GUIDE

Redspin
A Division of Clearwater

Preparing for Your CMMC Interview: Commonly Asked Questions – Personnel Security Edition

This domain emphasizes a thorough review and vetting of all personnel to ensure these individuals can be trusted with access to sensitive information. This is typically performed through an initial background check, ongoing review of accesses, and regular training; it is intended to mitigate the risks associated with our 'human firewalls'.

TABLE OF CONTENTS

Key

Domain Family

Identifier

Basic | Derived

Security Requirement

Security Requirement Table of Contents

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?

Personnel Security

PS.L2-3.9.1

Basic

Screen individuals prior to authorizing access to organizational systems containing CUI.

- What is your process for screening individuals before granting them access to systems with CUI?
- What specific criteria or checks are included in the screening process?
- How do you verify the provided information of individuals during the screening process?
- Are there different levels of screening based on the sensitivity or classification of the CUI?
- How do you ensure that the screening process complies with legal and privacy regulations?
- What mechanisms are in place to re-screen individuals at periodic intervals or upon role changes?
- How do you manage and document the results of individual screenings?
- What is the procedure for denying access based on the results of a screening?
- How do you handle third-party or external contractors in the screening process?
- Are individuals made aware of the reasons for screening and the criteria being checked?
- How do you ensure that the screening process is consistently applied across all departments and teams?
- How do you address potential false positives or disputes arising from the screening process?
- Describe any challenges or issues you've faced related to screening individuals and how they were addressed.
- How do you train or educate relevant personnel about the importance and procedures of the screening process?
- How do you integrate the screening process with other security measures, such as access controls or user authentication?
- Are there periodic audits or assessments to validate the effectiveness and consistency of your screening process?
- How do you stay updated on best practices or legal requirements related to screening individuals for access to CUI?
- How do you handle the screening process in emergency or urgent situations requiring rapid access to CUI?
- How do you ensure that the screening process doesn't inadvertently hamper operational efficiency or critical business functions?
- How do you ensure that the approach to screening individuals prior to granting access to CUI aligns with NIST guidelines and broader cybersecurity objectives?

Personnel Security

PS.L2-3.9.2

Basic

Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers

- How does your organization handle access to systems containing CUI during personnel terminations?
- What processes are in place to ensure that access rights to CUI are revoked or modified during personnel transfers?
- Describe the timeline and immediacy of actions taken to protect CUI when an employee is terminated.
- How do you ensure that transferred employees do not retain unauthorized access to CUI from their previous roles?
- Are there automated systems or alerts in place to notify IT or security teams of personnel terminations or transfers?
- How do you handle the physical and digital assets (like devices or media) that might contain CUI when an employee is terminated or transferred?
- What measures are in place to ensure that former employees cannot access organizational systems containing CUI remotely?
- How do you audit or verify the successful removal or modification of access rights after personnel actions?
- Describe any challenges or issues you've faced in protecting CUI during personnel actions and how they were addressed.
- How do you handle situations where a terminated employee had unique knowledge or control over systems containing CUI?
- What training or awareness programs are in place to educate HR and management about the importance of timely notifications related to personnel actions?
- How do you ensure third-party vendors or partners protect CUI during their own personnel actions?
- Are there periodic security reviews or assessments to validate the protection of CUI during and after personnel actions?
- How do you address potential insider threats related to personnel terminations or transfers concerning CUI?
- How do you manage backup or archived data containing CUI related to terminated or transferred personnel?
- How do you ensure the timely return or secure disposal of physical documents containing CUI from terminated or transferred employees?

- How do you handle shared or group accounts in the context of personnel actions, especially if they have access to CUI?
- What incident response measures are in place if unauthorized access to CUI is detected after a personnel action?
- How do you collaborate with other departments, like HR, to streamline and ensure the protection of CUI during personnel actions?
- How do you ensure that the approach to protecting CUI during and after personnel actions aligns with NIST guidelines and the broader cybersecurity objectives of the organization?

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