GUIDE

Redspin
A Division of Clearwater

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

Organizations benefit through regular checks of their operationalized cybersecurity mechanisms, including verifying that implemented security controls are operating 'as intended', producing the desired results, and are effective. This is usually accomplished through rigorous, ongoing checks of the organization's information systems to identify weaknesses or compliance gaps while providing a clear picture of the organization's cybersecurity health. This insight enables organizations to understand potential threats, address identified vulnerabilities, and improve overall security protocols.

Copyright © 2023 Redspin, a Division of Clearwater. All Rights Reserved.

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?

Copyright © 2023 Redspin, a Division of Clearwater. All Rights Reserved.

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?

Copyright © 2023 Redspin, a Division of Clearwater. All Rights Reserved.

Security Assessment

CA.L2-3.12.1

Basic

Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.

- How frequently does your organization conduct assessments of its security controls?
- What methodologies or frameworks are used for these periodic security control assessments?
- Who is responsible for conducting these assessments within your organization?
- How do you prioritize which security controls to assess during each review cycle?
- Describe the tools or platforms used for the assessment of security controls.
- How do you ensure that the assessment process covers all relevant systems and environments, including cloud and remote infrastructures?
- After an assessment, how are findings communicated to relevant stakeholders?
- What is the process for addressing identified weaknesses or gaps in the security controls?
- How do you track and manage the remediation of any issues found during the security control assessments?
- Are external third-party assessors or auditors involved in any of the periodic assessments?
- How do you incorporate feedback from incidents, breaches, or other security events into the assessment process?
- Are there specific metrics or key performance indicators (KPIs) used to measure the effectiveness of security controls?
- How do you ensure that the assessment process remains up-to-date with evolving threats and vulnerabilities?
- How do you integrate the results of security control assessments with other risk management or compliance processes?
- Are employees or end-users involved or considered in any part of the security control assessment process?
- How do you handle situations where immediate action is required based on the assessment findings?
- How do you ensure that the security control assessment process itself doesn't introduce new vulnerabilities or risks?
- How do you validate or test the effectiveness of controls, especially after they have been modified or updated?

Copyright © 2023 Redspin, a Division of Clearwater. All Rights Reserved.

- How do you store, secure, and manage the data and findings from these periodic assessments?
- How do you ensure that the approach to periodic security control assessments aligns with NIST guidelines and broader organizational cybersecurity objectives?

Security Assessment

CA.L2-3.12.2

Basic

Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

- How do you identify deficiencies or vulnerabilities in your organizational systems?
- Describe the process for developing plans of action in response to identified deficiencies or vulnerabilities.
- Who is responsible for creating, reviewing, and approving these plans of action?
- How do you prioritize which deficiencies or vulnerabilities to address first?
- What metrics or criteria are used to determine the success or completion of a plan of action?
- How are stakeholders informed and involved in the plans of action?
- What tools or platforms do you use to track and manage the progress of plans of action?
- How frequently are plans of action reviewed and updated?
- How do you ensure that implemented solutions or patches don't introduce new vulnerabilities?
- Describe any challenges or issues you've faced while implementing plans of action and how they were addressed.
- How do you integrate the plans of action process with other risk management and security processes?
- How do you manage third-party vendors or partners in relation to deficiencies or vulnerabilities in systems they provide or support?
- How do you handle situations where a vulnerability is identified but can't be immediately mitigated?
- Are there mechanisms in place to test or validate the effectiveness of measures taken in plans of action?
- How do you handle feedback or concerns related to plans of action?
- Describe any collaboration with external entities, industry peers, or security experts in the development of plans of action.
- How do you ensure that the organization's response to deficiencies and vulnerabilities aligns with industry best practices and standards?

Copyright © 2023 Redspin, a Division of Clearwater. All Rights Reserved.

- How do you educate and train relevant personnel on the importance and procedures related to plans of action?
- Are there periodic reviews or assessments to ensure the effective implementation and success of plans of action?
- How do you ensure that the approach to developing and implementing plans of action aligns with NIST guidelines and the organization's broader cybersecurity objectives?

Security Assessment

CA.L2-3.12.3

Basic

Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

- How do you ensure continuous monitoring of your security controls?
- What tools, platforms, or technologies are employed for the ongoing monitoring of security controls?
- How frequently are security controls assessed for their effectiveness?
- Describe the process for addressing and rectifying identified weaknesses or inefficiencies in security controls.
- How do you prioritize which security controls to monitor based on risk or potential impact?
- How are changes in the threat landscape incorporated into the ongoing monitoring process?
- How do you ensure that third-party vendors or integrated solutions adhere to your organization's standards for security control monitoring?
- What metrics or indicators are used to measure the effectiveness of security controls?
- How are stakeholders or decision-makers informed about the results of security control monitoring?
- How do you handle situations where a security control is determined to be ineffective or compromised?
- Are there automated alerts or mechanisms in place to notify relevant teams of potential security control failures or inefficiencies?
- How do you integrate the results of security control monitoring with other security processes, such as incident response or risk management?
- How do you ensure that the monitoring process itself does not introduce additional vulnerabilities or risks?
- How do you manage feedback or concerns related to the effectiveness of security controls from internal or external sources?

Copyright © 2023 Redspin, a Division of Clearwater. All Rights Reserved.

- Describe any challenges or issues you've faced related to the ongoing monitoring of security controls and how they were addressed.
- How do you ensure that monitoring processes are updated to align with new or updated security controls?
- How do you stay updated on best practices and industry standards related to security control monitoring?
- Are there periodic security audits or assessments to validate the comprehensiveness and effectiveness of your monitoring processes?
- How do you ensure continuity in security control monitoring during organizational changes, system upgrades, or the introduction of new technologies?
- How do you ensure that the approach to monitoring security controls on an ongoing basis aligns with NIST guidelines and broader cybersecurity objectives?

Security Assessment

3.12.4

Basic

Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

- Do you have a documented system security plan in place, and how often is it updated?
- How do you define and describe system boundaries within the security plan?
- Describe the process used to determine system environments of operation. How are they documented in the security plan?
- How does the security plan detail the implementation of security requirements?
- How are relationships or connections to other systems documented within the security plan?
- What stakeholders are involved in the development and review of the system security plan?
- How do you ensure that the system security plan remains aligned with the organization's broader cybersecurity strategy and objectives?
- Describe the process for handling changes or updates to the system that might impact the security plan.
- How do you communicate updates or changes to the security plan to relevant stakeholders?
- How do you ensure that third-party vendors or partners are aware of and adhere to the requirements outlined in the system security plan?
- What tools or platforms are used to manage, track, and update the system security plan?

Copyright © 2023 Redspin, a Division of Clearwater. All Rights Reserved.

- How do you validate or test the effectiveness and accuracy of the information provided in the security plan?
- How do you manage the security of the system security plan itself to prevent unauthorized access or modifications?
- Are there specific protocols or standards that you follow in the development and documentation of the security plan?
- How do you ensure continuity and consistency in the security plan during organizational changes, system migrations, or the introduction of new technologies?
- How do you handle feedback or concerns from stakeholders related to the content or updates of the system security plan?
- Are there periodic audits or assessments to validate the comprehensiveness and effectiveness of the system security plan?
- How do you incorporate lessons learned from security incidents or breaches into the security plan updates?
- How do you ensure that the system security plan addresses both current and emerging threats or vulnerabilities?
- How do you ensure that the approach to developing, documenting, and updating the system security plan aligns with NIST guidelines and compliance requirements?

Copyright © 2023 Redspin, a Division of Clearwater. All Rights Reserved.

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

Copyright © 2023 Redspin, a Division of Clearwater. All Rights Reserved. All trademarks, service marks and tradenames referenced in this material are the property of their respective owners.