GUIDE

Redspin
A Division of Clearwater

Preparing for Your CMMC Interview: Commonly Asked Questions – Media Protection Edition

This domain focuses on the protection of both digital and physical media, both in storage and in transit. This includes USB drives, DVDs, hard drives, and even printed documentation that may include sensitive data. Media protection ensures that the data cannot be accessed, altered, or breached by unauthorized entities. These protections could include things like, encryption, access control, physical locks, and secure transportation methods.

TABLE OF CONTENTS

Key

Domain Family

Identifier

Basic | Derived

Security Requirement

Security Requirement Table of Contents

Media Protection

- Protect the confidentiality of backup CUI at storage locations....4
- Prohibit the use of portable storage devices when such devices have no identifiable owner....5
- Control the use of removable media on system components....6
- Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas....7
- Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards....8
- Sanitize or destroy system media containing CUI before disposal or release for reuse....9
- Limit access to CUI on system media to authorized users....10
- Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital....11
- Mark media with necessary CUI markings and distribution limitations....12

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?

Incident Response

MP.L2-3.8.9

Derived

Protect the confidentiality of backup CUI at storage locations.

- How does your organization ensure the confidentiality of backup CUI during storage?
- What encryption methods and standards are employed to secure backup CUI at storage locations?
- Where are the backup storage locations for CUI, and how are they secured?
- How do you manage and control access to backup storage locations containing CUI?
- Are there any third-party or cloud-based storage solutions used for backup CUI? If so, how do you ensure their compliance with NIST guidelines?
- How frequently do you review and update security measures for backup CUI storage locations?
- How do you monitor and detect unauthorized access or breaches to backup CUI storage locations?
- What procedures are in place for securely restoring CUI from backups?
- How do you ensure that the encryption keys or credentials for backup CUI storage are securely managed and stored?
- Describe the retention policies for backup CUI. How do you ensure the secure disposal of outdated or unnecessary backups?
- Are there automated alerts or mechanisms to detect potential threats or vulnerabilities related to backup CUI storage locations?
- How do you handle backup CUI for remote or offsite locations, if applicable?
- Describe any challenges or issues you've faced in securing backup CUI at storage locations and how they were addressed.
- How do you test or validate the effectiveness of security measures in place for backup CUI storage?
- How do you educate and train relevant personnel on the importance and procedures for securing backup CUI at storage locations?
- How do you integrate the protection of backup CUI storage with other security tools, incident response systems, or risk management protocols?
- Are there periodic security audits or assessments to verify the confidentiality of backup CUI at storage locations?
- How do you ensure continuity and availability of backup CUI while maintaining its confidentiality?
- How do you handle incidents or breaches related to the confidentiality of backup CUI at storage locations?
- How do you ensure that the approach to protecting backup CUI at storage locations aligns with NIST guidelines and broader cybersecurity objectives?

Incident Response

MP.L2-3.8.8

Derived

Prohibit the use of portable storage devices when such devices have no identifiable owner.

- How does your organization track and identify the ownership of portable storage devices?
- What policies or protocols are in place to handle unidentified portable storage devices found within your premises?
- How do you ensure that employees and staff are aware of the prohibition against using unowned portable storage devices?
- Describe the technical controls in place to prevent the use of unowned portable storage devices on organizational systems.
- How do you handle exceptions or instances where an unidentified portable storage device must be accessed?
- What measures are in place to detect and alert on the connection of unowned or unauthorized portable storage devices?
- How do you manage and track third-party or visitor use of portable storage devices within the organization?
- Describe any challenges or issues you've faced related to unidentified portable storage devices and how they were addressed.
- Are there training programs or awareness campaigns to educate users about the risks of unowned portable storage devices?
- How do you handle the disposal or secure wiping of unowned or unidentified portable storage devices?
- What is the protocol for reporting the discovery of unowned portable storage devices within the organization?
- How do you integrate the prohibition of unowned portable storage devices with other security measures or protocols?
- How do you ensure that third-party vendors or partners are aware of and adhere to this prohibition when on-site?
- Are there specific areas or departments within the organization with stricter controls regarding portable storage devices?
- How do you stay updated on best practices and industry standards related to portable storage device security?
- Are there periodic security audits or assessments to verify adherence to the prohibition of unowned portable storage devices?

- How do you manage user feedback or concerns related to the use of portable storage devices?
- How do you ensure that the approach to prohibiting unowned portable storage devices aligns with NIST guidelines and broader cybersecurity objectives?
- In cases where an unowned device is found connected to a system, how is the incident managed and investigated?
- How do you ensure that the prohibition does not hinder legitimate business operations or tasks requiring the use of portable storage devices?

Incident Response

MP.L2-3.8.7

Derived

Control the use of removable media on system components.

- What is your organization's policy regarding the use of removable media on system components?
- How do you enforce and monitor adherence to your removable media policy?
- Are there specific tools or solutions in place to detect and manage removable media when connected to your systems?
- How do you ensure that data transferred to or from removable media is encrypted or otherwise protected?
- Are there specific types or brands of removable media that are approved for use, and how is this communicated to users?
- How do you handle unauthorized or unrecognized removable media devices when they are connected to your systems?
- What training or awareness programs are in place to educate users about the risks and guidelines associated with using removable media?
- Are there specific areas, departments, or systems where the use of removable media is strictly prohibited or restricted?
- How do you manage and log data transfers involving removable media?
- How do you handle the disposal or sanitization of removable media to ensure data cannot be retrieved?
- What measures are in place to scan removable media for malware or malicious content before use?
- How do you handle incidents where sensitive or restricted data is found on unauthorized removable media?
- Are there alerts or notifications in place to inform administrators or security teams of unauthorized removable media usage?

- How do you ensure third-party vendors or partners adhere to your organization's policies on removable media?
- Are there specific protocols for using removable media during system backups, migrations, or updates?
- How frequently is the removable media policy reviewed and updated to address new threats or technologies?
- Describe any challenges or incidents you've encountered related to removable media and how they were addressed.
- How do you integrate removable media controls with other security tools and protocols?
- Are there periodic audits or assessments to validate adherence to and effectiveness of removable media controls?
- How do you ensure that the approach to controlling removable media aligns with NIST guidelines and the broader cybersecurity objectives of your organization?

Incident Response

MP.L2-3.8.5

Derived

Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.

- How do you identify and label media containing CUI?
- What controls are in place to restrict access to media storing CUI?
- Describe the procedures for transporting media containing CUI outside of controlled areas.
- How do you ensure accountability and maintain a chain of custody for media containing CUI during transport?
- What tools or mechanisms are used to track the location and movement of CUI media?
- How do you handle the secure disposal or destruction of media containing CUI?
- How are individuals trained on the proper handling and transport of media containing CUI?
- Are there specific encryption or security measures applied to media storing CUI, especially during transport?
- How do you verify the identity and authorization of individuals accessing or transporting media with CUI?
- What measures are in place to detect and respond to unauthorized access or breaches involving media containing CUI?
- How do you handle the transport of CUI media by third-party vendors or partners?
- Describe any incidents or challenges encountered with CUI media transport, and how they were addressed.

- How do you ensure that backups or replicas of CUI media are also protected and controlled during transport?
- Are there periodic audits or assessments to validate the security and accountability of CUI media during transport?
- How do you manage the return or secure receipt of media containing CUI after transport?
- How do you maintain a record or log of all transport activities related to media containing CUI?
- How do you handle emergency or urgent transport scenarios involving media with CUI?
- How do you stay updated on best practices and industry standards related to the protection and transport of CUI media?
- What protocols are in place for reporting or escalating any loss, theft, or compromise of media containing CUI during transport?
- How do you ensure that the approach to controlling access and maintaining accountability for CUI media aligns with NIST guidelines and broader cybersecurity objectives?
- These questions aim to assess the organization's procedures, controls, and s

Incident Response

MP.L2-3.8.6

Derived

Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

- How do you identify and label media containing CUI?
- What controls are in place to restrict access to media storing CUI?
- Describe the procedures for transporting media containing CUI outside of controlled areas.
- How do you ensure accountability and maintain a chain of custody for media containing CUI during transport?
- What tools or mechanisms are used to track the location and movement of CUI media?
- How do you handle the secure disposal or destruction of media containing CUI?
- How are individuals trained on the proper handling and transport of media containing CUI?
- Are there specific encryption or security measures applied to media storing CUI, especially during transport?
- How do you verify the identity and authorization of individuals accessing or transporting media with CUI?

- What measures are in place to detect and respond to unauthorized access or breaches involving media containing CUI?
- How do you handle the transport of CUI media by third-party vendors or partners?
- Describe any incidents or challenges encountered with CUI media transport, and how they were addressed.

Incident Response

MP.L1-3.8.3

Basic

Sanitize or destroy system media containing CUI before disposal or release for reuse.

- Describe the processes and procedures in place for sanitizing or destroying media containing CUI.
- What tools or technologies are utilized for media sanitization?
- How do you ensure that all CUI has been effectively removed or destroyed before media disposal or reuse?
- How do you track and inventory media containing CUI?
- What protocols are in place for physical destruction of media, if applicable?
- How do you handle different types of media (e.g., HDDs, SSDs, USB drives, tapes) in terms of sanitization or destruction?
- Are there specific personnel or teams responsible for media sanitization or destruction? If so, how are they trained?
- How do you verify or validate that media has been properly sanitized or destroyed?
- What documentation or records are maintained to confirm sanitization or destruction of media containing CUI?
- How do you manage third-party vendors or partners that may handle media containing CUI in terms of sanitization or destruction requirements?
- Are there automated alerts or mechanisms to ensure that unsanitized media is not inadvertently released or reused?
- Describe any challenges or issues you've faced related to media sanitization or destruction and how they were addressed.
- How do you handle the sanitization or destruction of media in emergency or unplanned scenarios?
- How do you stay updated on best practices and industry standards related to media sanitization and destruction?

- Are there periodic security audits or assessments to verify adherence to media sanitization or destruction protocols?
- How do you manage feedback or concerns related to media sanitization or destruction processes?
- How do you ensure that sanitization or destruction methods are effective against potential data recovery attempts?
- How do you handle media that has been damaged or is otherwise non-operational in terms of sanitization or destruction?
- Are there specific protocols or considerations for sanitizing or destroying media used in critical or high-security environments?
- How do you ensure that the approach to sanitizing or destroying media containing CUI aligns with NIST guidelines and broader cybersecurity objectives?

Incident Response

MP.L2-3.8.2

Basic

Limit access to CUI on system media to authorized users

- How do you define and identify CUI within your organization's system media?
- Describe the access controls in place to ensure only authorized users can access CUI on system media.
- What mechanisms are used to authenticate users before granting them access to CUI?
- How do you track and log access to CUI on system media?
- How frequently do you review and update the list of users authorized to access CUI?
- How do you handle requests for access to CUI on system media?
- Are there automated alerts or mechanisms in place to detect unauthorized access attempts to CUI on system media?
- How do you ensure that third-party vendors or partners adhere to the organization's policies for accessing CUI on system media?
- What training programs are in place to educate users about the importance and protocols of accessing CUI on system media?
- How do you manage and monitor remote access to CUI on system media?
- Describe any encryption or additional security measures in place for CUI stored on system media.
- How do you ensure that backups or copies of system media containing CUI are also protected and accessible only to authorized users?

- What procedures are in place for deprovisioning or revoking access to CUI for users who no longer require it?
- How do you handle incidents or breaches related to unauthorized access to CUI on system media?
- Are there periodic security audits or assessments to validate the effectiveness of controls protecting CUI on system media?
- How do you stay updated on best practices and industry standards related to protecting CUI on system media?
- How do you ensure the continuity of access controls for CUI during system updates, migrations, or other changes?
- Are there specific protocols or layers of protection for CUI on system media considered highly sensitive or critical?
- How do you address feedback or concerns from stakeholders related to access controls for CUI on system media?
- How do you ensure that the approach to limiting access to CUI on system media aligns with NIST guidelines and broader cybersecurity objectives?

Incident Response

MP.L2-3.8.1

Basic

Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.

- How does your organization identify and classify media containing CUI?
- Describe the physical security measures in place to protect media containing CUI.
- How do you ensure digital media containing CUI is securely stored and encrypted?
- What protocols are in place for handling and transporting paper media containing CUI within and outside the organization?
- How do you track and inventory digital media that contains CUI?
- Describe the access controls implemented to restrict unauthorized access to media containing CUI.
- How is disposal or destruction of CUI-containing media managed and documented?
- Are there specific secure storage areas or containers designated for media containing CUI?
- How do you handle backup and replication of digital media containing CUI?
- How do you address the risk of unauthorized duplication or reproduction of CUI-containing media?
- What training or awareness programs are in place to educate staff about the proper handling of CUI-containing media?

- How do you manage third-party vendors or partners who handle or have access to media containing CUI?
- Are there automated alerts or mechanisms to detect unauthorized access or breaches related to CUI-containing media?
- Describe any challenges or issues you've faced related to protecting CUI-containing media and how they were addressed.
- How do you integrate the protection of CUI-containing media with other security and compliance systems or protocols?
- How frequently are protocols for handling CUI-containing media reviewed and updated?
- Are there periodic security audits or assessments to validate the protective measures for CUI-containing media?
- How do you address potential risks associated with cloud storage or offsite storage of CUI-containing media?
- How do you ensure that protective measures for CUI-containing media are in line with evolving threats and best practices?
- How do you ensure that the approach to protecting CUI-containing media aligns with NIST guidelines and broader cybersecurity objectives?

Incident Response

MP.L2-3.8.4

Derived

Mark media with necessary CUI markings and distribution limitations.

- How does your organization determine which media requires CUI markings?
- Describe the process for applying CUI markings to physical and electronic media.
- What types of media within your organization typically contain CUI?
- How do you ensure consistent application of CUI markings across various media formats?
- Are there automated tools or systems in place to facilitate the marking of media with CUI designations?
- How do you handle updates or changes to CUI categories and their associated markings?
- What training is provided to staff to ensure they understand and properly apply CUI markings and distribution limitations?
- How do you manage and monitor the distribution of media marked with CUI designations?
- What mechanisms are in place to detect and address unauthorized distribution or reproduction of CUI-marked media?

- How do you handle media that contains mixed information, both CUI and non-CUI?
- What protocols are in place for the disposal or declassification of CUI-marked media?
- How do you ensure that third-party vendors or partners adhere to the CUI marking and distribution limitations when handling your organization's media?
- Describe any challenges or issues you've encountered related to CUI marking and distribution and how they were addressed.
- How do you handle feedback or concerns related to CUI markings and distribution limitations?
- Are there periodic audits or assessments to ensure compliance with CUI marking and distribution guidelines?
- How do you stay informed about changes or updates to CUI requirements and marking standards?
- Are there mechanisms in place to verify the authenticity and correctness of CUI markings on media?
- How do you manage electronic backups or replications of CUI-marked media?
- How do you ensure that CUI markings are retained during media migrations or technology upgrades?
- How do you ensure that the approach to marking media with CUI designations and managing their distribution aligns with NIST guidelines and 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