions?
- Are there specific controls or protocols for MFA in critical or high-security systems during nonlocal maintenance?
- How do you handle feedback or concerns from users or technicians related to MFA during nonlocal maintenance?
- How do you ensure continuity in maintenance operations while enforcing MFA and session termination protocols?
- How do you collaborate with external entities, industry peers, or security experts to stay updated on best practices for MFA during nonlocal maintenance?
- Are there periodic security audits or assessments to verify the consistent application of MFA and session termination for nonlocal maintenance?
- How do you ensure that third-party vendors or partners adhere to your organization's MFA requirements for nonlocal maintenance?
- How do you ensure that the approach to MFA and session termination for nonlocal maintenance aligns with NIST guidelines and broader cybersecurity objectives?

## Maintenance

## MA.L2-3.7.6

Derived

### Supervise the maintenance activities of maintenance personnel without required access authorization.

- How do you identify and track maintenance personnel who do not have the required access authorization?
- What protocols are in place to ensure that such maintenance personnel are always supervised during their activities?
- Who within the organization is responsible for supervising these maintenance activities?
- Describe the process or measures to ensure unauthorized personnel do not access sensitive or classified information during maintenance.
- How do you handle situations where maintenance needs to be performed urgently or outside of regular business hours?
- What training or guidelines are provided to supervisors overseeing maintenance personnel without required access authorization?
- How do you log and document the activities of maintenance personnel who are supervised?

- Are there any tools or technologies in place to aid in the supervision of maintenance activities, such as video surveillance or real-time monitoring?
- How do you handle scenarios where maintenance personnel without the required access authorization need to interact with third-party vendors or external systems?
- What measures are in place to prevent or detect unauthorized actions or deviations by maintenance personnel during their activities?
- How do you ensure that the maintenance performed by such personnel does not inadvertently introduce vulnerabilities or security risks?
- Are there periodic audits or reviews of the supervision process to ensure its effectiveness and adherence to protocols?
- Describe any challenges or issues you've encountered related to supervising maintenance personnel without required access, and how they were addressed.
- How do you handle feedback or concerns from supervisors or other staff related to this supervision process?
- How do you stay updated on best practices and industry standards related to supervising maintenance activities?
- How do you manage scenarios where maintenance personnel require temporary access to areas or data beyond their usual scope?
- How do you ensure that third-party maintenance providers or vendors adhere to your supervision protocols?
- How do you validate the credentials or background of maintenance personnel before they perform their tasks?
- Are there specific protocols for supervising maintenance activities in critical or high-security environments?
- How do you ensure that the approach to supervising maintenance personnel aligns with NIST guidelines and your organization's broader cybersecurity objectives?

## WHY REDSPIN

- Over 100 security advisors and assessors, ready to scale with you as needed
- Possesses the know-how from performing over 1,000 assessments in highly regulated industries, including multiple Joint Surveillance Voluntary Assessment Program (JSVAP) assessments
- Uplifts its service offering to validate your security, giving you the confidence that your people, processes, and technology are effective
- Our team understands CMMC requirements and follows professional conduct to help you on your journey to becoming CMMC-ready and certified

Redspin, a division of Clearwater, has become one of the most trusted cybersecurity companies for the Defense Industrial Base. Our exclusive focus on tailoring our CMMC assessment, training, consulting, and managed services for each client delivers peace of mind by lowering the risk of a security incident or breach, and meeting/maintaining compliance regulations. Since our founding in 2001, we've become a thought leader in IT security, helped countless clients control their security risk, develop their security strategy, and avoid a breach headline.

Redspin
A Division of Clearwater

40 Burton Hills Blvd
Suite 200
Nashville, TN 37215

info@redspin.com
www.redspin.com