GUIDE

Redspin
A Division of Clearwater

Preparing for Your CMMC Interview: Commonly Asked Questions – System and Information Integrity Edition

This domain focuses on ensuring the accuracy, reliability, and overall integrity of data and systems – by ensuring the trustworthiness and proper functioning of the organization's information systems. This includes detecting, preventing, and responding to potential compromises or corruptions in the data and system operations.

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?

System and Information Integrity

SI.L1-3.14.5

Derived

Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

- How frequently does your organization perform periodic scans of its systems?
- What tools or platforms are used for performing these scans?
- Describe the scope and depth of the periodic scans. Do they include all organizational systems?
- How does your organization handle real-time scans of files from external sources?
- Are there automated alerts or mechanisms in place to notify relevant personnel of suspicious or malicious findings during scans?
- How do you ensure that files from external sources are scanned as they are downloaded, opened, or executed?
- What actions are taken when potentially malicious content is detected during real-time scanning?
- How do you manage false positives or exceptions during scanning?
- How frequently are the scanning tools and their signatures or definitions updated?
- Describe any challenges or issues you've faced related to system scanning and how they were addressed.
- How do you handle encrypted files or content during the scanning process?
- Are scan results logged and retained for future reference or analysis?
- How do you ensure minimal disruption or performance impact during periodic scans?
- How are stakeholders or system owners notified of scan results, especially if remediation actions are required?
- How do you integrate the scanning process with other security tools, incident response systems, or risk management protocols?
- How do you ensure that third-party vendors or integrated solutions adhere to your organization's scanning requirements?
- Are there periodic reviews or assessments to validate the effectiveness and coverage of your scanning processes?
- How do you stay updated on emerging threats or vulnerabilities and ensure they are covered in the scanning process?
- How do you manage and prioritize remediation efforts based on scan findings?
- How do you ensure that the approach to periodic and real-time scanning aligns with NIST guidelines and broader cybersecurity objectives?

System and Information Integrity

SI.L1-3.14.4

Derived

Update malicious code protection mechanisms when new releases are available.

- How do you stay informed about new releases or updates to your malicious code protection mechanisms?
- Describe the process for testing and validating new releases of malicious code protection tools before deployment.
- What is the average timeframe between the release of an update and its implementation in your organization?
- How do you ensure that all systems and devices receive malicious code protection updates promptly?
- Are there automated mechanisms in place to deploy updates to malicious code protection tools?
- How do you handle situations where an update to a malicious code protection tool might conflict with other system components?
- What protocols are in place to roll back or address issues arising from a malicious code protection update?
- How do you manage and track updates for third-party or external systems connected to your environment?
- How often do you review and assess the effectiveness of your malicious code protection tools after updates?
- Are there any systems or applications that are exceptions to immediate updates, and if so, how are they managed?
- How do you communicate and coordinate malicious code protection updates with relevant stakeholders or departments?
- Are there training or awareness programs to educate staff about the importance of timely updates to malicious code protection mechanisms?
- Describe any challenges or issues you've faced related to updating malicious code protection tools and how they were addressed.
- How do you prioritize updates if multiple updates are available at the same time for different tools or components?
- How do you ensure the authenticity and integrity of updates to malicious code protection tools?
- Are there automated alerts or notifications set up to inform of a missed or failed update?
- How do you handle end-of-life scenarios where updates might no longer be available for certain malicious code protection tools?

- How do you collaborate with vendors or industry peers to ensure timely and effective updates to malicious code protection mechanisms?
- Are there periodic security audits or assessments to verify the consistent and effective updating of malicious code protection tools?
- How do you ensure that the approach to updating malicious code protection mechanisms aligns with NIST guidelines and broader cybersecurity objectives?

System and Information Integrity

SI.L2-3.14.6

Derived

Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

- What tools or solutions do you use for monitoring organizational systems and communications traffic?
- How do you monitor inbound communications to detect malicious or suspicious activity?
- Describe your approach to monitoring outbound communications to identify potential data exfiltration or command-and-control traffic.
- How do you differentiate between legitimate traffic and potential indicators of attacks?
- Are there automated alerts or mechanisms in place to notify relevant personnel of detected attacks or suspicious activities?
- How do you ensure that encrypted traffic is inspected for potential threats?
- What is your retention policy for logs and data related to system and traffic monitoring?
- How do you ensure that monitoring tools and solutions are continuously updated to detect the latest attack vectors and techniques?
- Describe the process for reviewing and analyzing the collected monitoring data.
- How do you correlate data from multiple sources or systems to detect complex or multi-stage attacks?
- How do you handle false positives or irrelevant alerts in your monitoring process?
- What training do the personnel responsible for monitoring and analysis receive to stay updated on emerging threats?
- How do you manage and monitor third-party or partner connections to your organizational systems?
- Describe any challenges or issues you've encountered related to system and traffic monitoring and how they were addressed.

- How do you integrate system and traffic monitoring with other security systems, such as intrusion prevention systems or security information and event management (SIEM) solutions?
- How do you prioritize responses or investigations based on the detected attacks or potential attack indicators?
- How do you ensure the privacy of legitimate user data while monitoring communications traffic?
- How do you collaborate with external entities, industry peers, or security experts to stay updated on monitoring best practices and threat intelligence?
- Are there periodic security audits or assessments to validate the effectiveness of your monitoring practices?
- How do you ensure that the approach to monitoring organizational systems and communications traffic aligns with NIST guidelines and broader cybersecurity objectives?

System and Information Integrity

SI.L1-3.14.2

Basic

Provide protection from malicious code at designated locations within organizational systems.

- How does your organization identify and designate locations within systems that require protection from malicious code?
- What tools or solutions are implemented to provide protection against malicious code at these locations?
- How frequently are these protective measures updated or reviewed?
- How do you ensure that designated locations remain protected when system updates or changes occur?
- Describe the process for detecting and responding to malicious code detected at designated locations.
- How are end-users made aware of the designated locations and the importance of their protection?
- Are there automated alerts or mechanisms in place to notify of potential malicious code breaches at these designated locations?
- How do you handle false positives or legitimate activities flagged as malicious code?
- How do you ensure third-party software or integrations don't introduce malicious code into the designated locations?
- How do you stay updated on emerging threats or new forms of malicious code relevant to your organizational systems?

- Describe any challenges or incidents related to malicious code at designated locations and how they were addressed.
- How do you integrate malicious code protection with other cybersecurity measures or tools in the organization?
- Are there specific protocols or enhanced measures for designated locations within critical or high-importance systems?
- How do you test or validate the effectiveness of your malicious code protection measures at designated locations?
- What training or awareness programs are in place to educate users about the risks of malicious code?
- How do you manage and update whitelists or blacklists related to software or processes allowed at designated locations?
- How do you ensure continuity of operations when a potential malicious code threat is detected at a designated location?
- How do you collaborate with external entities, industry peers, or security experts regarding best practices for malicious code protection?
- Are there periodic security audits or assessments to verify the protection measures at designated locations?
- How do you ensure that the approach to protecting designated locations from malicious code aligns with NIST guidelines and broader cybersecurity objectives?

System and Information Integrity

SI.L1-3.14.1

Basic

Identify, report, and correct system flaws in a timely manner.

- How does your organization identify system flaws or vulnerabilities?
- What tools or platforms are used for vulnerability scanning or flaw detection?
- How frequently are system vulnerability assessments or scans conducted?
- Describe the process for reporting identified system flaws.
- Who is responsible for addressing and correcting reported flaws?
- What is the average timeframe for addressing and resolving critical flaws upon detection?
- How do you prioritize the correction of identified system flaws?
- How are stakeholders or affected users informed about identified flaws and potential impacts?
- Describe any automated systems or alerts in place for immediate flaw detection and reporting.

- How do you ensure third-party software or integrated systems are free of flaws, or how are they managed if detected?
- What measures are in place to prevent the exploitation of identified but uncorrected flaws?
- How do you track and ensure the timely resolution of all reported flaws?
- Are there mechanisms to verify the effective correction of identified flaws?
- How do you integrate flaw identification and correction with other security protocols, like patch management?
- Describe any challenges or issues you've faced related to flaw detection and correction, and how they were addressed.
- How do you stay updated on potential new system flaws or vulnerabilities relevant to your technology stack?
- How do you handle flaws that might require significant system changes or downtime to address?
- Are there periodic security reviews or assessments to validate the thoroughness of your flaw detection and correction processes?
- How do you collect and address feedback or concerns related to system flaws from users or departments?
- How do you ensure that the approach to identifying, reporting, and correcting system flaws aligns with NIST guidelines and broader cybersecurity objectives?

System and Information Integrity

SI.L2-3.14.3

Basic

Monitor system security alerts and advisories and take action in response.

- How does your organization monitor and stay updated on system security alerts and advisories?
- Which sources or platforms do you rely on for security alerts and advisories?
- Describe the process you follow upon receiving a security alert or advisory.
- How do you prioritize and categorize the alerts and advisories you receive?
- What mechanisms or tools are in place to automate the monitoring of security alerts and advisories?
- How quickly, on average, does your organization respond to critical security alerts?
- Who within the organization is responsible for reviewing and acting upon security advisories and alerts?
- Describe any incident response plans or procedures that are triggered by specific alerts or advisories.
- How do you ensure that relevant stakeholders are promptly informed about critical security alerts or advisories?

- How do you validate the authenticity of security advisories or alerts before taking action?
- How are lessons learned from previous alerts and advisories incorporated into future response strategies?
- Are there automated mechanisms in place to block or mitigate threats based on received security alerts?
- How do you handle false positives or irrelevant security alerts and advisories?
- How do you ensure continuous monitoring of security alerts, especially outside of regular business hours or during holidays?
- How do you track and document the organization's response to specific security alerts or advisories?
- Are there periodic drills or simulations conducted to test the organization's response to security advisories or alerts?
- How do you stay updated on emerging threats or vulnerabilities that may not yet have official advisories or alerts?
- How do you collaborate with external entities, industry peers, or security experts regarding security alerts and advisories?
- Are there any challenges or issues you've faced related to monitoring and responding to security alerts and advisories, and how were they addressed?
- How do you ensure that the approach to monitoring and responding to security advisories and alerts aligns with NIST guidelines and broader cybersecurity objectives?

System and Information Integrity

SI.L2-3.14.7

Derived

Identify unauthorized use of organizational systems.

- How do you detect unauthorized access or use of your organizational systems?
- What tools or solutions are in place to monitor system activity for signs of unauthorized use?
- How are alerts or notifications configured for potential unauthorized activities?
- Describe the protocols followed when unauthorized use is detected.
- What baseline behaviors or patterns are established to differentiate between authorized and unauthorized use?
- How frequently do you review and update criteria or thresholds for detecting unauthorized use?

- Are there any machine learning or AI-based tools employed to enhance detection of unauthorized activities?
- How do you ensure that legitimate users are not falsely flagged as unauthorized?
- How do you handle persistent unauthorized access attempts from specific IP addresses or regions?
- What training or awareness programs are in place to educate personnel about recognizing and reporting potential unauthorized activities?
- How do you validate the effectiveness of your unauthorized use detection mechanisms?
- Are there specific protocols in place for critical or sensitive systems to detect and respond to unauthorized access?
- How do you integrate unauthorized use detection with other security measures, such as incident response or intrusion prevention systems?
- How do you manage potential unauthorized use stemming from third-party vendors or partners with system access?
- Describe any challenges or incidents related to unauthorized use detection and how they were addressed.
- How frequently are logs and records related to system access reviewed for signs of unauthorized activity?
- How do you collaborate with external entities or industry peers to stay updated on patterns or indicators of unauthorized use?
- Are there periodic security audits or assessments to evaluate the capability of detecting unauthorized system use?
- How do you ensure that false positives, or legitimate activities mistakenly flagged as unauthorized, are managed and minimized?
- How do you ensure that the approach to detecting unauthorized use 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