





Preparing for Your CMMC Interview: Commonly Asked Questions – Incident Response Edition

Incident Response operates much like our emergency services, responding quickly and appropriately to a fire or other emergency. It encompasses the strategies, processes, procedures, tools, resources, training, and other elements that are necessary to ensure an appropriate and meaningful response through the detection, management, and mitigation of security incidents. The primary focus is to respond in a manner that limits damage, reduces recovery time and costs, and ensures that the organization may resume normal operations as swiftly as possible.

Key

-  Domain Family
-  Identifier
-  Basic | Derived
-  Security Requirement

Security Requirement Table of Contents

Incident Response

- Test the organizational incident response capability.....4
- Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.....5
- Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.....6

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

IR.L2-3.6.3

Derived

Test the organizational incident response capability.

- How often does your organization conduct incident response tests or drills?
- What methodologies or frameworks do you use to simulate incident scenarios during testing?
- How do you ensure that your incident response tests are comprehensive and representative of real-world threats?
- Who participates in the incident response tests, and what roles do they play?
- How do you incorporate lessons learned from past incidents into your testing scenarios?
- Are the results of incident response tests documented and communicated to relevant stakeholders?
- How do you measure the effectiveness of your incident response capability during testing?
- Are third-party entities or external experts involved in any aspect of the incident response testing?
- How do you handle gaps or weaknesses identified during incident response testing?
- Are there automated tools or platforms used to facilitate or evaluate the incident response tests?
- How do you ensure that sensitive or critical data is protected during incident response testing?
- Do you conduct both tabletop exercises and live drills for incident response testing?
- How do you incorporate feedback from participants or observers into refining your incident response capability?
- How do you update or adjust your incident response plan based on the outcomes of tests?
- Are there specific scenarios, like data breaches or ransomware attacks, that are prioritized in your incident response testing?
- How do you handle the communication and coordination aspects during incident response tests?
- How do you ensure that new employees or team members are familiarized with the incident response process through testing?
- How do you balance operational needs and business continuity with incident response testing?
- Are there any legal, regulatory, or contractual obligations that influence how you conduct incident response testing?
- How do you ensure that your approach to testing the incident response capability aligns with NIST guidelines and broader cybersecurity objectives?



Incident Response



IR.L2-3.6.1



Basic



Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

- How have you structured your incident-handling capability for organizational systems?
- Describe the preparation measures you have in place for potential security incidents.
- What tools or systems do you use for the detection of security incidents?
- How do you analyze and categorize incidents once they are detected?
- Describe your procedures for containing security incidents, both short-term and long-term.
- What is your process for system recovery after an incident has occurred?
- How do you communicate with affected users during and after a security incident?
- How often do you conduct drills or simulations to test your incident-handling capabilities?
- How do you ensure continuous improvement of the incident-handling process based on lessons learned from past incidents?
- How are roles and responsibilities defined within your incident-handling team?
- What training and awareness programs are in place for your incident response team and the broader organization?
- How do you coordinate with external entities, such as law enforcement or other organizations, during and after a security incident?
- Are there specific procedures for handling incidents involving sensitive or regulated data?
- How do you prioritize and manage multiple incidents if they occur simultaneously?
- What mechanisms are in place to ensure the confidentiality and integrity of data during an incident?
- How do you integrate your incident-handling capability with other security measures, such as threat intelligence or vulnerability management?
- How do you measure the effectiveness of your incident-handling capability?
- Describe any challenges or issues you've faced in establishing or operating your incident-handling capability and how they were addressed.
- How do you ensure that your incident-handling processes and procedures align with NIST guidelines?
- How frequently do you review and update your incident-handling procedures to adapt to evolving threats and organizational changes?



Incident Response



IR.L2-3.6.2



Basic



Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.

- How does your organization define a security incident?
- Describe the process for tracking and documenting incidents once they are detected.
- Which tools or platforms are used for incident tracking and documentation?
- Who are the designated officials within the organization responsible for handling and overseeing incident response?
- What is the process for escalating and reporting incidents to these officials?
- How are incidents categorized or prioritized based on their severity or impact?
- Are there specific protocols for reporting incidents to external authorities or regulatory bodies? If so, which ones?
- What is the timeline or deadline for reporting incidents internally and externally?
- How does your organization ensure confidentiality and integrity while documenting and reporting incidents?
- How are stakeholders or affected parties informed about incidents?
- How do you handle incidents involving third-party vendors or partners?
- Describe any challenges or issues you've faced in incident tracking, documentation, or reporting, and how they were addressed.
- How do you incorporate feedback from post-incident reviews or assessments to refine your reporting process?
- Are there periodic drills or simulations to test and refine the incident reporting process?
- How do you ensure that all employees are aware of and adhere to the incident reporting process?
- How does your organization handle incidents that may have legal or public relations implications?
- Are there mechanisms in place to provide updates or follow-ups on previously reported incidents?
- How do you collaborate with external entities, industry peers, or security experts to stay updated on best practices for incident reporting?
- How do you ensure the continuity of business operations during and after the incident reporting process?
- How do you ensure that the incident tracking, documentation, and reporting processes align 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.



40 Burton Hills Blvd
Suite 200
Nashville, TN 37215

info@redspin.com
www.redspin.com