GUIDE

Redspin
A Division of Clearwater

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

Think of this as checking the weather before going on a hike. By identifying potential threats and vulnerabilities, organizations can prepare and guard against them. This involves systematically identifying, evaluating, and understanding potential threats and vulnerabilities that could adversely impact an organization's assets and operations. By assessing and evaluating these risks, organizations may prioritize their resources and responses based on the needs of the organization.

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?

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?

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

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.

Risk Assessment

RA.L2-3.11.3

Derived

Remediate vulnerabilities in accordance with risk assessments.

- How do you prioritize vulnerability remediation based on your risk assessments?
- Describe the process for conducting risk assessments on identified vulnerabilities.
- What tools or platforms do you use for vulnerability scanning and risk assessment?
- How frequently are vulnerability assessments conducted within the organization?
- Once a vulnerability is identified, what is the typical timeframe for its remediation based on its risk rating?
- How do you ensure that high-risk vulnerabilities are addressed promptly?
- What mechanisms are in place to track and monitor the remediation of identified vulnerabilities?
- How do you handle vulnerabilities for which no immediate patch or fix is available?
- How do you validate that a vulnerability has been successfully remediated?
- Are there automated alerts or notifications in place for critical or high-risk vulnerabilities?
- How do you communicate vulnerability information and remediation status to relevant stakeholders within the organization?
- How do you handle vulnerabilities associated with third-party software or systems?
- Describe any challenges or issues you've faced related to vulnerability remediation and how they were addressed.
- How do you ensure that vulnerability remediation activities do not disrupt organizational operations or services?
- How do you integrate vulnerability remediation with other security operations, such as incident response or threat intelligence?
- How do you stay informed about emerging vulnerabilities or threats relevant to your organization's systems and technologies?
- Are there periodic security audits or assessments to validate the effectiveness of your vulnerability remediation processes?
- How do you manage feedback or concerns related to vulnerability remediation from users or departments?
- How do you collaborate with external entities, industry groups, or security communities to enhance your vulnerability remediation processes?
- How do you ensure that the approach to vulnerability remediation based on risk assessments aligns with NIST guidelines and broader cybersecurity objectives?

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

Risk Assessment

RA.L2-3.11.1

Basic

Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI

- How frequently do you conduct vulnerability scans on your organizational systems and applications?
- Which tools or solutions are employed for vulnerability scanning within your environment?
- How do you ensure that newly identified vulnerabilities are promptly scanned for in your systems and applications?
- Describe the process for reviewing and analyzing the results of vulnerability scans.
- How do you prioritize vulnerabilities identified during the scans?
- What is the protocol for addressing or remediating identified vulnerabilities?
- Are there automated alerts or notifications set up to inform relevant stakeholders of critical vulnerabilities?
- How do you handle false positives or discrepancies identified during vulnerability scans?
- How are third-party systems, applications, or integrations handled in your vulnerability scanning process?
- Describe the process for updating or refining scan criteria and configurations in response to evolving threats or new vulnerability definitions.
- How do you ensure that vulnerability scans do not adversely affect system performance or availability?
- How do you manage vulnerability scanning for cloud environments or remote infrastructure?
- Are there specific challenges or considerations you've encountered in your vulnerability scanning process, and how were they addressed?
- How do you maintain and update your vulnerability database or feed to ensure it reflects the latest known vulnerabilities?
- How do you ensure that all components, including legacy systems, are included in the vulnerability scanning process?
- Describe any integration between your vulnerability scanning tools and other security or incident response systems.
- How do you validate the effectiveness of your vulnerability scanning process in identifying and reporting real-world threats?
- Are there periodic reviews, assessments, or third-party validations of your vulnerability scanning procedures?

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

- How do you educate and train relevant personnel on the importance and procedures of vulnerability scanning?
- How do you ensure that your vulnerability scanning process and protocols align with NIST guidelines and broader cybersecurity objectives?

Risk Assessment

RA.L2-3.11.2

Derived

Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

- How frequently do you conduct vulnerability scans on your organizational systems and applications?
- Which tools or solutions are employed for vulnerability scanning within your environment?
- How do you ensure that newly identified vulnerabilities are promptly scanned for in your systems and applications?
- Describe the process for reviewing and analyzing the results of vulnerability scans.
- How do you prioritize vulnerabilities identified during the scans?
- What is the protocol for addressing or remediating identified vulnerabilities?
- Are there automated alerts or notifications set up to inform relevant stakeholders of critical vulnerabilities?
- How do you handle false positives or discrepancies identified during vulnerability scans?
- How are third-party systems, applications, or integrations handled in your vulnerability scanning process?
- Describe the process for updating or refining scan criteria and configurations in response to evolving threats or new vulnerability definitions.
- How do you ensure that vulnerability scans do not adversely affect system performance or availability?
- How do you manage vulnerability scanning for cloud environments or remote infrastructure?
- Are there specific challenges or considerations you've encountered in your vulnerability scanning process, and how were they addressed?
- How do you maintain and update your vulnerability database or feed to ensure it reflects the latest known vulnerabilities?
- How do you ensure that all components, including legacy systems, are included in the vulnerability scanning process?

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

- Describe any integration between your vulnerability scanning tools and other security or incident response systems.
- How do you validate the effectiveness of your vulnerability scanning process in identifying and reporting real-world threats?
- Are there periodic reviews, assessments, or third-party validations of your vulnerability scanning procedures?
- How do you educate and train relevant personnel on the importance and procedures of vulnerability scanning?
- How do you ensure that your vulnerability scanning process and protocols align with NIST guidelines and broader cybersecurity objectives?

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.